Microsoft Bing's Digital Services Act (DSA) and Code of Conduct on Disinformation (COCD) Report

DSA: June 1, 2025 to May 31, 2026

COCD: July 1, 2025 to May 31, 2026

Table of Contents

Independent Accountant's Report – Digital Services Act (DSA) **2**

Management of Microsoft Bing's Assertion – Digital Services Act (DSA) **6**

Independent Accountant's Report – Code of Conduct on Disinformation (COCD) **7**

Management of Microsoft Bing's Assertion – Code of Conduct on Disinformation (COCD) **11**

Appendix 1 – The specific test procedures we performed, along with the nature, timing, and results of those tests **12**

Appendix 1A – Digital Services Act (DSA) **15**

Summary of Audit Conclusions at the Obligation Level 16
Section 1: Provisions applicable to all providers of intermediary services 17
Section 2: Additional provisions applicable to providers of hosting services, including online platforms 34
Section 3: Additional provisions applicable to providers of online platforms 34
Section 4: Additional provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders 34
Section 5: Additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks 35
Section 6: Other provisions concerning due diligence obligations 89

Appendix 1B – Code of Conduct on Disinformation (COCD) **90**

Summary of Audit Conclusions at the Commitment and Measure Level 91
Section 1: Preamble 92
Section 2: Scrutiny of ad placements 92
Section 3: Political advertising 92
Section 4: Integrity of services 93
Section 5: Empowering users 95
Section 6: Empowering the research community 108
Section 7: Empowering the fact-checking community 114
Section 8: Transparency Centre 115
Section 9: Permanent Task-force 124
Section 10: Monitoring of the Code 131

Appendix 2 – Obligations that are out of scope (DSA) **140**

Appendix 3 - Template for the audit report referred to in Article 6 of Delegated Regulation **142**

Section A: General information 143
Section B: Auditing organization 144
Section C: Summary of the main findings 146
Section D: Description of the findings: compliance with Regulation (EU) 2022/2065 147
Section E: Description of the findings concerning compliance with codes of conduct and crisis protocol 150
Section F: Third parties consulted 152
Section G: Any other information the auditing body wishes to include in the audit report (such as a description of possible inherent limitations) 153

Appendix 4A – Written agreement between VLOSE and the auditing organization (DSA) **154**

Appendix 4B – Written agreement between VLOSE and the auditing organization (COCD) **178**

Appendix 5 – Documents relating to the audit risk analysis **202**

Appendix 6 – Documents attesting that the auditing organization complies with the obligations laid down in Article 37.3 point (a), (b), (c) **211**

Appendix 7 – Documentation and results of any tests performed by the auditing organization, including as regards algorithmic systems of the Audited Provider **213**

Appendix 8 – Definitions **215**

Deloitte & Touche LLP
1015 Second Avenue, Suite 500
Seattle, WA 98104
Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

Independent Accountant's Report – Digital Services Act (DSA)

Microsoft Ireland Operations Limited

One Microsoft Place
South Country Business Park, Leopardstown
Dublin 18, D18 P521

Scope

We were engaged by Microsoft Corporation to examine the assertion ("Assertion") of Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries ("Audited Provider" or "Microsoft"), included in Appendix 1A, regarding in-scope services and features identified by management for Bing's ("audited service") compliance with all applicable obligations (the "Subject Matter") in aggregate and each applicable obligation individually, referred to in Article 37(1)(a) of European Union Regulation 2022/2065 of the European Parliament and the Council (the "Act") (the "Specified Requirements") during the period from June 1, 2025 through May 31, 2026 (the "Examination Period"). Our responsibility is to express an opinion on the audited service's compliance with the Specified Requirements based on conducting our examination in accordance with our professional standards. Unless referenced otherwise, each obligation is defined at the sub-article level of the Specified Requirements.

Additionally, the information included in the Audited Provider's separately provided Audit Implementation Report is presented by the Audited Provider to provide additional information. Such information has not been subject to the procedures applied in our examination, and accordingly, we do not express an opinion, conclusion, or any form of assurance on it.

Microsoft's responsibilities

The management of the Audited Provider is responsible for:

- Determining the applicability of all obligations and each obligation in the Act during the Examination Period;
- Identifying which Bing services and features are in scope or out of scope for the Specified Requirements;
- Complying with the Specified Requirements by designing, implementing, and maintaining the audited service's system and manual processes (and related controls) to comply with the Act;
- Selecting the Specified Requirements, making interpretations, and developing benchmarks, as needed, to implement the Specified Requirements;
- Evaluating and monitoring Bing's compliance with the Specified Requirements;
- Its Assertion of compliance with the Specified Requirements; and
- Having a reasonable basis for its Assertion;

This responsibility includes establishing and maintaining internal controls, maintaining adequate records, and making estimates relevant to the preparation of its Assertion and evaluation of its audited service's system and manual processes (and related controls) in place, such that it is free from material misstatement, whether due to fraud or error.

Our responsibilities and procedures performed

Our responsibility is to:

- Plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the audited service complies with the Specified Requirements;
- Form an independent opinion on whether the audited service complies with the Specified Requirements based on the procedures we have performed and the evidence we have obtained; and
- Express our opinion to the Audited Provider.

For additional responsibilities of Microsoft and Deloitte & Touche LLP (hereafter referred to as D&T), see Appendix 4A for the engagement statement of work executed on February 13, 2026.

We conducted our examination in accordance with the *International Standard for Assurance Engagements Other Than Audits or Reviews of Historical Financial Information* ("ISAE 3000 (Revised)"), the attestation standards established by the American Institute of Certified Public Accountants ("AICPA"), Section III and IV of the Commission Delegated Regulation (EU) 2024/436, supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines ("Delegated Regulation") dated October 20, 2023 and the terms of reference for this examination as agreed with Microsoft on February 13, 2026. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether Bing complied, in all material respects, with the Specified Requirements referenced in the Independent Accountant's Report. The nature, timing, and extent of the selected procedures depend on our judgment, including our assessment of the risks of material noncompliance, whether due to fraud or error. We believe the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following procedures, among others:

- Obtaining an understanding of the characteristics of the services provided by the Audited Provider;
- Evaluating the appropriateness of the Specified Requirements applied and their consistent application, including evaluating the reasonableness of estimates made by the Audited Provider;
- Obtaining an understanding of the systems and processes implemented to comply with the Act, including obtaining an understanding of the internal control environment relevant to our examination, but not for the purpose of expressing an opinion on the effectiveness of the Audited Provider's internal control;
- Identifying and assessing the risks of whether compliance with the Specified Requirements is incomplete or inaccurate, whether due to fraud or error, and designing and performing further assurance procedures responsive to those risks; and
- Obtaining assurance evidence that is sufficient and appropriate to provide a basis for our opinion.

We collected evidence to assess Bing's compliance with the Specified Requirements during the Examination Period from June 1, 2025 through May 31, 2026.

Our independence and quality management

We are required to be independent of Microsoft and to meet our other ethical responsibilities, as applicable, for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA and other relevant ethical requirements required for our engagement.

We also applied the International Standard on Quality Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements, and the AICPA's quality management standards, which require that we design, implement, and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Furthermore, Appendix 6 includes our attestation that the auditing organization complies with the obligations laid down in Article 37(3), points (a), (b), and (c).

Description of additional information on each of the applicable audit obligations

The opinion; criteria, materiality thresholds, procedures, and results; overview and description of information relied upon as audit evidence; explanation of how the reasonable level of assurance was achieved; notable changes to the systems and functionalities audited; identification of any specific element which could not be examined (if applicable) or conclusion not reached; and other relevant observations and findings associated with our examination of the obligations are included in Appendix 1A. Additionally, our summary of risk analysis under Article 9 of the Act, including our assessment of inherent, control, and detection risk for each obligation, is included in Appendix 5. See Appendix 2 for a listing of obligations not subjected to procedures since they were not applicable during the Examination Period.

Inherent limitations

The services in the digital sector and the types of practices relating to these services can change quickly and significantly. Therefore, projections of any evaluation to future periods are subject to the risk that the entity's compliance with the Specified Requirements may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

The Subject Matter is subject to measurement uncertainties resulting from limitations inherent in the Subject Matter and the methods used in determining such systems and processes implemented to comply with the Specified Requirements. The selection of different but acceptable measurement techniques, including benchmarks, can result in materially different measurements, and the precision of various measurement techniques may also vary.

Our examination was limited to certain aspects of Bing's algorithmic systems, as required by Regulation (EU) 2022/2065. Furthermore, algorithms may not consistently operate as intended or at an appropriate level of precision. Because of their nature and inherent limitations, algorithms may introduce biases in the human programmer, resulting in repeated errors or favoring certain results or outputs by the model in favor of certain results. Accordingly, we do not express an opinion or other form of assurance on the design, operation, and monitoring of the algorithmic systems.

It is inherently judgmental to perform risk assessments, including the identification of systemic risks. Risk assessments are often conducted at a specific point in time and may not capture the dynamic nature of risks. Because the identification of systemic risks relies on known risks and expert judgment, the identification of systemic risks may not account for new or unprecedented events for which there is limited or no historical information.

Emphasis of certain matters

Applying the Specified Requirements requires the audited service to develop benchmarks and interpret obligations, including certain terminology. We deemed these benchmarks and interpretations necessary for report users to make decisions, and they are described in Appendix 1A for applicable obligations.

We are not responsible for the Audited Provider’s interpretations of, or compliance with, laws, statutes, and regulations (outside of the Specified Requirements) applicable to Microsoft in the jurisdictions within which Microsoft operates, including the determination of which obligations are applicable to the audited service. Accordingly, we do not express an opinion or other form of assurance on the Audited Provider’s compliance or legal determinations.

Our examination included understanding and assessing certain internal controls. Because of their nature and inherent limitations, controls may not prevent, detect, or correct all errors or fraud that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that internal controls may become inadequate because of changes in conditions, that the degree of compliance with such internal controls may deteriorate, or that changes made to the system or internal controls, or the failure to make needed changes to the system or internal controls, may alter the validity of such evaluations.

Opinion

Under Article 37(4)(g) of the Act, the conclusions on compliance with the Specified Requirements, individually and in the aggregate, must be phrased as Positive, Positive with Comments, or Negative. Article 8(8) of the Delegated Regulation requires an explanation for individual Specified Requirements where an opinion could not be reached.

In our opinion, Bing complied with **46** Specified Requirements, individually, and in the aggregate, during the Examination Period, in all material respects. **Forty-four (44)** Specified Requirements resulted in a **Positive** conclusion. **Two (2)** Specified Requirements resulted in a **Positive with Comments** conclusion. This opinion equates to a **Positive with Comments** conclusion under Article 37(4)(g) of the Act.

Conclusions on each applicable individual Specified Requirement

For conclusions on each of the applicable Specified Requirements, see Appendix 1A.

Restricted use

This report is intended solely for the information and use of Microsoft, the European Commission, and the applicable Digital Services Coordinator of establishment as mandated under DSA Article 42(4) (collectively, the "Specified Parties") for assessing the audited service's compliance with the Specified Requirements, and is not intended to be, and should not be, used by anyone other than these Specified Parties or for other purposes.



August 25, 2026

Microsoft Ireland Operations Limited
One Microsoft Place
South Country Business Park
Leopardstown
Dublin 18
D18 P521

Management of Microsoft Bing's Assertion – Digital Services Act (DSA)

For the period from June 1, 2025 through May 31, 2026

We, as members of the management of Microsoft, are responsible for determining the applicability of all obligations in aggregate and each applicable obligation individually, referred to in Article 37(1)(a) of the European Union Regulation 2022/2065 of the European Parliament and of the Council (the "Act") (the "Specified Requirements") during the period from June 1, 2025 through May 31, 2026 (the "Examination Period"). Management is responsible for Bing's compliance with the Specified Requirements, and for identifying which Bing services and features are in scope or out of scope for the Specified Requirements. In addition, management selects or develops the criteria and benchmarks, which management believes provide an objective basis for measuring and reporting on the Specified Requirements. The criteria for the Specified Requirements selected by management have been included in Appendix 1A of the Independent Accountant's Report ("Appendix 1A") under the Audit Criteria label for each of the Specified Requirements ("Criteria").

Without providing legal opinion, management asserts the following:

- Bing in-scope services and features for the Specified Requirements include Answers, Autosuggest and Related Suggestions, Image, Video, Image Creator from Bing, Copilot Search: FKA Deep Search and Generative Search, and Bing Video Creator. Further, Bing out of scope services and features include Maps, Shopping, News, Travel, Translate, Discover Feed, and Advertisements (with the exception of Article 39).
- Bing determined that **46** Specified Requirements are applicable throughout the Examination Period.
- Bing complied with **46** of the Specified Requirements throughout the Examination Period. These are indicated with a **Positive** or **Positive with Comments** conclusion in Appendix 1A.
- Certain Specified Requirements either did not exist or were not applicable to Bing during the Examination Period. These are indicated as **out of scope** obligations in Appendix 2 of the Independent Accountant's Report.

Deloitte & Touche LLP
1015 Second Avenue, Suite 500
Seattle, WA 98104
Tel: +1 206 716 7000
Fax: +1 206 965 7000
www.deloitte.com

Independent Accountant's Report – Code of Conduct on Disinformation (COCD)

Microsoft Ireland Operations Limited

One Microsoft Place
South Country Business Park, Leopardstown
Dublin 18, D18 P521

Scope

We were engaged by Microsoft Corporation to examine the assertion ("Assertion") of Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries ("Audited Provider" or "Microsoft"), included in Appendix 1B, regarding in-scope services and features identified by management for Bing's ("audited service") compliance with all applicable commitments and measures (the "Subject Matter") in aggregate and for each applicable commitment and measure referred to in the Code of Conduct on Disinformation in Article 37(1)(b) of European Union Regulation 2022/2065 of the European Parliament and of the Council (the "Act") (the "Specified Requirements"), during the period from July 1, 2025 through May 31, 2026 (the "Examination Period"). Our responsibility is to express an opinion on the audited service's compliance with the Specified Requirements based on conducting our examination in accordance with our professional standards. Unless referenced otherwise, each measure is defined at the sub-commitment level of the Specified Requirements.

Additionally, the information included in the Audited Provider's separately provided audit implementation report is presented by the Audited Provider to provide additional information. Such information has not been subject to the procedures applied in our examination, and accordingly, we do not express an opinion, conclusion, or any form of assurance on it.

Microsoft's responsibilities

The management of the Audited Provider is responsible for:

- Determining the applicability of all commitments and measures and each commitment and measure in the Act during the Examination Period;
- Identifying which Bing services and features are in scope or out of scope for the Specified Requirements;
- Complying with the Specified Requirements by designing, implementing, and maintaining the audited service's system and manual processes (and related controls) to comply with the Act;
- Selecting the Specified Requirements, making interpretations, and developing benchmarks, as needed, to implement the Specified Requirements;
- Evaluating and monitoring Bing's compliance with the Specified Requirements;
- Its Assertion of compliance with the Specified Requirements;
- Having a reasonable basis for its Assertion

This responsibility includes establishing and maintaining internal controls, maintaining adequate records, and making estimates relevant to the preparation of its Assertion and evaluation of its audited service's system and manual processes (and related controls) in place, such that it is free from material misstatement, whether due to fraud or error.

Our responsibilities and procedures performed

Our responsibility is to:

- Plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the audited service complies with the Specified Requirements;

- Form an independent opinion on whether the audited service complies with the Specified Requirements based on the procedures we have performed and the evidence we have obtained; and
- Express our opinion to the Audited Provider.

For additional responsibilities of Microsoft and Deloitte & Touche LLP (hereafter referred to as D&T), see Appendix 4B for the engagement statement of work executed on May 5, 2026.

We conducted our examination in accordance with the International Standard for Assurance Engagements Other Than Audits or Reviews of Historical Financial Information ("ISAE 3000 (Revised)"), the attestation standards established by the American Institute of Certified Public Accountants ("AICPA"), Section III and IV of the Commission Delegated Regulation (EU) 2024/436, supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines ("Delegated Regulation") dated October 20, 2023 and the terms of reference for this examination as agreed with Microsoft on May 5, 2026. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether Bing complied, in all material respects, with the Specified Requirements referenced in the Independent Accountant's Report. The nature, timing, and extent of the selected procedures depend on our judgment, including our assessment of the risks of material noncompliance, whether due to fraud or error. We believe the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following procedures, among others:

- Obtaining an understanding of the characteristics of the services provided by the Audited Provider;
- Evaluating the appropriateness of the Specified Requirements applied and their consistent application, including evaluating the reasonableness of estimates made by the Audited Provider;
- Obtaining an understanding of the systems and processes implemented to comply with the Act, including obtaining an understanding of the internal control environment relevant to our examination, but not for the purpose of expressing an opinion on the effectiveness of the Audited Provider's internal control;
- Identifying and assessing the risks of whether compliance with the Specified Requirements is incomplete or inaccurate, whether due to fraud or error, and designing and performing further assurance procedures responsive to those risks; and
- Obtaining assurance evidence that is sufficient and appropriate to provide a basis for our opinion.

We collected evidence to assess Bing's compliance with the Specified Requirements during the Examination Period from July 1, 2025, through May 31, 2026.

Our independence and quality management

We are required to be independent of Microsoft and to meet our other ethical responsibilities, as applicable, for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA and other relevant ethical requirements required for our engagement.

We also applied the International Standard on Quality Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements, and the AICPA's quality management standards, which require that we design, implement, and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Furthermore, Appendix 6 includes our attestation that the auditing organization complies with the obligations laid down in Article 37 (3), points (a), (b), and (c).

Description of additional information on each of the applicable audit commitments

The opinion; criteria, materiality thresholds, procedures, and results; overview and description of information relied upon as audit evidence; explanation of how the reasonable level of assurance was achieved; notable changes to the systems and functionalities audited; identification of any specific element which could not be examined (if applicable) or conclusion not reached; and other relevant observations and findings associated with our examination of the commitments and measures are

included in Appendix 1B. Additionally, our summary of risk analysis under Article 9 of the Act, including our assessment of inherent, control, and detection risk for each measure, is included in Appendix 5.

Inherent limitations

The services in the digital sector and the types of practices relating to these services can change quickly and significantly. Therefore, projections of any evaluation to future periods are subject to the risk that the entity's compliance with the Specified Requirements may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

The Subject Matter is subject to measurement uncertainties resulting from limitations inherent in the Subject Matter and the methods used in determining such systems and processes implemented to comply with the Specified Requirements. The selection of different but acceptable measurement techniques, including benchmarks, can result in materially different measurements, and the precision of various measurement techniques may also vary.

It is inherently judgmental to perform risk assessments, including the identification of systemic risks. Risk assessments are often conducted at a specific point in time and may not capture the dynamic nature of risks. Because the identification of systemic risks relies on known risks and expert judgment, the identification of systemic risks may not account for new or unprecedented events for which there is limited or no historical information.

Emphasis of certain matters

Applying the Specified Requirements requires the audited service to develop benchmarks and interpret commitments and measures including certain terminology. We deemed these benchmarks and interpretations necessary for report users to make decisions, and they are described in Appendix 1B for applicable commitments and measures.

We are not responsible for the Audited Provider's interpretations of, or compliance with, laws, statutes, and regulations (outside of the Specified Requirements) applicable to Microsoft in the jurisdictions within which Microsoft operates, including the determination of which commitments and measures are applicable to the audited service. Accordingly, we do not express an opinion or other form of assurance on the Audited Provider's compliance or legal determinations.

Our examination included understanding and assessing certain internal controls. Because of their nature and inherent limitations, controls may not prevent, detect, or correct all errors or fraud that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that internal controls may become inadequate because of changes in conditions, that the degree of compliance with such internal controls may deteriorate, or that changes made to the system or internal controls, or the failure to make needed changes to the system or internal controls, may alter the validity of such evaluations.

Opinion

Under Article 37(4)(g) of the Act, the conclusions on compliance with the Specified Requirements, individually and in the aggregate, must be phrased as Positive, Positive with Comments, or Negative. Article 8(8) of the Delegated Regulation requires an explanation for individual Specified Requirements where an opinion could not be reached.

In our opinion, Bing complied with **34** Specified Requirements, individually, and in the aggregate, during the Examination Period, in all material respects. **Thirty-two (32)** Specified Requirements resulted in a **Positive** conclusion. **Two (2)** Specified Requirements resulted in a **Positive with Comments** conclusion. This opinion equates to a **Positive with Comments** conclusion under Article 37(4)(g) of the Act.

Conclusions on each applicable individual Specified Requirement

For conclusions on each of the applicable Specified Requirements, see Appendix 1B.

Restricted use

This report is intended solely for the information and use of Microsoft, the European Commission, and the applicable Digital Services Coordinator of establishment as mandated under DSA Article 42(4) (collectively, the "Specified Parties") for assessing the Audited Provider's compliance with the Specified Requirements, and is not intended to be, and should not be, used by anyone other than these Specified Parties or for other purposes.



August 25, 2026

Microsoft Ireland Operations Limited
One Microsoft Place
South Country Business Park
Leopardstown
Dublin 18
D18 P521

Management of Microsoft Bing's Assertion – Code of Conduct on Disinformation (COCD)

For the period from July 1, 2025 through May 31, 2026

We, as members of the management of Microsoft, are responsible for determining the applicability of all measures in aggregate and each applicable measure individually, referred to in the Code of Conduct on Disinformation ("Code of Conduct"), in Article 37(1)(b) of the European Union Regulation 2022/2065 of the European Parliament and of the Council (the "Act") (the "Specified Requirements") during the period from July 1, 2025 through May 31, 2026 (the "Examination Period"). Management is responsible for Bing's compliance with the Specified Requirements, and for identifying which Bing services and features are in scope or out of scope for the Specified Requirements. In addition, management selects or develops the criteria and benchmarks, which management believes provide an objective basis for measuring and reporting on the Specified Requirements. The criteria for the Specified Requirements selected by management have been included in Appendix 1B of the Independent Accountant's Report ("Appendix 1B") under the Audit Criteria label for each of the Specified Requirements ("Criteria").

Without providing legal opinion, management asserts the following:

- Bing in-scope services and features for the Specified Requirements include Answers, Autosuggest and Related Suggestions, Image, Video, Image Creator from Bing, Copilot Search: FKA Deep Seach and Generative Search, and Bing Video Creator. Further, Bing out-of-scope services and features include Maps, Shopping, News, Travel, Translate, Discover Feed, and Advertisements.
- Bing determined that **34** Specified Requirements are applicable throughout the Examination Period.
- Bing complied with **34** of the Specified Requirements throughout the Examination Period. These are indicated with a **Positive** or **Positive with Comments** conclusion in Appendix 1B.

Appendix 1 – The specific test procedures we performed, along with the nature, timing, and results of those tests

The specific test procedures we performed, along with the nature, timing, and results of those tests

Appendix 1A (Digital Services Act, herein after referred to as "DSA") and Appendix 1B (Code of Conduct on Disinformation, herein after referred to as "COCD") of the Independent Accountant's Reports for Microsoft Bing offer a detailed analysis of compliance with the DSA and COCD requirements. This section provides stakeholders with comprehensive insights into the obligations and commitments under Article 37.1.a of European Union Regulation 2022/2065, collectively referred to as "Specified Requirements".

Audit criteria composition

For DSA, the audit criteria for this examination consist of two primary elements: the specific requirements outlined by the DSA and the benchmarks and definitions provided by Microsoft. These benchmarks clarify the requirements and align them with the requirement for suitable criteria as defined by AT-C Section 315 of the AICPA Attestation Standards. This dual approach aids in interpreting the regulatory text for Bing and is detailed in the tables within Appendix 1A.

For COCD, the audit criteria for this examination consist of two primary elements: the specific commitments and measures detailed in the COCD and the benchmarks and definitions provided by Microsoft. These benchmarks clarify the requirements and align them with the requirement for suitable criteria as defined by AT-C Section 315 of the AICPA Attestation Standards. This dual approach aids in interpreting the regulatory text for Bing and is detailed in the tables within Appendix 1B.

Sampling approach

For both DSA and COCD, a robust sampling methodology is employed that aligns with AICPA guidance, facilitating effective control testing without the necessity to examine every item in a population. Sample sizes are determined based on factors such as population size, risk of control failure, and the auditor's assessment of the tolerable rate of deviation. This approach provides a reasonable basis for conclusions about the population. Both statistical and nonstatistical sampling methods are utilized. Statistical sampling uses mathematical models for sample size determination and result evaluation, enhancing objectivity. Nonstatistical sampling relies on auditor judgment, leveraging experience and understanding of the control operations. The results are evaluated to confirm that the sample is representative of the population and that controls are operating effectively.

Procedures for Control testing and Substantive testing

In accordance with the DSA and COCD, sufficient testing is conducted to confirm that digital platforms comply with transparency and accountability requirements. This involves two main types of testing: control testing and substantive testing.

Control testing

The effectiveness of internal controls related to DSA and COCD compliance is evaluated. This includes assessing platforms' systems for collecting and reporting data on content moderation activities to ensure transparency reports are accurate. Additionally, platforms are examined to confirm they meet DSA obligations and COCD commitments and measures, such as user complaint reporting and regulatory responses. For Very Large Online Search Engines (VLOSEs), the transparency and fairness of automated moderation tools are evaluated to ensure alignment with DSA and COCD standards.

Substantive testing

Substantive testing focuses on verifying the accuracy and completeness of transparency reports. The VLOSE's annual risk assessments and the effectiveness of their mitigation measures are also reviewed. Independent audits are conducted to assess overall compliance with the DSA obligations and the COCD commitments and measures, providing verification of transparency reports and risk management practices.

These procedures help confirm that digital platforms meet DSA obligations and COCD commitments and measures, promoting transparency and accountability in the digital services sector. We reached reasonable assurance through the performance of these controls and substantive testing procedures.

As part of the controls and substantive testing, we performed inquiries with management and detailed interviews with relevant personnel accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.

Allocation of responsibilities

The following table outlines the allocation of responsibilities for the various components within Appendix 1A and Appendix 1B:

Component	Responsibility
Audit criteria	Microsoft
Summary of controls, systems, and processes	Microsoft
Materiality threshold	Deloitte & Touche LLP
Procedures and information relied upon	Deloitte & Touche LLP
Changes to audit procedures during the examination	Deloitte & Touche LLP
Conclusion on compliance	Deloitte & Touche LLP
Recommendations	Deloitte & Touche LLP
Recommended timeframe to implement specific measures	Deloitte & Touche LLP

This introduction provides a structured framework for understanding Bing's compliance with the DSA and COCD, detailing the audit's scope, methodology, and division of responsibilities.

Reliability of information produced by Microsoft

We performed procedures to evaluate whether the information provided by the Audited Provider, which includes (a) information in response to ad hoc requests from the auditing organization, and (b) information used in the execution of a control or a process, was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Our procedures to evaluate whether this information was sufficiently reliable included procedures to address (a) the accuracy and completeness of source data, and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of controls and substantive testing.

Use of the work of others

We did not use the work of another practitioner, auditor, specialist, or other third party in performing this engagement. All procedures were planned, performed, and evaluated by D&T and the conclusion expressed herein is based solely on the evidence obtained through our procedures.

Appendix 1A – Digital Services Act (DSA)

The specific test procedures we performed, along with the nature, timing, and results of those tests

Summary of Audit Conclusions at the Obligation Level

The table below summarizes audit conclusions for in-scope obligations.

Note: DSA obligations under Sections 2, 3, 4, and 6 are not in scope. For additional information, please refer to Appendix 2.

Section 1	Section 5
11.1	24.2
11.2	24.3
11.3	34.1
12.1	34.2
12.2	34.3
14.1	35.1
14.2	36.1
14.4	37.1
14.5	37.2
14.6	37.3
15.1	37.4
	37.5
	37.6
	38
	39.1
	39.2
	39.3
	40.1
	40.3
	40.4
	40.5
	40.6
	40.7
	40.12
	41.1
	41.2
	41.3
	41.4
	41.5
	41.6
	41.7
	42.1
	42.3
	42.4
	42.5

Legend

- Positive – Compliant
- Positive with Comments – Compliant
- Negative – Partial Compliance and Remediated
- Negative – Partial Compliance
- Negative – Noncompliant
- Disclaimer of Opinion

Section 1: Provisions applicable to all providers of intermediary services

Article 11 DSA - Points of Contact for Member States' Authorities, the Commission, and the Board

Obligation:	Audit criteria:	Materiality threshold:
11.1	**Requirement:** Providers of intermediary services shall designate a single point of contact to enable them to communicate directly, by electronic means, with Member States' authorities, the Commission and the Board referred to in Article 61 for the application of this Regulation. **Definitions and Benchmarks:** • **Single point of contact:** The person, team, email address, or web page form which facilitates direct communication with the responsible person or team identified as the Point of Contact.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains an "EU Digital Services Act information" webpage for Bing that provides information on the single point of contact to enable Member States' authorities, the Commission, and the Board to contact Bing. Bing maintains and monitors the shared mailbox where the Member States' authorities can communicate with Bing. At least once a year, management reviews the contact information for the single point of contact published on Bing's EU DSA information webpage.	1. Inspected Microsoft's EU Digital Services Act information for Bing webpage throughout the DSA Examination Period to ascertain whether management has designated a single point of contact to enable them to communicate directly, by electronic means, with Member States' authorities, the Commission, and the Board as referred to in Article 61 for the application of this Regulation. 2. Inspected the single point of contact shared mailbox to ascertain Bing restricted access to the mailbox to appropriate and authorized individuals through the owners and members of the email alias. Furthermore, ascertained that Bing monitored the mailbox so that no direct communication from Member States' authorities is missed. 3. Inspected the annual review performed by management over the single point of contact's information to ascertain that a single point of contact was designated and whether it was reviewed and approved by management.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 11.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
11.2	**Requirement:** Providers of intermediary services shall make public the information necessary to easily identify and communicate with their single points of contact. That information shall be easily accessible and shall be kept up to date. **Definitions and Benchmarks:** • **Easily identify:** Bing used the information published to the following publicly available and discoverable web pages as a benchmark for determining whether the relevant information could be easily identified: – EU Digital Services Act information – Microsoft Support – Microsoft Services Agreement • **Single points of contact:** The person, team, email address, or web page form which facilitates direct communication with the responsible person or team identified as the Point of Contact. • **Easily accessible:** Bing used the examples listed in DSA Recital 43 as a benchmark to determine whether the relevant information was easily accessible.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains an "EU Digital Services Act information" webpage for Bing that provides information on the single point of contact to enable Member States' authorities, the Commission, and the Board to contact Bing. At least once a year, management reviews the contact information for the single point of contact published on Bing's EU DSA information webpage.	1. Inspected Microsoft's EU DSA information webpage for Bing throughout the DSA Examination Period to ascertain whether Bing has designated a single point of contact and ascertained that it is publicly available and accessible through their webpage. 2. Inspected Microsoft's EU DSA information webpage for Bing throughout the DSA Examination Period to ascertain whether: • The designated single point of contact's information is listed and is publicly available to enable Member States' authorities, the Commission, and the Board to contact Bing. • Information on the webpage about the single point of contact was up-to-date, easy to identify, and easily accessible. • Bing has identified the official language(s) of the Member State in which Bing has its main establishment or where its legal representative resides or is established. 3. Inspected the annual review performed by management over the single point of contact's information to ascertain whether the review included steps to confirm that the information is up to date and easily accessible.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 11.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
11.3	**Requirement:** Providers of intermediary services shall specify in the information referred to in paragraph 2 the official language or languages of the Member States which, in addition to a language broadly understood by the largest possible number of Union citizens, can be used to communicate with their points of contact, and which shall include at least one of the official languages of the Member State in which the provider of intermediary services has its main establishment or where its legal representative resides or is established. **Definitions and Benchmarks:** • **Point of contact:** The person, team, email address, or web page form which facilitates direct communication with the responsible person or team identified as the Point of Contact.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The information for a single point of contact is publicly available on Microsoft "EU Digital Services Act information webpage" for Bing and specifies the languages that are available to communicate, including a language broadly understood by the largest possible number of Union citizens, and at least one official language of each Member State.	1. Inspected evidence of the annual review performed by management over the single point of contact's information to ascertain whether management reviews Microsoft's EU DSA information webpage for Bing, confirming the webpage specifies which languages are available to communicate with the single point of contact, including a language broadly understood by the largest possible number of Union citizens and at least one official language of each Member State. 2. Inspected the designated single point of contact's information on Microsoft's EU DSA information webpage for Bing throughout the DSA Examination Period to reperform management's review and to ascertain whether the Website specifies which languages are available to communicate with the single point of contact, including a language broadly understood by the largest possible number of Union citizens and at least one official language of each Member State.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 11.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 12 DSA - Points of contact for recipients of the service

Obligation:	Audit criteria:	Materiality threshold:
12.1	**Requirement:** Providers of intermediary services shall designate a single point of contact to enable recipients of the service to communicate directly and rapidly with them, by electronic means and in a user-friendly manner, including by allowing recipients of the service to choose the means of communication, which shall not solely rely on automated tools. **Definitions and Benchmarks:** • **Single point of contact:** The person, team, email address, or web page form which facilitates direct communication with the responsible person or team identified as the Point of Contact. • **Directly and rapidly:** Straightforward in manner.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains an "EU Digital Services Act information" webpage for Bing that provides information for a designated point of contact, enabling service recipients to communicate directly and rapidly with Bing in a user-friendly manner. Bing allows service recipients to choose a means of communication that does not solely rely on automated tools. Service recipients can communicate via a tool called "Bing Report a Concern Tool" and/or a "Feedback Channel" option published on the information page. Additionally, management reviews the contact information for the single point of contact published on Bing's EU DSA information webpage at least once a year.	1. Inspected Microsoft's EU DSA information webpage for Bing throughout the DSA Examination Period to ascertain whether Bing has designated a single point of contact to enable recipients of the service to communicate with Microsoft directly and rapidly. 2. Inspected a sample of tickets for both the "Report a Concern" tool and "Feedback Channel" option and successfully traced tickets from each tool to ascertain whether there are other means of contacting the single point of contact and whether it is monitored, user-friendly, and does not solely rely on automated tools. 3. Inspected management's annual review for the single point of contact's information, to ascertain whether the review included steps to confirm that the designated single point of contact information was publicly available, enabling the recipients of the service to communicate with Microsoft through electronic means that do not solely rely on automated tools. 4. Inspected Bing's EU DSA information webpage throughout the DSA Examination Period to ascertain whether Microsoft's EU DSA information webpage for Bing has been kept up to date throughout the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 12.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
12.2	**Requirement:** In addition to the obligations provided under Directive 2000/31/EC, providers of intermediary services shall make public the information necessary for the recipients of the service in order to easily identify and communicate with their single points of contact. That information shall be easily accessible, and shall be kept up to date. **Definitions and Benchmarks:** • **Easily identifiable:** Bing used the information published to the following publicly available and discoverable web pages as a benchmark for determining whether the relevant information could be easily identified: – EU Digital Services Act information – Microsoft Support – Microsoft Services Agreement • **Single points of contact:** The person, team, email address, or web page form which facilitates direct communication with the responsible person or team identified as the Point of Contact. • **Easily accessible:** Bing used the examples listed in DSA Recital 43 as a benchmark to determine whether the relevant information was easily accessible.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains an "EU Digital Services Act information" webpage that provides information on the designated point of contact's information to enable recipients of the service to communicate with Bing. In addition, Bing has other means for its users to communicated with Bing such as "Bing Report a Concern Tool" and/or "Feedback Channel" options. At least once a year, management reviews and signs off on the contact information of the single point of contact published on Microsoft's EU DSA webpage for Bing to confirm that the single point of contact for recipients of the service is easily identifiable, publicly available, easily accessible, and kept up to date.	1. Inspected the single point of contact's information on Microsoft's EU DSA information webpage for Bing throughout the DSA Examination Period and ascertained that Bing has made public the information necessary for the recipients of the service in order to easily identify and communicate with Bing's single point of contact and that the information is easily accessible. 2. Inspected management's annual review over the single point of contact's information to ascertain whether the review included steps to confirm the information over Single Point of Contact for recipients of the service is easily identifiable, publicly available, easily accessible, and kept up to date. In addition, inspected management tools and ticketing systems used as other means for its users to communicate with Bing. 3. Inspected Bing's EU DSA information webpage throughout the DSA Examination Period, to ascertain whether Microsoft's EU DSA information webpage for Bing has been kept up to date throughout the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 12.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 14 DSA - Terms and conditions

Obligation:	Audit criteria:	Materiality threshold:
14.1	**Requirement:** Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format. **Definitions and Benchmarks:** • **Clear, plain, intelligible, user-friendly, and unambiguous language:** Clear, and able to be understood broadly by reasonable users of the service, as determined through review by management. • **Easily accessible:** Bing used the examples listed in DSA Recital 43 as a benchmark to determine whether the relevant information was easily accessible. • **Machine-readable:** Webpage is in a format that can be easily processed by a computer, such as in Hypertext Markup Language (HTML).	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Annually, management reviews Microsoft's terms and conditions for Bing to check they include information on the restrictions to the use of the service, on content moderation policies and processes, and on the complaint handling system.	1. Observed Bing's website to ascertain whether Microsoft's terms and conditions for Bing are publicly available for the recipients of the service and include information on: • Restrictions to the use of the service. • Measures and tools used for the purpose of content moderation, including algorithmic decision-making and human reviews. • Rules of procedure for the internal complaint handling system. 2. Inspected management's periodic review of Microsoft's terms and conditions for Bing to ascertain whether the review included steps to test that: • The policies, procedures, measures, and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of the internal complaint handling system, are included in the terms and conditions. • The terms and conditions are publicly available in clear, plain, intelligible, user-friendly, and unambiguous language, in an easily accessible and machine-readable format. 3. Inspected a log of changes made to the terms and conditions to ascertain whether the updates were reviewed and approved by the appropriate individuals.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 14.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
14.2	**Requirement:** Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions. **Definitions and Benchmarks:** • **Significant change:** A significant change to the applicable Terms and Conditions is one that impacts a recipient of the service's rights, remedies, obligations, or ability to access, use, or contest the service.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Recipients of the service are notified through Bing's services or by other means before significant changes are made, as determined by the Legal Team, to Microsoft's terms and conditions for Bing. Notifications are sent out via email, webpage notifications, and app notifications to all the recipients of the service, both verified and non-verified, in a timely manner, typically within 45 days prior to and 45 days after the publication of the new version of the terms.	1. Inspected a log of changes made to the terms and conditions to ascertain whether any significant changes were made during the Examination Period. 2. Inspected a sample of significant changes to ascertain that notifications were sent to inform the recipients of the service of the changes for any significant change.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 14.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
14.4	**Requirement:** Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter. **Definitions and Benchmarks:** • **Diligent, objective, and proportionate:** In a conscientious, balanced manner.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Annually, management reviews Microsoft's terms and conditions for Bing to check they include information on the restrictions to the use of the service, on content moderation policies and processes, and on the complaint handling system. Bing performs an annual Systemic Risk Assessment (SRA) over various risks including the risks to freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms. The results of the risk assessment inform Bing's terms and conditions and its enforcement. Bing has several mechanisms in which recipients of the service can raise feedback or concerns around the search product. Dedicated operation teams review those requests, complaints, and feedback, following Microsoft's terms and conditions for Bing, in a diligent, objective, and proportionate manner. Any action item taken is reported back to the recipients of the service with a documented rationale of the action taken.	1. Observed Bing's website to ascertain whether Microsoft's terms and conditions for Bing are publicly available for the recipients of the service and include information to enforce the restrictions referred to in Article 14.1. 2. Inspected management's periodic review of Microsoft's terms and conditions for Bing to ascertain whether the review included steps to test that Terms & Conditions were in compliance with Article 14.1. 3. Inspected evidence of Management's review of the system risk assessment to ascertain whether management aligned the contents of the assessment with the obligations of Article 14.4. 4. Inspected evidence that systemic risks were identified, analyzed, assessed, and mitigated, and that the SRA covered risks related to rights and legitimate interests, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 14.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
14.5	**Requirement:** Providers of very large online platforms and of very large online search engines shall provide recipients of services with a concise, easily-accessible and machine-readable summary of the terms and conditions, including the available remedies and redress mechanisms, in clear and unambiguous language. **Definitions and Benchmarks:** • **Concise:** An overview which allows recipients of the service to quickly understand the main topics and easily determine what topics are included in the document. • **Easily accessible:** Bing used the examples listed in DSA Recital 43 as a benchmark to determine whether the relevant information was easily accessible. • **Machine-readable:** Webpage is in a format that can be easily processed by a computer, such as in Hypertext Markup Language (HTML). • **Clear and unambiguous language:** Clear, and able to be understood broadly by reasonable users of the service, as determined through review by management.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft's terms and conditions for Bing are publicly accessible on its website, to be transparent with restrictions that they impose in their service for providers of intermediary services and to the recipients of the service. Annually, management reviews Microsoft's terms and conditions for Bing to evaluate if they are concise, easily-accessible, and summarized for recipients of the service in a machine-readable format, including providing available remedies and redress mechanisms in clear and unambiguous language.	1. Inspected Bing's website to ascertain whether Microsoft's terms and conditions for Bing are publicly available for recipients of the service and include a concise and easily-accessible summary of the terms and conditions in a machine-readable format, including the available remedies and redress mechanisms, in clear and unambiguous language. 2. Inspected management's periodic review of Microsoft's terms and conditions for Bing to ascertain whether the review included steps to test that Bing has provided the recipients of the service with a concise and easily-accessible summary of the terms and conditions in a machine-readable format, including the available remedies and redress mechanisms, in clear and unambiguous language. 3. Inspected updates made to Bing's terms and conditions to ascertain whether the updates were reviewed and approved by the appropriate individuals to ensure compliance with Article 14.5.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 14.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
14.6	**Requirement:** Very large online platforms and very large online search engines within the meaning of Article 33 shall publish their terms and conditions in the official languages of all the Member States in which they offer their services. **Definitions and Benchmarks:** • **Official Languages of all the Member States:** The 24 official languages of the EU: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, and Swedish.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft's terms and conditions for Bing are publicly available on its website in the 24 official languages of the 27 relevant EU Member States to be transparent with restrictions that they impose in their service for providers of intermediary services and to the recipients of the service. Annually, management reviews Microsoft's terms and conditions for Bing to check that they are published in the official languages of the 27 relevant EU Member States.	1. Inspected Microsoft Bing's website to ascertain whether Microsoft's terms and conditions for Bing are publicly available for recipients of the service and are published in 24 official languages of the 27 relevant EU Member States. 2. Inspected management's review of Microsoft's terms and conditions for Bing to ascertain whether the review included steps to test that Bing had published the terms and conditions in the 24 official languages of the 27 relevant EU Member States. 3. Inspected updates made to Microsoft's terms and conditions for Bing to ascertain whether the updates were reviewed and approved by the appropriate individuals. 4. For a sample of EU official languages, inspected the translated terms and conditions (for those published in languages other than English) to ascertain that they aligned with the terms and conditions available in English.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 14.6 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 15 DSA - Transparency reporting obligations for providers of intermediary services		
Obligation:	**Audit criteria:**	**Materiality threshold:**
15.1	**Requirement:** Providers of intermediary services shall make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period. Those reports shall include, in particular, information on the following, as applicable: a) for providers of intermediary services, the number of orders received from Member States' authorities including orders issued in accordance with Articles 9 and 10, categorised by the type of illegal content concerned, the Member State issuing the order, and the median time needed to inform the authority issuing the order, or any other authority specified in the order, of its receipt, and to give effect to the order; b) for providers of hosting services, the number of notices submitted in accordance with Article 16, categorised by the type of alleged illegal content concerned, the number of notices submitted by trusted flaggers, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, the number of notices processed by using automated means and the median time needed for taking the action; c) for providers of intermediary services, meaningful and comprehensible information about the content moderation engaged in at the providers' own initiative, including the use of automated tools, the measures taken to provide training and assistance to persons in charge of content, the number and type of measures taken that affect the availability, visibility and accessibility of information provided by the recipients of the service and the recipients' ability to provide information through the service, and other related restrictions of the service; the information reported shall be categorised by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied; d) for providers of intermediary services, the number of complaints received through the internal complaint handling systems in accordance with the provider's terms and conditions and additionally, for providers of online platforms, in accordance with Article 20, the basis for those complaints, decisions taken in respect of those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed; e) any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied. **Note:** The point (b) of the requirement is not relevant to the VLOSE. **Definitions and Benchmarks:** • **Machine-readable format:** Webpage is in a format that can be easily processed by a computer, such as in Hypertext Markup Language (HTML).	We have applied a 5% materiality threshold for this obligation.

- **Meaningful and comprehensible information:** Bing considers that the benchmark for this obligation is whether the items listed in Article 15.1 are all included in the report.
- **Availability, visibility, and accessibility of information:** Bing considers that these terms are the same as those used in DSA Article 3, Definitions. Specifically, Article 3(t) which provides further explanation: "demotion, demonetization, disabling of access to, or removal therefore, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account."

Summary of controls, systems, and processes:	Audit procedures:
Before Bing's DSA Transparency Report is released to the public on a semi-annual basis, it undergoes multiple levels of review by appropriate personnel, including both the core working group and leadership group, to determine that the details outlined in 15.1 are represented appropriately. Government Request Order (GRO) numbers are collected from multiple sources where the criteria established to extract the data have been baselined, approved, and tested. The numbers are then aggregated into a final number, which is reviewed and approved by the leadership teams, including Digital Safety Unit (DSU), Digital Trust & Safety (DigiTS), Bing Corporate, External and Legal Affairs (CELA), and Bing Product Management teams, before publication on the website. Digital Trust & Safety (DigiTS) collects data on content moderation initiated by Bing from multiple sources, using criteria that has been baselined, approved, and tested. DigiTS then aggregates the numbers into a final number, which is reviewed and approved by the leadership teams, including Digital Trust & Safety (DigiTS), Bing Corporate, External and Legal Affairs (CELA), and Bing Product Management (BPM) teams, before publication on the website. Appeals information is collected from multiple sources where the criteria established to extract the data has been approved and tested. The Digital Trust &	1. Inspected the DSA Transparency Reports published in August 2025 and February 2026 to ascertain that Bing made publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period and included the information specified in Article 15.1, where applicable. 2. Inspected the query criteria executed by Bing teams for calculating the number of GROs categorized, the number of content moderation actions taken by Bing, and the number of appeals as required in the Digital Services Act (DSA) for the August 2025 and February 2026 Transparency Reports, to ascertain whether the criteria to extract the data has been baselined, approved, and tested by management. 3. Inspected the DSA Transparency Reports published in August 2025 and February 2026 to ascertain whether the report described any automated means for content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied. 4. Inspected the review and approval performed by the core working group in August 2025 and February 2026 to ascertain whether management reviewed the reports to check that they were accessible in a machine-readable format and were published semi-annually, complying with transparency standards. Further, inspected the review and sign-off logs to ascertain whether relevant leadership teams, including DSU, DigiTS, CELA, and BPM, had approved their sections of the report, and whether the required reviews had been completed prior to publication on the website. 5. Inspected various communication channels and databases such as the Bing mailbox and the intermediary databases, which collect and process the related numbers, to validate the handling and classification of GROs received from EU member states. Further, recalculated and traced the number of GROs reported in the Transparency Reports for August 2025 and February 2026 to ascertain that the transparency reports contained details of the number of orders received to act against illegal content, the number of orders to provide information, median time to inform the authority of the receipt of the order to act against illegal content, and the median time to give affect to the order to act against illegal content completely and accurately.

Safety (DigiTS) team then aggregates the numbers into a final number, which is reviewed and approved by the leadership teams, including Digital Trust & Safety (DigiTS), Bing Corporate, External and Legal Affairs (CELA), and Bing Product Management teams, before publication on the website.

Any use of automated means for content moderation within the Bing environment, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied, are documented within the DSA Transparency Report.

6. Inspected various communication channels and databases, such as intermediary databases, which collect and process the related numbers to validate the actions taken to moderate content in EU member states. Further, selected a sample of content moderation actions to test the use of automated means to moderate content at Bing's own initiative leveraging automation that matches an image hash to the industry-standard hash set. Ascertained through the conjunction of these procedures that the Transparency Reports for August 2025 and February 2026 completely and accurately reported metrics related to content moderation engaged in at the providers' own initiative, including the use of automated tools, the measures taken to provide training and assistance to persons in charge of content, the number and type of measures taken that affect the availability, visibility, and accessibility of information provided by the recipients of the service and the recipients' ability to provide information through the service, and other related restrictions of the service, categorized by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied.
7. Inspected various communication channels and databases, such as the intermediary databases that collect and maintain the appeal numbers, to validate the handling of appeals received from recipients of the service, including whether there were appeals that would relate to a rate of error. Further, recalculated and traced the number of appeals on the Transparency Reports for August 2025 and February 2026 to ascertain the completeness and accuracy of the number of complaints received through the internal complaint handling systems in accordance with Bing's terms and conditions and the basis for those complaints, decisions taken in respect of those complaints, the median time needed for taking those decisions, the number of instances here those decisions were reversed, the use of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy, and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied.

Changes to audit procedures during the examination:

Shifted from controls and substantive testing to substantive testing only.

Conclusion:

Positive with Comments – In our opinion, Bing complied with Obligation 15.1 during the Examination Period, in all material respects.

Although the audited obligation has been met, we noted the following:

The Transparency Report published on February 27, 2026, for the period of July to December of 2025, was subsequently restated on May 18, 2026, following the self-identification, by management, of an incorrect classification of certain in-scope services. This classification error resulted in minor inaccuracies within the reported metrics and disclosures associated with Articles 15.1.c, 15.1.d, and 15.1.e.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
D&T recommends that Bing enhance its review and approval processes prior to the public release of the Transparency Report.	By January 31, 2027

Section 2: Additional provisions applicable to providers of hosting services, including online platforms

Bing is an online search engine, provisions for hosting services, including online platforms, are not applicable to Bing. As a result, Articles 16, 17, and 18 are not applicable to Bing.

Section 3: Additional provisions applicable to providers of online platforms

Bing is an online search engine, provisions for hosting services, including online platforms, are not applicable to Bing. As a result, Articles 19, 20, 21, 22, 23, 24 (1, 4-6), 25, 26, 27, and 28 are not applicable to Bing.

Section 4: Additional provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders

Bing does not allow consumers to conclude distance contracts with traders and Bing is an online search engine. As a result, Articles 29, 30, 31, and 32 are not applicable to Bing.

Section 5: Additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks

Article 24 DSA - Transparency reporting obligations for providers of online platforms

Obligation:	Audit criteria:	Materiality threshold:
24.2	**Requirement:** By 17 February 2023 and at least once every six months thereafter, providers shall publish for each online platform or online search engine, in a publicly available section of their online interface, information on the average monthly active recipients of the service in the Union, calculated as an average over the period of the past six months and in accordance with the methodology laid down in the delegated acts referred to in Article 33.3, where those delegated acts have been adopted. **Definitions and Benchmarks:** • N/A	We have applied a 5% materiality threshold for this obligation.

Summary of controls, systems, and processes:	Audit procedures:
Semi-annually, management reviews and approves the DSA Transparency Report to ascertain it specifies the monthly active recipients of the service in the Union, calculated as an average over the preceding six-month period and in accordance with the methodology laid down in the delegated acts referred to in Article 33.3, where such delegated acts have been adopted. Once approved, management makes the report publicly available. Prior to the issuance of the DSA Transparency Report, management reviews and approves the logic and code used for the calculation of monthly active recipients of the service included in the Transparency Report.	1. Inspected the query criteria executed by Bing teams for calculating the number of Monthly Active Users (MAUs), as required in the Digital Services Act (DSA), for the August 2025 and February 2026 Transparency Reports, to ascertain whether the criteria to extract MAU data has been baselined, approved, and tested by management. 2. Inspected the online versions of the Transparency Reports to ascertain whether they were published at least every six months and included the average monthly active recipients of the service in the Union. 3. Inspected the review and approval performed by the core working group to ascertain whether management's review confirmed the reports were publicly accessible and were published semi-annually, complying with transparency standards. Further, inspected the review and sign-off logs to ascertain whether all relevant leadership teams had approved their sections of the report and required reviews, including the review of code and logic used for calculation of monthly active recipients of the service, were completed prior to publication on the website. 4. Inspected data flow diagrams and configurations to understand the data transfer process involved in the calculation of MAUs. 5. Traced a sample of users from the source system through the intermediary databases to the final system; queried and recalculated the number of MAUs reported on the Transparency Reports for August 2025 and February 2026 to ascertain whether the numbers agree to the MAUs reported, and to confirm the reports' accuracy and completeness.

Changes to audit procedures during the examination:

Shifted from controls and substantive testing to substantive testing only.

Conclusion:

Positive – In our opinion, Bing complied with Obligation 24.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
24.3	**Requirement:** Providers of online platforms or of online search engines shall communicate to the Digital Services Coordinator (DSC) of establishment and the Commission, upon their request and without undue delay, the information referred to in paragraph 2, updated to the moment of such request. That Digital Services Coordinator or the Commission may require the provider of the online platform or of the online search engine to provide additional information as regards the calculation referred to in that paragraph, including explanations and substantiation in respect of the data used. That information shall not include personal data. **Definitions and Benchmarks:** • **Without undue delay:** Bing's benchmark for determining whether responses to regulator inquiries about its monthly active users are timely is the deadline listed by the regulator in its inquiry. • **Personal data:** Data directly identifying a specific person, as defined per GDPR Article 4.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing receives all requests from regulators around Monthly Active Users (MAUs) in its Single Point of Contact Outlook inbox and responds in a timely manner (i.e., by the date requested in the inquiry). Requests are tracked in a Single Point of Contact request tracking system.	1. Inspected the Single Point of Contact mailbox, the Single Point of Contact tracking system, and European Commission public webpages to ascertain whether Bing received any inquiries for information regarding Average Monthly Active Users from the regulators during the Examination Period. Furthermore, ascertained that there were no instances of inquiries from the regulators during the Examination Period, and therefore, no responses were required from Bing. 2. Inquired with management to ascertain whether Bing received any inquiries for information regarding Average Monthly Active Users from the regulators during the Examination Period. Corroborated there were no instances of inquiries from the regulators during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 24.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 34 DSA - Risk assessment

Obligation:	Audit criteria:	Materiality threshold:
34.1	**Requirement:** Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. They shall carry out the risk assessments by the date of application referred to in Article 33.6, second subparagraph, and at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks: a) the dissemination of illegal content through their services; b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter; c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security; d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being. **Definitions and Benchmarks:** • **Diligent and proportionate:** In a conscientious, balanced manner. • **Algorithmic systems:** Systems that rely on a structured set of rules or instructions designed to perform specific tasks or solve problems through automated processes (often personalized). • **Functionalities:** Operations that can be run on a computer or other electronic systems. • **Critical impact:** Significant, measurable impact that is substantial enough to affect the safety, security, and fundamental rights of users. • **Negative effects:** Potential or known harmful consequences or adverse impacts that may arise can hinder the exercise of fundamental rights as defined in the Charter of Fundamental Rights of the European Union (see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT). • **Personal data:** Data directly identifying a specific person as defined per GDPR Article 4.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Annually and as needed prior to launching changes or new features, the Digital Safety Unit delivers a report to the European Commission that identifies, analyses, and assesses systemic risks in the Union stemming from the design or functioning of its service and its related systems, including algorithmic systems, or from the use made of its services. The Microsoft Artificial Intelligence (MAI) Compliance team has a process in place to determine whether a risk assessment is needed prior to the launch of changes or new features on Bing with a potential critical impact on systemic risks in the Union. Annually, prior to submission to the European Commission (EC), the Article 41 Compliance Officer reviews and approves the systemic risk assessment report to inspect that it is conducted in accordance with a suitable methodology, includes the relevant systemic risks, and identifies mitigations that address the risks.	1. Inspected the Systemic Risk Assessment (SRA) and relevant supporting documents to ascertain whether the systemic risks are identified, analyzed, assessed, and mitigated, and the SRA is submitted to the EC in line with the reporting period set out in the DSA. 2. Inspected evidence of how risks are ranked to ascertain whether ranking considers severity and probability (e.g., risk matrix). 3. Inspected and recalculated the ranking of inherent risk and residual risks to ascertain whether the numbers agree to risk ranking performed by management, and the residual risk rating was reasonable for each risk area. 4. Inspected the SRA and supporting documents to ascertain whether management's assumptions were appropriate in relation to the risk assessment. 5. Inspected the SRA and supporting documents to ascertain whether systemic risks listed within the points (a) – (d) in Article 34.1 are included. 6. Inspected evidence to ascertain whether the requisite internal approvals were obtained in a timely manner prior to submission of the SRA. 7. Inspected evidence to ascertain that management observed the procedures and results of the SRA during the Examination Period prior to providing requisite approval for submission to the EC. 8. Inspected policies and processes describing the design and development of the SRA to ascertain whether report results are comprehensive and inclusive of the required stakeholders. 9. Inspected the Responsible AI (RAI) Assessments conducted for new features and changes to ascertain whether functionalities were evaluated for potential DSA impact using defined triaging criteria, reviewed through established RAI governance processes, and appropriately documented and tracked, including identification of functionalities subject to further Critical Impact Risk Assessment (CIRA). 10. Inspected the Critical Impact Risk Assessment (CIRA) questionnaire to ascertain whether functionalities that impact the DSA that are likely to have a critical impact on systemic risks in the points (a) – (d) in Article 34.1 are appropriately identified. 11. Sampled and inspected RAI and CIRA assessments conducted for new features and functionalities deployed to ascertain whether an off-cycle SRA was triggered. 12. Inspected processes for monitoring risks identified in the SRA to ascertain whether developments and evolution of risk would be addressed and reflected in the final SRA. 13. Inspected guidelines and publications published by the EC, including additional provisions as outlined in Article 13 of the Delegated Regulation.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 34.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
34.2	**Requirement:** When conducting risk assessments, providers of very large online platforms and of very large online search engines shall take into account, in particular, whether and how the following factors influence any of the systemic risks referred to in paragraph 1: a) the design of their recommender systems and any other relevant algorithmic system; b) their content moderation systems; c) the applicable terms and conditions and their enforcement; d) systems for selecting and presenting advertisements; e) data related practices of the provider. The assessments shall also analyse whether and how the risks pursuant to paragraph 1 are influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions. The assessment shall take into account specific regional or linguistic aspects, including when specific to a Member State. **Definitions and Benchmarks:** • **Algorithmic system:** A system that relies on structured set of rules or instructions designed to perform specific tasks or solve problems that provide outputs or results. • **Inauthentic use or automated exploitation of the service:** Use or other manipulation of the service by automated user accounts.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Annually and as needed prior to launching changes or new features, the Digital Safety Unit delivers a report to the European Commission that identifies, analyses, and assesses systemic risks in the Union stemming from the design or functioning of its service and its related systems, including algorithmic systems, or from the use made of its services. Annually, prior to submission to the European Commission (EC), the Article 41 Compliance Officer reviews and approves the systemic risk assessment report to inspect that it is conducted in accordance with a suitable methodology, includes the relevant systemic risks, and identifies mitigations that address the risks.	1. Inspected the SRA to ascertain whether the systemic risks were assessed in consideration of the factors outlined in the points (a) – (e) in Article 34.2. 2. Inspected the SRA to ascertain whether the assessment addressed the intentional manipulation of the service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions. 3. Inspected the SRA to ascertain whether the assessment addressed regional and linguistic considerations relevant across the Member States and to confirm that the report was relevant across the Member States.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 34.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
34.3	**Requirement:** Providers of very large online platforms and of very large online search engines shall preserve the supporting documents of the risk assessments for at least three years after the performance of risk assessments, and shall, upon request, communicate them to the Commission and to the Digital Services Coordinator of establishment. **Definitions and Benchmarks:** • **Upon request:** At the written direction of the Commission and the Digital Services Coordinator of establishment, through the established Single Point of Contact.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Annually and as needed prior to launching changes or new features, the Digital Safety Unit delivers a report to the European Commission that identifies, analyses, and assesses systemic risks in the Union stemming from the design or functioning of its service and its related systems, including algorithmic systems, or from the use made of its services. For a minimum of three years following the conduct of an annual or ad hoc Systemic Risk Assessment, the MAI Compliance Oversight team maintains a SharePoint site with supporting documentation used for the assessment.	1. Inspected the repository where the SRA and supporting documentation are stored to ascertain that, to date, no records have been deleted, and that documentation is being retained consistent with the requirement to preserve records for at least three years after the performance of the risk assessments. 2. Inspected email communication to ascertain whether the final SRA report and its supporting documents were sent to the EC. 3. Inquired with management and inspected the European Commission's website detailing communications between the EC and Bing to ascertain that that were no requests for information (RFIs) related to the SRA from the EC during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 34.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 35 DSA - Mitigation of risks		
Obligation:	**Audit criteria:**	**Materiality threshold:**
35.1	**Requirement:** Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable: a) adapting the design, features or functioning of their services, including their online interfaces; b) adapting their terms and conditions and their enforcement; c) adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision- making processes and dedicated resources for content moderation; d) testing and adapting their algorithmic systems, including their recommender systems; e) adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide; f) reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk; g) initiating or adjusting cooperation with trusted flaggers in accordance with Article 22 and the implementation of the decisions of out-of-court dispute settlement bodies pursuant to Article 21; h) initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively; i) taking awareness-raising measures and adapting their online interface in order to give recipients of the service more information; j) taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate; k) ensuring that an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces, and, in addition, providing an easy to use functionality which enables recipients of the service to indicate such information.	Not applicable

Definitions and Benchmarks:

- **Reasonable, proportionate, and effective mitigation measures:** Mitigation measures that are reasonable under the circumstances, proportionate to the nature of risks identified and ordinary usage of the service.
- **Terms and conditions and their enforcement:** Defined in DSA Art. 3(u). Enforcement is outlined in each Terms and Conditions: Microsoft Services Agreement and Image Creator from Designer Terms.
- **Speed and quality of processing notices:** Standard time to act and action taken by Bing after Bing has received a report of illegal content.
- **Expeditious removal:** Removed without unreasonable delay.
- **Disabling of access:** Limiting or removing access to a feature or service.
- **Illegal hate speech:** Per Council Framework Decision 2008/913/JHA: All conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin.
- **Cyber violence:** Online forms of violence, such as bullying, stalking or harassment.
- **Algorithmic systems:** Systems that rely on structured set of rules or instructions designed to perform specific tasks or solve problems that provide outputs or results.
- **Targeted measures:** Specific actions or interventions. (Art. 35.1: Mitigation of risks).
- **Limiting or adjusting the presentation of advertisements:** Changing the type of advertisements or how they are shown to users of the service.

Summary of controls, systems, and processes:	Audit procedures:
Annually, prior to submission to the European Commission (EC), the Article 41 Compliance Officer reviews and approves the systemic risk assessment report to inspect that it is conducted in accordance with a suitable methodology, includes the relevant systemic risks, and identifies mitigations that address the risks. As needed, the MAI Compliance Oversight team establishes and tracks implementation of action plans to enhance mitigations as identified during the Systemic Risk Assessment. Monthly, the Bing Trust and Safety team reviews trends in systemic risk on Bing with Digital Safety Unit (DSU), MAI Compliance Oversight team, and Corporate, External, and Legal Affairs (CELA) teams to monitor the effectiveness of mitigations and take action to address issues as appropriate.	1. Inspected the SRA and relevant supporting documents to ascertain that the systemic risks are identified, analyzed, assessed, and mitigated. 2. Inspected the SRA and relevant supporting documents to ascertain that all categories listed in points (a) – (k) in Article 35.1 are mapped to risk mitigation measures for SRA. 3. Inspected the SRA and relevant supporting documents to ascertain that the residual and inherent risk corroborate with a reduction in risk rating before and after mitigation measures, and that all risks are responded to, including the exercise of fundamental rights. 4. Inspected samples of mitigation measures that include categories listed in points (a) – (k) in Article 35.1 to ascertain that they were appropriately designed and executed. 5. Inspected evidence for monitoring the risks identified in the SRA, including trackers of mitigation action plans and implementation activities, to ascertain that mitigations are adequately reviewed and enhanced as identified during the SRA. 6. Inspected meeting invites and minutes where regular updates on enhancing mitigation measures were discussed to ascertain that compliance officers are adequately involved in the risk assessment report and risk mitigation measures.

7. Inspected monthly meeting decks to ascertain that the effectiveness of mitigation measures was monitored and that issues were identified, tracked, and addressed.
8. Inspected guidelines and publications published by the EC, including additional provisions as outlined in Article 14 of the Delegated Regulation.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 35.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 36 DSA - Crisis response mechanism

Obligation:	Audit criteria:	Materiality threshold:
36.1	**Requirement:** Where a crisis occurs, the Commission, acting upon a recommendation of the Board may adopt a decision requiring one or more providers of very large online platforms or of very large online search engines to take one or more of the following actions: a) assess whether, and if so to what extent and how, the functioning and use of their services significantly contribute to a serious threat as referred to in paragraph 2 or are likely to do so. b) identify and apply specific, effective, and proportionate measures, such as any of those provided for in Article 35.1 or Article 48.2, to prevent, eliminate or limit any such contribution to the serious threat identified pursuant to point (a) of this paragraph. c) report to the Commission by a certain date or at regular intervals specified in the decision, on the assessments referred to in point (a), on the precise content, implementation and qualitative and quantitative impact of the specific measures taken pursuant to point (b) and on any other issue related to those assessments or those measures, as specified in the decision. When identifying and applying measures pursuant to point (b) of this paragraph, the service provider or providers shall take due account of the gravity of the serious threat referred to in paragraph 2, of the urgency of the measures and of the actual or potential implications for the rights and legitimate interests of all parties concerned, including the possible failure of the measures to respect the fundamental rights enshrined in the Charter. **Definitions and Benchmarks:** • **Crisis:** Where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it as dictated by the EC. • **Significantly contribute:** Plays a substantial role in amplifying, or sustaining the threat of crisis.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing maintains a documented process to assess whether the functioning and use of their services significantly contribute to a serious threat in the event of a Crisis. Bing maintains a documented process to identify and apply specific measures to prevent, eliminate or limit any such contribution to the serious threat in the event of a Crisis. Bing maintains a documented process to report to the Commission by a certain date or at regular intervals specified in	1. Inspected documented processes, relevant policies, and respective controls to evaluate whether Bing: • Had established and documented processes and a control specifically for crisis management. • Maintained policies and procedures that provided clear and actionable guidance for crisis response. • Implemented guidelines and a control to monitor their effectiveness in supporting an effective crisis management strategy. • Confirmed compliance with specified requirements, identifying and addressing any non-compliance or gaps.

the decision, on the assessments and impact of the specific measures taken and on any other issue related to those assessments or those measures in the event of a Crisis.	2. Inspected the Bing Crisis inbox, inquired with management, and ascertained that Bing received no communications from the EC and that no serious threats or crisis events were declared during the Examination Period. 3. Performed internet searches over publicly available data on EU and EC crisis events and inspected the official webpage of the European Union during the Examination Period to corroborate that no crisis events occurred that would require Bing to act under Article 36. Further, ascertained that the sources used were official and current as of the end of the Examination Period. As a result, no relevant population was available to test this obligation.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 36.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 37 DSA - Independent audit

Obligation:	Audit criteria:	Materiality threshold:
37.1	**Requirement:** Providers of very large online platforms and of very large online search engines shall be subject, at their own expense and at least once a year, to independent audits to assess compliance with the following: a) the obligations set out in Chapter III. b) any commitments undertaken pursuant to the codes of conduct referred to in Articles 45 and 46 and the crisis protocols referred to in Article 48. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
On an annual basis, Bing completes an independent audit, at their own expense, to assess compliance with the obligations set out in Chapter III and the commitments made to codes of conduct and crisis protocols.	1. Inspected Bing's published 2025 DSA Audit Report and the signed Statement of Work (SOW) for the 2025 DSA audit to ascertain that Bing engaged Deloitte & Touche LLP to perform an independent audit assessing compliance with the obligations set out in Chapter III of the DSA, and that the costs associated with the audit are borne by Bing.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 37.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
37.2	**Requirement:** Providers of very large online platforms and of very large online search engines shall afford the organisations carrying out the audits pursuant to this Article the cooperation and assistance necessary to enable them to conduct those audits in an effective, efficient and timely manner, including by giving them access to all relevant data and premises and by answering oral or written questions. They shall refrain from hampering, unduly influencing or undermining the performance of the audit. Such audits shall ensure an adequate level of confidentiality and professional secrecy in respect of the information obtained from the providers of very large online platforms and of very large online search engines and third parties in the context of the audits, including after the termination of the audits. However, complying with that requirement shall not adversely affect the performance of the audits and other provisions of this Regulation, in particular those on transparency, supervision and enforcement. Where necessary for the purpose of the transparency reporting pursuant to Article 42.4, the audit report and the audit implementation report referred to in paragraphs 4 and 6 of this Article shall be accompanied with versions that do not contain any information that could reasonably be considered to be confidential. **Definitions and Benchmarks:** • **Timely manner:** Within agreed upon timeframes.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing has engaged the external auditor to carry out the audits pursuant to this Article and will provide the cooperation and assistance necessary to enable the external auditor to conduct those audits in an effective, efficient, and timely manner. Bing also provides the external auditor with access to relevant data and premises, answers oral or written questions, and refrains from hampering, unduly influencing, or undermining the performance of the audit. The audits help ensure an adequate level of confidentiality and professional secrecy in respect to the information obtained from Bing, including after the audit completes. Where necessary for the purpose of the transparency reporting pursuant to Article 42.4, the audit report referred to in paragraphs 4 and 6 of this Article includes a redacted version that does not contain confidential information, and the Audit	1. Inspected the SOW outlining the level of confidentiality and professional secrecy in respect of the information obtained from Bing, including after the completion of the audit. 2. Ascertained that management provided assistance and cooperation in providing access to relevant data and premises and answering oral or written questions to allow the external auditor to conduct the audit in an effective, efficient, and timely manner. 3. Inspected the public audit report and Audit Implementation Report to assess whether information had been included that could reasonably be considered confidential.

Implementation Report does not have any redactions as no confidential information is included.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 37.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
37.3	**Requirement:** Audits performed pursuant to paragraph 1 shall be performed by organisations which: a) are independent from, and do not have any conflicts of interest with, the provider of very large online platforms or of very large online search engines concerned and any legal person connected to that provider; in particular: i. have not provided non-audit services related to the matters audited to the provider of very large online platform or of very large online search engine concerned and to any legal person connected to that provider in the 12 months' period before the beginning of the audit and have committed to not providing them with such services in the 12 months' period after the completion of the audit; ii. have not provided auditing services pursuant to this Article to the provider of very large online platform or of very large online search engine concerned and any legal person connected to that provider during a period longer than 10 consecutive years; iii. are not performing the audit in return for fees which are contingent on the result of the audit; b) have proven expertise in the area of risk management, technical competence and capabilities; c) have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The external auditor is required to be independent from Bing and free from conflicts of interest. The external auditor is prohibited from providing non-audit services related to matters auditing for time periods outlined in the requirement. The external auditor is required to have expertise in risk management, technical competence and capabilities, and maintain proven objectivity and professional ethics.	1. Inspected the independence provisions included in the 2025 Statement of Work (SOW) and Bing's 2025 DSA Audit Report to ascertain that the external auditor should not provide non-audit services for Bing or any legal person connected to Bing related to the matters audited in the 12-month period before the beginning of the audit, and commitments to not provide such services in the 12-month period after the completion of the audit. Inspected Audit Committee meeting minutes to ascertain that the external auditor maintained independence. 2. Inspected Bing's 2025 DSA Audit Report and the signed Statement of Work (SOW) for the 2025 DSA audit to ascertain the external auditor's tenure as Bing's DSA auditor has not provided auditing services pursuant to Article 37 to Bing and any legal person connected to Bing for a period exceeding 10 consecutive years. 3. Inspected Bing's 2025 DSA Audit Report and the signed Statement of Work (SOW) for the 2025 DSA audit to assess that audit fees were not contingent upon audit results. 4. Inspected Bing's 2025 DSA Audit Report and the signed Statement of Work (SOW) for the 2025 DSA audit to assess the professional qualifications of the audit team members to determine that they possess appropriate expertise in risk management, technical competence, and capabilities to perform the

	engagement. Confirmed that all engagement personnel complied with applicable ethics and independence requirements throughout the audit.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 37.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
37.4	**Requirement:** Providers of very large online platforms and of very large online search engines shall ensure that the organisations that perform the audits establish an audit report for each audit. That report shall be substantiated, in writing, and shall include at least the following: a) the name, address and the point of contact of the provider of the very large online platform or of the very large online search engine subject to the audit and the period covered. b) the name and address of the organisation or organisations performing the audit. c) a declaration of interests. d) a description of the specific elements audited, and the methodology applied. e) a description and a summary of the main findings drawn from the audit. f) a list of the third parties consulted as part of the audit. g) an audit opinion on whether the provider of the very large online platform or of the very large online search engine subject to the audit complied with the obligations and with the commitments referred to in paragraph 1, namely 'positive', 'positive with comments' or 'negative'. h) where the audit opinion is not 'positive', operational recommendations on specific measures to achieve compliance and the recommended timeframe to achieve compliance. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing has engaged the external auditor to perform an independent audit and to prepare a written audit report in accordance with applicable DSA requirements. The written report includes the required elements, including contact information for Bing and the external auditor, declaration of interests, a description of the audit scope and methodologies, summary of findings, information regarding third party consultations, an audit opinion, and where applicable, corresponding operational recommendations identifying specific measures timeframe to achieve compliance.	1. Inspected Bing's 2025 audit report to ascertain whether the audit report was prepared in accordance with stipulated requirements described in Article 37.4(a)-Article 37.4(h) of the DSA. 2. Inspected the audit report to ascertain that it included an audit opinion expressing whether Bing complied with obligations and commitments subject to the audit. 3. For obligations that had a conclusion other than a 'Positive' opinion, ascertained whether the audit report included operational recommendations identifying specific measures to achieve compliance and the recommended timeframe to achieve compliance.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 37.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
37.5	**Requirement:** Where the organisation performing the audit was unable to audit certain specific elements or to express an audit opinion based on its investigations, the audit report shall include an explanation of the circumstances and the reasons why those elements could not be audited. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing engaged the external auditor to perform and conduct the independent audit and to prepare a written audit report in accordance with applicable DSA requirements for the prior year. The external auditor included descriptions of the circumstances and reasons that prevented the external auditor from examining certain elements or expressing an audit opinion based on its investigation.	1. Inquired with management to ascertain whether any circumstances existed in Bing's 2025 audit report that prevented the external auditor from auditing specific elements or expressing an audit opinion. 2. Inspected Bing's 2025 DSA audit report to determine whether any specific elements were identified as not auditable or whether the external auditor was unable to express an audit opinion based on its investigations. 3. Where limitations were identified, inspected the independent audit report and determined that the affected elements, circumstances giving rise to the limitation, and reasons why those elements could not be audited or an audit opinion could not be expressed were appropriately described.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 37.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
37.6	**Requirement:** Providers of very large online platforms or of very large online search engines receiving an audit report that is not 'positive' shall take due account of the operational recommendations addressed to them with a view to take the necessary measures to implement them. They shall, within one month from receiving those recommendations, adopt an audit implementation report setting out those measures. Where they do not implement the operational recommendations, they shall justify in the audit implementation report the reasons for not doing so and set out any alternative measures that they have taken to address any instances of non-compliance identified. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Within one month of receiving an audit report containing an opinion other than 'Positive', Bing has a process to publish an Audit Implementation Report in which they acknowledge any operational recommendations and include details on planned and implemented measures to address the recommendations. Where a recommendation is not implemented, Bing documents the justification and any alternative measure(s) taken to achieve compliance.	1. Inspected the 2025 Audit Implementation Report to ascertain that the report was delivered and submitted timely within one month of receiving the operational recommendations. 2. Inspected Bing's 2025 DSA audit report and the 2025 Audit Implementation Report to ascertain whether for each obligation that had an audit conclusion other than positive in the 2025 DSA audit report, Bing acknowledged the applicable operational recommendations and described the measures planned or implemented to address them. 3. If any operational recommendations were not implemented, ascertained whether Bing's Audit Implementation Report included the rationale for not implementing the recommendation and identified alternative measures to address the underlying instance of non-compliance and support achievement of compliance with the applicable obligation.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 37.6 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 38 DSA - Recommender systems

Obligation:	Audit criteria:	Materiality threshold:
38	**Requirement:** In addition to the requirements set out in Article 27, providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679. **Definitions and Benchmarks:** • **Recommender system:** Fully or partially automated systems to suggest or prioritize in online interface specific information to recipients of the service, excluding advertising systems. Article 38 requires that those recommender systems that are based on profiling provide at least one option for each of their recommender systems which is not based on profiling. Profiling means any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location, or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. Together this means that those recommender systems that use profiling are in scope. • **Profiling:** Per GDPR (General Data Protection Regulation): Any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The Bing Compliance and Privacy teams maintain processes to identify and assess recommender systems and associated profiling across the Bing platform through both event-driven and periodic activities. New or updated features are evaluated through the Critical Impact Risk Assessment (CIRA) process to determine whether they materially impact recommender systems. Where such impact is identified, an assessment is performed to determine whether the feature should be included within the scope of recommender systems under Article 38.	1. Inspected documentation of the CIRA process, including the questionnaire, to ascertain whether evaluation of recommender system impact is captured and documented. 2. Inspected a sample CIRA assessment to ascertain whether consideration of recommender system impact was performed and the outcome was documented. 3. Inspected documentation of the annual review of core and generative features identified within the SRA to ascertain whether each feature was assessed to determine whether they utilize profiling. 4. Examined evidence of management review and approval to ascertain whether the inventory and analysis were reviewed and signed off and segregation of duties was maintained. 5. Selected samples of potential recommender systems and reperformed management's analysis to ascertain whether the features use profiling through observation of feature behavior and compared the results of testing to

On an annual basis, the Bing Compliance and Privacy teams perform a review of all core and generative features on the Bing platform identified within the Systemic Risk Assessment (SRA). Each feature was assessed to determine whether it uses profiling and whether it should be considered a recommender system under Article 38.

The resulting inventory and analysis are documented and tracked, and are subject to management review and approval, with segregation of duties maintained between preparation and approval. This annual review, along with the CIRA process, supports completeness of recommender system identification.

management's analysis to ascertain whether the determination of profiling was consistent.

6. Inspected the results of management's annual review of all core and generative features on the Bing platform identified within the SRA and ascertained it supported the conclusion that there were no relevant recommender systems during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 38 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 39 DSA - Additional online advertising transparency

Obligation:	Audit criteria:	Materiality threshold:
39.1	**Requirement:** Providers of very large online platforms or of very large online search engines that present advertisements on their online interfaces shall compile and make publicly available in a specific section of their online interface, through a searchable and reliable tool that allows multicriteria queries and through application programming interfaces, a repository containing the information referred to in paragraph 2, for the entire period during which they present an advertisement and until one year after the advertisement was presented for the last time on their online interfaces. They shall ensure that the repository does not contain any personal data of the recipients of the service to whom the advertisement was or could have been presented, and shall make reasonable efforts to ensure that the information is accurate and complete. **Definitions and Benchmarks:** • **Publicly available:** Able to be accessed by the general public. • **Searchable:** In the context of the ad repository, data is available to the generable public and is organized in a way that enables users to query and retrieve information based on user input. • **Reliable tool:** Bing used the following as a benchmark for tool reliability under Article 39.1: The service recipient is able to query the Ad Library for ads with 98% availability of that functionality across the examination period, any issues with downtime are resolved within 96 hours. • **Personal data:** Data directly identifying a specific person as defined per GDPR Article 4. • **Accurate and complete:** Including all relevant information without omissions or gaps, where the information is verifiable and reliable.	We have applied a 5% materiality threshold for this obligation.

Summary of controls, systems, and processes:	Audit procedures:
Bing's Ad Library provides access to query and retrieve Ads data that includes: • Advertisement content • Advertiser entity details • Paying entity details • Advertisement presentation period • Impressions number and their percentage distribution by country • Top targeting criteria Bing has automated job runs to pull relevant Ads information from Ads systems into the Ad Library. Monitoring is performed to validate the job is running as expected. Issues are investigated and resolved in a timely manner.	1. Inspected the link to the Ad Library to ascertain that it is publicly available in a specific section of the online interface. 2. Inspected the Ad Library to ascertain that it is publicly available through an application programming interface. 3. Inspected the Ad Library through the online interface to ascertain that the search functionality allows for multicriteria queries. 4. Inspected the Ad Library through the application programming interface to ascertain that it allows for multicriteria queries. 5. Inspected the Ad Library to ascertain that it includes advertisements served across EU Member States and that all countries are appropriately represented. 6. Inspected code configurations to ascertain whether the data transfer from Bing's Ads systems to the Ad Library is complete and accurate. 7. Inspected evidence of management's review of advertisement data transferred to the Ad Library to confirm that the review was in fact performed, and identified discrepancies were investigated and remediated where appropriate.

Annually, a sample of ads is traced from their source to the Ad Library to verify the complete and accurate transfer of Ad data. Any discrepancies found during this process are thoroughly investigated to confirm data integrity of the Ad Library.

Bing conducts an annual review of data elements stored within the Ads library database to ensure that personally identifiable information (PII) is not present. If PII is identified, management promptly removes it and performs an impact assessment.

Bing has an automated job configured to check the last shown date for an ad, to determine the need to continue including the ad and its related information in the Ad Library. The ad and related information is made available to users of the Ad Library User Interface (UI) for 1 year from the last impression date. Monitoring (via alerting) is performed to validate the job is running as expected. Issues are investigated and resolved in a timely manner.

8. For a sample of advertisements served in the EU, inspected and traced the information referred to within paragraph 2 from the source systems to the Ad Library to ascertain whether the information included within the Ad Library is complete and accurate.
9. Inspected configurations in place to ascertain whether the Ad Library retains information for at least one year after the advertisement was presented for the last time.
10. Inspected evidence of monitoring activities over automated jobs supporting the Ad Library. For a sample of job failures, inspected evidence that exceptions were investigated and resolved in a timely manner.
11. Inspected a list of data elements stored within the Ad Library database to ascertain whether personal data of the recipients is not present.
12. For a sample of advertisements served in the EU, inspected the content captured in the Ad Library for the advertisements to ascertain whether personal data of the recipients is not present.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 39.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
39.2	**Requirement:** The repository shall include at least all of the following information: a) the content of the advertisement, including the name of the product, service or brand and the subject matter of the advertisement; b) the natural or legal person on whose behalf the advertisement is presented; c) the natural or legal person who paid for the advertisement, if that person is different from the person referred to in point (b); d) the period during which the advertisement was presented; e) whether the advertisement was intended to be presented specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose including where applicable the main parameters used to exclude one or more of such particular groups; f) the commercial communications published on the very large online platforms and identified pursuant to Article 26.2; g) the total number of recipients of the service reached and, where applicable, aggregate numbers broken down by Member State for the group or groups of recipients that the advertisement specifically targeted. **Note:** The point (f) of the requirement is not relevant to the VLOSE. **Definitions and Benchmarks:** • N/A	We have applied a 5% materiality threshold for this obligation.

Summary of controls, systems, and processes:	Audit procedures:
Bing's Ad Library includes advertisement data elements required under Article 39.2, including: • Advertisement content • Advertiser entity • Paying entity • Advertisement presentation period • Targeting parameters • Impressions data and geographic distribution A monthly impressions validation process is performed, whereby management executes a validation job to compare impressions data between source systems and the Ad Library for a sample of advertisements. Output files detailing results of the comparison are generated and reviewed, and any variances above defined thresholds are investigated to ensure the accuracy and completeness of impressions data reported in the Ad Library	1. Inspected evidence of management's annual review whereby management traces a sample of advertisements served in the E.U from source systems to the Ad Library to ascertain whether the Ad Library included all of the points (a) – (e) and (g) in Article 39.2 completely and accurately. 2. Inspected evidence supporting the investigation of discrepancies identified during management's review to confirm that variances were assessed and resolved. 3. For a sample of advertisements served in the E.U, independently inspected and traced information from source systems to the Ad Library to ascertain whether the Ad Library included all of the points (a) – (e) and (g) in Article 39.2 completely and accurately. 4. For a sample of advertisements served in the EU, inspected information presented in the Ad Library and traced the information to the underlying source systems, to ascertain that the information required was complete and accurate. 5. Inspected evidence of management's monthly validation of impressions data, including output files generated from the validation job and documentation of management's review. 6. Re-performed management's monthly review of impressions data to identify any mismatches and assessed whether variances were appropriately investigated.

An annual sample-based review is performed, whereby management traces a sample of advertisements from source systems to the Ad Library. This review validates that advertisement data elements, including content, advertiser, payor, dates, impressions, and targeting parameters, are transferred completely and accurately. Any discrepancies identified during the review are investigation and remediated. Bing has automated job runs to pull relevant Ads information from Ads systems into Ad Library. Monitoring is performed to validate that the job is running as expected. Issues are investigated and resolved in a timely manner.	7. Inspected system logs evidencing successful completion of data pipeline jobs to ascertain whether the data transfer from Bing's Ads systems to the Ad Library is complete and accurate. 8. Inspected system logs and pipeline monitoring records to identify instances of job failures during the audit period. For a sample of job failures, inspected evidence of alert notifications, incident tickets, and remediation actions to ascertain that failures were investigated and resolved in a timely manner.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 39.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
39.3	**Requirement:** As regards paragraph 2, points (a), (b) and (c), where a provider of very large online platform or of very large online search engine has removed or disabled access to a specific advertisement based on alleged illegality or incompatibility with its terms and conditions, the repository shall not include the information referred to in those points. In such case, the repository shall include, for the specific advertisement concerned, the information referred to in Article 17.3, points (a) to (e), or Article 9.2, point (a)(i), as applicable. **Definitions and Benchmarks:** • **Alleged illegality or incompatibility with its terms and conditions:** Content which has been removed from advertising inventory by either Bing or its ads provider (for reasons of illegal content or other violations of Microsoft Advertising Policies) has had certain fields modified in the Ads Library as required by the DSA. • **Egregious violations:** For Microsoft Advertising, egregious violations are defined as violations that involve illegal content or activity, pose a threat to user safety or security, or degrade or impair the security of the services provided by Microsoft or its partners. These violations indicate an intent to misuse Microsoft Advertising's service in a fraudulent, harmful, or illegal manner.	We have applied a 5% materiality threshold for this obligation.

Summary of controls, systems, and processes:	Audit procedures:
Bing enforces eligibility criteria for ad serving, whereby advertisements must be associated with active campaigns and approved order status prior to being served. Monitoring is performed to identify instances where ads are served outside of the eligibility criteria for ad serving, and any issues identified are investigated and resolved. Automated configurations within the data pipeline enforce the detection and removal of post-serving advertisement containing illegal content or violating Microsoft Advertising policies. Bing performs an annual sample-based review of advertisements removed after serving to validate that: • advertisement content is no longer displayed; • required explanatory information is present; • links to policy references are included and functional.	1. Inspected configurations within the data pipeline to ascertain that logic is in place to detect advertisements containing illegal content or violations of terms and conditions and to remove such content from the Ad Library. 2. Inspected evidence of management's review for a sample of rejected advertisements to ascertain that the review was performed in accordance with the control design, rejected advertisements were appropriately removed from the Ad Library with the required disclosures, and any identified discrepancies were appropriately investigated and remediated. 3. For a sample of illegal advertisements served on Bing's platform in the EU, independently inspected evidence to ascertain: • that the advertisement was removed from the Ad Library and did not contain the following: – The content of the advertisement, including the name of the product, service, or brand and the subject matter of the advertisement. – The natural or legal person on whose behalf the advertisement is presented. – The natural or legal person who paid for the advertisement. • that the Ad Library included a statement of reason detailing the action taken on the information, its scope and duration, the reasons and process behind the decision (including any automated tools used), and, if relevant, the legal or contractual grounds and explanations for considering the content illegal or incompatible.

Issues identified as part of the annual review are investigated and remediated.	4. Evaluated controls over information systems supporting this obligation to understand their design and implementation.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive with Comments – In our opinion, Bing complied with Obligation 39.3 during the Examination Period in all material respects. Although the audited obligation has been met, we noted the following:

a) The explanation as to why the advertisement was considered illegal content or incompatible with Microsoft's terms and conditions was available to users; however, user-friendly links to easily view the specific portion of the relevant policy(ies) were not available from 6/1/2025-7/22/2025.

b) This functionality was enhanced on 7/23/2025, was applied retroactively across the advertisements in the Ad Library UI, and was in place for the remainder of the Examination Period.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable – Bing remediated this issue during the Examination Period	Not applicable

Article 40 DSA - Data access and scrutiny

Obligation:	Audit criteria:	Materiality threshold:
40.1	**Requirement:** Providers of very large online platforms or of very large online search engines shall provide the Digital Services Coordinator of establishment or the Commission, at their reasoned request and within a reasonable period specified in that request, access to data that are necessary to monitor and assess compliance with this Regulation. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains the "Bing Qualified Researcher Program" portal, where the Digital Services Coordinator (DSC) of establishment can submit data access requests to Bing. Bing reviews these requests and responds within 15 business days with a decision. Once management determines a decision, access will be granted or denied based on the decision.	1. Inspected Bing's research resources webpage to ascertain whether Bing has a mechanism in place for the DSC to request access to the data, and that Bing reviews and responds to access requests within a reasonable period. 2. Inspected the list of data access requests and ascertained there were no requests from the DSC made during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 40.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
40.3	**Requirement:** For the purposes of paragraph 1, providers of very large online platforms or of very large online search engines shall, at the request of either the Digital Service Coordinator of establishment or of the Commission, explain the design, the logic, the functioning, and the testing of their algorithmic systems, including their recommender systems. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains the "Bing Qualified Researcher Program" portal, where the DSC can submit information and data access requests to Bing. Bing reviews these requests and responds within 15 business days with a decision. Once management determines a decision, access will be granted or denied based on the decision.	1. Inspected Bing's research resources webpage to ascertain whether Bing has a mechanism in place for the DSC to request information and data, and that Bing reviews and responds to access requests within a reasonable period. 2. Inspected the list of data access requests and ascertained there were no requests from the DSC made during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 40.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
40.4	**Requirement:** Upon a reasoned request from the Digital Services Coordinator of establishment, providers of very large online platforms or of very large online search engines shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraph 8 of this Article, for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out pursuant to Article 34.1, and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35. **Definitions and Benchmarks:** • **Adequacy, efficiency and impacts:** Whether access to data provided to vetted researchers enables the assessment of the design and effectiveness of risk mitigation measures implemented pursuant to Article 35, based on management's assessment of the request.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains the "Bing Qualified Researcher Program" portal, where the DSC can submit information and data access requests to Bing for vetted researchers. Bing reviews these requests and responds within 15 business days with a decision. Once management determines a decision, access will be granted or denied based on the decision.	1. Inspected Bing's research resources webpage to ascertain whether Bing has a mechanism in place for the DSC to request access to the data, and that Bing reviews and responds to access requests within a reasonable period. 2. Inspected the list of data access requests from DSC and ascertained there were no requests from the DSC made during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 40.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
40.5	**Requirement:** Within 15 days following receipt of a request as referred to in paragraph 4, providers of very large online platforms or of very large online search engines may request the Digital Services Coordinator of establishment, to amend the request, where they consider that they are unable to give access to the data requested because one of following two reasons: a) they do not have access to the data; b) giving access to the data will lead to significant vulnerabilities in the security of their service or the protection of confidential information, in particular trade secrets. **Definitions and Benchmarks:** • **Significant vulnerabilities:** Substantial risks arising from the provision of the requested data that could compromise the security, integrity, or resilience of the service, or the protection of confidential information, and that cannot be sufficiently mitigated through the conditions of access requested.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft has established a process to review data access requests within a defined timeframe and determine whether the requested data is available and accessible. If Microsoft does not possess or cannot provide access to the requested data, procedures are in place to formally request the Digital Services Coordinator to amend a data access request within 15 days of receipt if providing the requested data would result in significant security risks to its services.	1. Inspected the list of data access requests from DSC and ascertained there were no requests from the DSC made during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 40.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
40.6	**Requirement:** Requests for amendment pursuant to paragraph 5 shall contain proposals for one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request. The Digital Services Coordinator of establishment shall decide on the request for amendment within 15 days and communicate to the provider of the very large online platform or of the very large online search engine its decision and, where relevant, the amended request and the new period to comply with the request. **Definitions and Benchmarks:** • **Appropriate and sufficient:** Alternative data or access modalities that are capable of supporting research purposes under Article 40 without introducing significant vulnerabilities, as defined in Article 40.5.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft has established a process whereby when amendments are needed, alternative data or access methods may be proposed, and the Digital Services Coordinator reviews the request and communicates the decision, any amended request, and updated timelines.	1. Inspected the list of data access requests from DSC and ascertained there were no requests from the DSC made during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 40.6 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
40.7	**Requirement:** Providers of very large online platforms or of very large online search engines shall facilitate and provide access to data pursuant to paragraphs 1 and 4 through appropriate interfaces specified in the request, including online databases or application programming interfaces. **Definitions and Benchmarks:** • **Appropriate interfaces:** In a commonly used and machine-readable format.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft has a mechanism in place to provide access to approved data through appropriate interfaces.	1. Inspected the list of data access requests from DSC and ascertained there were no requests from the DSC made during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 40.7 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
40.12	**Requirement:** Providers of very large online platforms or of very large online search engines shall give access without undue delay to data, including, where technically possible, to real-time data, provided that the data is publicly accessible in their online interface by researchers, including those affiliated to not for profit bodies, organisations and associations, who comply with the conditions set out in paragraph 8, points (b), (c), (d) and (e), and who use the data solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union pursuant to Article 34.1. **Definitions and Benchmarks:** • **Undue delay:** Bing used 15 days as a benchmark for providing data access in response to researcher requests.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains open source and self-service research tools that provide access to researchers to publicly accessible data. Microsoft maintains the "Bing Qualified Researcher Program" portal, where researchers can submit information and data access requests to Bing. Bing reviews these requests and responds within 15 business days with a decision. Once management determines a decision, access will be granted or denied based on the decision.	1. Observed and inspected the Bing research resources webpage to ascertain whether Bing provides access to public data without undue delay to researchers. 2. Inspected Bing's research resources webpage where researchers can submit data access requests to ascertain whether Bing has a mechanism in place for researchers to request access to data, and that Bing reviews access requests and approves/denies access according to the conditions defined in Article 40.12. 3. Obtained a list of the DSA researcher access requests made during the Examination Period. For a sample of requests, obtained and inspected evidence to ascertain whether the following attributes were considered by management to grant/deny access, according to the conditions defined in Article 40.12: a. The application is reviewed. b. Management vets the applications to check that applicants would use the data solely for performing research that contributes to the detection, identification, and understanding of systemic risks in the Union. c. The response is sent to the applicant within 15 days with a decision. Additionally, where access to real-time data was required, such access was provisioned only to applicants upon successful approval, in line with the established process.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 40.12 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 41 DSA - Compliance function

Obligation:	Audit criteria:	Materiality threshold:
41.1	**Requirement:** Providers of very large online platforms or of very large online search engines shall establish a Compliance Function, which is independent from their operational functions and composed of one or more compliance officers, including the head of the Compliance Function. That Compliance Function shall have sufficient authority, stature and resources, as well as access to the management body of the provider of the very large online platform or of the very large online search engine to monitor the compliance of that provider with this Regulation. **Definitions and Benchmarks:** • **Independent:** Bing used organizational reporting lines as a benchmark for determining the compliance function's independence from the operation of the Bing service. For these purposes, Bing considers teams or individuals who report to different corporate VP's/GM's to be independent of each other.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The DSA Board Committee ("Management Body") is responsible for the establishment of the Compliance Function, which is independent from the operational functions of Microsoft Ireland Operations Limited, to operationalize measures and monitor compliance with the DSA. The DSA Board Committee Charter sets out the key responsibilities of the DSA Compliance Function. The Head of DSA Compliance Function reports directly to the management body for the purposes of leading the DSA Compliance Function and DSA implementation risk. Annually, the DSA Board Committee of Microsoft Ireland Operations Limited reviews and updates as needed the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter and governance arrangements of the Digital Services Act Compliance Function.	1. Inspected the organizational structure, including the reporting lines of the DSA Compliance Function and the operational functions, to ascertain whether the DSA Compliance Function is independent of the operational functions, and has access to the management body. 2. Conducted inquiries with management to determine whether any changes were made to the Charter during the period under review and, where applicable, inspected supporting documentation to confirm alignment with prior year (PY) documentation. 3. Inspected the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter, to determine whether the DSA Compliance Function is formally established, operates independently of operational functions, and is responsible for monitoring compliance with the DSA, including having appropriate access to the management body. 4. Inspected the DSA Board Committee meeting minutes to ascertain that there were no changes to the compliance function. The governance structure and responsible roles remain unchanged from the prior period. 5. Inspected the DSA Board Committee meeting minutes to ascertain that the DSA Board Committee Charter and the changes in the DSA Compliance Function governance structure were documented and reviewed by the DSA Board Committee on an annual basis.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 41.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
41.2	**Requirement:** The management body of the provider of the very large online platform or of the very large online search engine shall ensure that compliance officers have the professional qualifications, knowledge, experience and ability necessary to fulfil the tasks referred to in paragraph 3. The management body of the provider of the very large online platform or of the very large online search engine shall ensure that the head of the compliance function is an independent senior manager with distinct responsibility for the compliance function. The head of the compliance function shall report directly to the management body of the provider of the very large online platform or of the very large online search engine, and may raise concerns and warn that body where risks referred to in Article 34 or non-compliance with this Regulation affect or may affect the provider of the very large online platform or of the very large online search engine concerned, without prejudice to the responsibilities of the management body in its supervisory and managerial functions. The head of the compliance function shall not be removed without prior approval of the management body of the provider of the very large online platform or of the very large online search engine. **Definitions and Benchmarks:** • **Independent:** Bing used organizational reporting lines as a benchmark for determining the compliance function's independence from the operation of the Bing service. For these purposes, Bing considers teams or individuals who report to different corporate VP's/GM's to be independent of each other.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The DSA Board Committee is responsible for the establishment of the Compliance Function and the appointment of the Head of Compliance, who has distinct responsibility for the Compliance Function, and reports directly to the Committee. Prior to the appointment of each compliance officer, the DSA Board Committee evaluates the professional qualifications, knowledge, and experience of each compliance officer within the Compliance Function necessary to fulfil the tasks referred to in paragraph 3 of Article 41.2. The DSA Board Committee Charter sets out the key responsibilities of the DSA Compliance Function. The DSA Board Committee Charter sets out the roles and responsibilities of the DSA Board	1. Inspected the organizational structure, including the reporting lines of the DSA Compliance Function and the operational functions, to ascertain whether the Head of the DSA Compliance Function holds a senior leadership position, with sufficient authority to effectively oversee and enforce DSA compliance. 2. Inspected the DSA Board Committee meeting minutes to ascertain that there were no changes to the compliance function. The governance structure and responsible roles remain unchanged from the prior period. 3. Inspected governance documentation to confirm that the process for evaluating compliance officers' professional qualifications, knowledge, experience, and ability necessary to fulfil the tasks prior to appointment remain unchanged from the prior year. 4. Conducted inquiry with management to determine whether any changes were made to the Charter during the period under review and, where applicable, inspected supporting documentation to confirm alignment with prior year (PY) documentation. 5. Inspected the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter to show that the Head of Compliance reports directly to the DSA Board Committee, has distinct responsibility for the Compliance Function,

Committee and prohibits the removal of the Head of Compliance without the prior approval of DSA Board Committee. Annually, the DSA Board Committee of Microsoft Ireland Operations Limited reviews and updates as needed the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter and governance arrangements of the Digital Services Act Compliance Function.	and cannot be removed without the prior approval of the DSA Board Committee. 6. Inspected the meeting invitations, attendee lists, and minutes of Bing DSA compliance monthly meetings to ascertain the regular occurrence of monthly compliance meetings, including agenda topics so that risks referred to in Article 34 are identified and reported on, and that the compliance officers are monitoring the compliance of Bing with its commitments. 7. Inspected the DSA Board Committee meeting minutes to ascertain that the DSA Board Committee Charter and the changes in the DSA Compliance Function governance structure were documented and reviewed by the DSA Board Committee on an annual basis.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 41.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
41.3	**Requirement:** Compliance officers shall have the following tasks: a) cooperating with the Digital Services Coordinator of establishment and the Commission for the purpose of this Regulation; b) ensuring that all risks referred to in Article 34 are identified and properly reported on and that reasonable, proportionate and effective risk-mitigation measures are taken pursuant to Article 35; c) organising and supervising the activities of the provider of the very large online platform or of the very large online search engine relating to the independent audit pursuant to Article 37; d) informing and advising the management and employees of the provider of the very large online platform or of the very large online search engine about relevant obligations under this Regulation; e) monitoring the compliance of the provider of the very large online platform or of the very large online search engine with its obligations under this Regulation; f) where applicable, monitoring the compliance of the provider of the very large online platform or of the very large online search engine with commitments made under the codes of conduct pursuant to Articles 45 and 46 or the crisis protocols pursuant to Article 48. **Note:** The point (f) of the requirement is not relevant to the VLOSE. **Definitions and Benchmarks:** • **Properly reported:** Bing considers that the words "properly reported on" in DSA Article 41.3.b reference the risk assessment process (including the methodology employed, recording findings, preparation of the report, and supporting documentation). • **Reasonable, proportionate, and effective risk-mitigation measures:** Mitigation measures appropriate for the systemic risks identified pursuant to DSA Article 34 are tailored to the severity and likelihood of the identified risks and reasonably support in minimizing or mitigating such risks.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The Compliance Function mission letter sets out the key responsibilities of the Compliance Function, including: • Cooperating with the Digital Services Coordinator (DSC) of establishment and the Commission in relation to Bing's compliance with DSA, including by reporting on the measures that Bing has implemented to comply with applicable obligations in the DSA. • Ensuring that risks referred to in Article 34 are identified and reported,	1. Inspected the annual review of the Bing EU DSA information webpage by the MAI Compliance team to ascertain whether the contact information of the Single Point of Contact for Member States' authorities, the Commission, and the Board is published on the webpage for cooperation with the DSC of establishment and the Commission for the purpose of this Regulation. 2. Inspected the meeting invitations, attendee lists, and minutes of Bing DSA compliance monthly meetings to confirm the regular occurrence of monthly compliance meetings, including agenda topics so that risks referred to in Article 34 are identified and reported on; that reasonable, proportionate, and effective risk-mitigation measures are taken pursuant to Article 35; that the compliance officers are supervising the activities of Bing in relation to the independent audit

and that reasonable, proportionate, and effective risk-mitigation measures are taken pursuant to Article 35.
- Organizing and supervising the activities of Bing relating to the independent audit pursuant to Article 37.
- Informing and advising management and employees of Bing about relevant obligations under the DSA.
- Monitoring the compliance of Bing with its obligations under the DSA.
- Where applicable, monitoring the compliance of Bing with commitments made under the codes of conduct pursuant to Articles 45 and 46 or the crisis protocols pursuant to Article 48.

pursuant to Article 37, and monitoring the compliance of Bing with its obligations.

3. Inspected the list of required attendees for the Bing DSA compliance training and corresponding training materials, to ascertain whether the Compliance Functions involved in the process have been actively monitoring the training progress, the correct parties attended the trainings, and the training contents included relevant information pursuant to this article. Further, for individuals who did not attend or attest to completion of the training, inspected alternative mechanisms (e.g., workflow embedded guidance, standard operating procedures, role based instructions) to assess whether ongoing informing and advising of relevant DSA obligations is provided while performing their roles and responsibilities.
4. Inspected the project timelines and email approvals for the SRA report sent to the EC to evaluate how the compliance officers performed their tasks with respect to Article 41.3.b through 41.3.e and, where applicable, 41.3.f.
5. Inspected email communications from the compliance officers to the DSC of establishment and to the EC to ascertain that the DSA Compliance Function cooperated with the DSC and the Commission for the purpose of this Regulation.
6. Inspected the annual review of strategies and policies for managing, monitoring, and maintaining risks identified in the DSA to ascertain that the compliance officers are monitoring Bing's compliance with its obligations under this Regulation and, where applicable, are monitoring the Bing's compliance with commitments made under the codes of conduct pursuant to Articles 45 and 46 or the crisis protocols pursuant to Article 48.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 41.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
41.4	**Requirement:** Providers of very large online platforms or of very large online search engines shall communicate the name and contact details of the head of the compliance function to the Digital Services Coordinator of establishment and to the Commission. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Changes to the Head of the DSA Compliance Function are approved by the DSA Board Committee in a written resolution prior to the position being effective and are communicated to the Digital Services Coordinator (DSC) of establishment and to the Commission.	1. Conducted inquiry with management to determine whether any changes were made to the Charter during the period under review and, where applicable, inspected supporting documentation to confirm alignment with prior year (PY) documentation. 2. Inspected the Digital Services Act Board Committee Charter to ascertain whether the process of communicating the name and contact details of the Head of Compliance to the DSC of establishment and to the Commission is in place. 3. Inspected the DSA Board Committee meeting minutes to ascertain that there were no changes to the compliance function. The governance structure and responsible roles remain unchanged from the prior period. 4. Inspected email communication from the Head of DSA Compliance Function, sent at the start of the DSA Examination Period, to the DSC of establishment and to the European Commission to ascertain that Microsoft Bing engaged with the DSC and the Commission in accordance with the requirements of the Regulation.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 41.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
41.5	**Requirement:** The management body of the provider of the very large online platform or of the very large online search engine shall define, oversee and be accountable for the implementation of the provider's governance arrangements that ensure the independence of the compliance function, including the division of responsibilities within the organisation of the provider of very large online platform or of very large online search engine, the prevention of conflicts of interest, and sound management of systemic risks identified pursuant to Article 34. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The DSA Board Committee Charter sets out the roles and responsibilities of the DSA Board Committee, which include defining, overseeing, and being accountable for the implementation of Bing's governance arrangements, to instill the independence of the Compliance Function, including the division of responsibilities within the organization, the prevention of conflicts of interest, and the sound management of systemic risks. Prior to the appointment of each compliance officer, the DSA Board Committee evaluates the professional qualifications, knowledge, and experience of each compliance officer within the Compliance Function necessary to fulfil the tasks referred to in paragraph 3 of Article 41.2. Any potential conflicts of interest are considered as part of this evaluation and resolved prior to the appointment of a compliance officer. Annually, the DSA Board Committee of Microsoft Ireland Operations Limited reviews, updates as needed the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter and governance arrangements of the Digital Services Act Compliance Function.	1. Conducted inquiry with management to determine whether any changes were made to the Charter during the period under review and, where applicable, inspected supporting documentation to confirm alignment with prior year (PY) documentation. Inspected the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter to ascertain that the roles and responsibilities of the DSA Board Committee include defining, overseeing, and being accountable for the implementation of Bing's governance arrangements, instilling the independence of the Compliance Function, including the division of responsibilities within the organization, the prevention of conflicts of interest, and sound management of systemic risks. 2. Inspected the DSA Board Committee meeting minutes to ascertain that the DSA Board Committee Charter and the governance structure of the DSA Compliance Function were documented and reviewed by the DSA Board Committee on an annual basis. Ascertained that no amendments were required to the Company's DSA governance structure as it remains fit for purpose and effective in achieving the objectives of the Committee. 3. Inspected the organizational structure, including the reporting lines of the DSA Compliance Function and the operational functions, to ascertain whether the DSA Compliance Function is independent of the operational functions. 4. Inspected communication evidence to verify that the Systemic Risk Assessment (SRA) report, which includes systemic risks identified pursuant to DSA Article 34.1, was properly inspected, reviewed, commented upon, and approved by the Bing DSA Board Committee and Head of Compliance prior to submission to the European Commission as part of the overall review and approval process.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 41.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
41.6	**Requirement:** The management body shall approve and review periodically, at least once a year, the strategies and policies for taking up, managing, monitoring and mitigating the risks identified pursuant to Article 34 to which the very large online platform or the very large online search engine is or might be exposed to. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The DSA Board Committee Charter sets out the roles and responsibilities of the DSA Board Committee, which include approving and reviewing periodically, at least annually, the strategies and policies taking up, managing, monitoring, and mitigating the risks identified pursuant to Article 34 to which the Company is or might be exposed to. The DSA Board Committee reviews and approves the Systemic Risk Assessment (SRA) report, which identifies risks pursuant to Article 34, prior to its delivery to the EC. As part of the review, the DSA Board Committee uses the identified risks to inform the strategies and policies for taking up, managing, monitoring, and mitigating those risks. Annually, the DSA Board Committee of Microsoft Ireland Operations Limited reviews, updates as the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter and governance arrangements of the Digital Services Act Compliance Function.	1. Conducted inquiry with management to determine whether any changes were made to the Charter during the period under review and, where applicable, inspected supporting documentation to confirm alignment with prior year (PY) documentation. Inspected the Microsoft Ireland Operations Limited Digital Services Act Board Committee Charter to ascertain whether the roles and responsibilities of the DSA Board Committee include approving and reviewing, at least annually, the strategies and policies taking up, managing, monitoring, and mitigating the risks identified pursuant to Article 34 to which the Company is or might be exposed to. 2. Inspected the DSA Board Committee meeting minutes to ascertain whether a detailed assessment of the Company's DSA governance structure had been undertaken, including reviewing the strategies and policies for taking up, managing, monitoring and mitigating the risks identified pursuant to Article 34 of the DSA to which the Company is or might be exposed to. 3. Inspected the review and approval of the Bing SRA report by a member of the DSA Board Committee.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 41.6 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
41.7	**Requirement:** The management body shall devote sufficient time to the consideration of the measures related to risk management. It shall be actively involved in the decisions related to risk management, and shall ensure that adequate resources are allocated to the management of the risks identified in accordance with Article 34. **Definitions and Benchmarks:** • **Sufficient time:** Microsoft Ireland Operations Limited (service provider of Bing) established a benchmark of at least one annual Committee meeting, together with the fact that the Head of Compliance (HoC) presents at these meetings and has direct access to speak with the Committee and the MIOL Board of Directors as the HoC may deem necessary. • **Adequate resources:** The Bing Compliance Function included one or more full-time employees and a number of third parties (vendor organizations) with specific subject matter expertise who were engaged to augment the capabilities of the FTEs. This resourcing was reviewed with Bing's DSA management body (the MIOL DSA Board Committee).	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The DSA Board Committee Charter sets out the roles and responsibilities of the DSA Board Committee, which include devoting sufficient time to the consideration of the measures related to risk management, being actively involved in the decisions related to risk management and ensuring that adequate resources are allocated to the management of the risks identified in accordance with Article 34 of the DSA. Annually, the DSA Board Committee of Microsoft Ireland Operations Limited (MIOL) reviews, updates as needed the Microsoft Ireland Operations Limited (MIOL)Digital Services Act Board Committee Charter and governance arrangements of the Digital Services Act Compliance Function.	1. Conducted inquiry with management to determine whether any changes were made to the Charter during the period under review and, where applicable, inspected supporting documentation to confirm alignment with prior year (PY) documentation. Inspected the Microsoft Ireland Operations Limited (MIOL) Digital Services Act Board Committee Charter to ascertain that the roles and responsibilities of the DSA Board Committee include approving and reviewing, at least annually, the strategies and policies taking up, managing, monitoring, and mitigating the risks identified pursuant to Article 34 to which the Company is or might be exposed to. 2. Inspected the DSA Board Committee meeting minutes and Bing's SRA report to ascertain that the review and approval of the Bing SRA report was completed by members of the DSA Board Committee. 3. Inspected the organizational structure to ascertain whether the management body had devoted adequate resources to the management of the risks identified in accordance with Article 34. 4. Inspected email communications from the DSA Committee members and DSA Board Committee meeting minutes to evidence management body's annual documentation and review of the governance arrangements of the Compliance Function, demonstrating the management body is actively involved in the decisions related to risk management and that adequate resources are allocated to the management of the risks identified in accordance with Article 34. 5. Inspected the meeting invitations, attendee lists, and minutes of Bing DSA compliance monthly meetings to confirm the regular occurrence of monthly compliance meetings, including agenda topics so that risks referred to in Article 34 are identified and reported on; that reasonable, proportionate, and effective risk-mitigation measures are taken pursuant to Article 35; that the compliance

	officers are supervising the activities of Bing in relation to the independent audit pursuant to Article 37, and monitoring the compliance of Bing with its obligations.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 41.7 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Article 42 DSA - Transparency reporting obligations

Obligation:	Audit criteria:	Materiality threshold:
42.1	**Requirement:** Providers of very large online platforms or of very large online search engines shall publish the reports referred to in Article 15 at the latest by two months from the date of application referred to in Article 33.6, second subparagraph, and thereafter at least every six months. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Before Bing's DSA Transparency Report is released to the public on a semi-annual basis, it undergoes multiple levels of review by appropriate personnel, including both the core working group and leadership group to determine that the details outlined in Article 15.1.a – 15.1.e are represented appropriately. The approved report is published on a public site.	1. Inspected the Transparency Reports issued during the Examination Period to ascertain whether they were published on a semi-annual basis, within the required timelines, and contained the relevant and necessary information under Article 15. 2. Inspected the leadership approval documentation and sign-offs for both Transparency Reports to ascertain whether approval was obtained prior to report publication on the Bing site.

Changes to audit procedures during the examination:

Shifted from controls and substantive testing to substantive testing only.

Conclusion:

Positive – In our opinion, Bing complied with Obligation 42.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
42.3	**Requirement:** In addition to the information referred to in Articles 24.2, the providers of very large online platforms or of very large online search engines shall include in the reports referred to in paragraph 1 of this Article the information on the average monthly recipients of the service for each Member State. **Definitions and Benchmarks:** • N/A	We have applied a 5% materiality threshold for this obligation.

Summary of controls, systems, and processes:	Audit procedures:
Semi-annually, management reviews and approves the DSA Transparency Report to ascertain it specifies the monthly active recipients of the service in the Union, calculated as an average over the preceding six-month period and in accordance with the methodology laid down in the delegated acts referred to in Article 33.3, where such delegated acts have been adopted. Once approved, management makes the report publicly available. Prior to the issuance of the DSA Transparency Report, management reviews and approves the logic and code used for the calculation of monthly active recipients of the service included in the Transparency Report.	1. Inspected the query criteria executed by Bing teams for calculating the number of Monthly Active Users (MAUs) categorized, as required in the Digital Services Act (DSA) for the August 2025 and February 2026 Transparency Reports, to ascertain whether the criteria to extract MAU data has been baselined, approved, and tested by management. 2. Inspected the review and approval performed by the core working group to ascertain whether management's review confirmed the reports were publicly accessible and were published semi-annually, complying with transparency standards. Further, inspected the review and sign-off logs to ascertain whether all relevant leadership teams had approved their sections of the report and required reviews, including the review of code and logic used for the calculation of monthly active recipients of the service, were completed prior to publication on the website. 3. Inspected data flow diagrams and configurations to understand the data transfer process involved in the calculation of MAUs. Further, traced a sample of users from the source system through the intermediary databases to the final system; queried and recalculated the number of MAUs reported on the Transparency Reports for August 2025 and February 2026 to ascertain whether the numbers agree to the MAUs reported, and to confirm the reports' accuracy and completeness.

Changes to audit procedures during the examination:

Shifted from controls and substantive testing to substantive testing only.

Conclusion:

Positive – In our opinion, Bing complied with Obligation 42.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
42.4	**Requirement:** Providers of very large online platforms or of very large online search engines shall transmit to the Digital Services Coordinator of establishment and the Commission, without undue delay upon completion, and make publicly available at the latest three months after the receipt of each audit report pursuant to Article 37.4: a) a report setting out the results of the risk assessment pursuant to Article 34; b) the specific mitigation measures put in place pursuant to Article 35.1; c) the audit report provided for in Article 37.4; d) the audit implementation report provided for in Article 37.6; e) where applicable, information about the consultations conducted by the provider in support of the risk assessments and design of the risk mitigation measures. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Within three months of receipt of the DSA Audit Report, Bing's DSA compliance function makes publicly available the Systemic Risk Assessment (SRA) report, the DSA Audit Report, and the Audit Implementation Report. Bing transmits the reports to the Digital Services Coordinator (DSC) and the European Commission (EC) within 1 month after receipt of the DSA Audit Report. Bing also provides information about any consultations conducted in support of the risk assessments, where applicable.	1. Inspected evidence to ascertain whether Bing transmits the Systemic Risk Assessment report, the DSA Audit Report, and the Audit Implementation Report, including information on consultations conducted, to the DSC and the EC without undue delay. 2. Inspected evidence to ascertain that within three months of receipt of the DSA Audit Report, Bing made the following reports publicly available: the Systemic Risk Assessment report, the DSA Audit Report, and the Audit Implementation Report, including information on consultations conducted where applicable.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 42.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Obligation:	Audit criteria:	Materiality threshold:
42.5	**Requirement:** Where a provider of very large online platform or of very large online search engine considers that the publication of information pursuant to paragraph 4 might result in the disclosure of confidential information of that provider or of the recipients of the service, cause significant vulnerabilities for the security of its service, undermine public security or harm recipients, the provider may remove such information from the publicly available reports. In that case, the provider shall transmit the complete reports to the Digital Services Coordinator of establishment and the Commission, accompanied by a statement of the reasons for removing the information from the publicly available reports. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing removes confidential information in the DSA Audit Report related to fees and payment terms to the independent auditor, and certain names and contact information for privacy purposes. Along with the redacted versions of the report, Bing transmits a statement of reasons to the Digital Services Coordinator (DSC) and the European Commission (EC), explaining what information was redacted and the reasons for these redactions. Bing does not redact information from the publicly available Systemic Risk Assessment (SRA) report or the Audit Implementation Report, as there is no confidential information.	1. Inspected evidence to ascertain whether Bing transmitted to the DSC and the Commission the relevant reports referenced in Article 42.4, along with a statement of reasons (as applicable) for any information redacted from the DSA Audit Report, the Audit Implementation Report, and the System Risk Assessment (SRA) Report, along with the complete reports. 2. Inspected the publicly available reports where redactions were made to ascertain whether Bing transmitted all redactions, along with a statement of reasons in line with the circumstances permitted by Article 24.5, to the DSC and the Commission. 3. Inspected the publicly available reports and Bing's transmittal of reports to the DSC and the EC to ascertain whether the statement of reasons aligned with the redactions within the report and to evaluate whether the reports had any redacted information, without a statement of reasons.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Obligation 42.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Section 6: Other provisions concerning due diligence obligations

The Commission, not the audited service, is responsible for obligations in this section. Therefore, Articles 44, 45, 46, 47, and 48 do not apply to Bing.

Appendix 1B – Code of Conduct on Disinformation (COCD)

The specific test procedures we performed, along with the nature, timing, and results of those tests.

Summary of Audit Conclusions at the Commitment and Measure Level

The table below summarizes audit conclusions for in-scope commitments and measures.

Note: Bing has not subscribed to certain commitments and measures. For additional information regarding Bing's subscriptions, please refer to Bing's report available in the Transparency Center (https://disinfocode.eu/).

Sections[1]					
4. Integrity of Services	5. Empowering Users	6. Empowering the Research Community	8. Transparency Centre	9. Permanent Task-force	10. Monitoring of the Code
Measure 16.1	Measure 18.2	Measure 26.1	Measure 34.1	Measure 37.1	Commitment 38
	Measure 19.1	Measure 26.3	Measure 34.2	Measure 37.2	Measure 40.1
	Measure 19.2	Measure 28.2	Measure 34.3	Measure 37.4	Measure 40.3
	Measure 20.2	Measure 28.3	Measure 34.4	Measure 37.5	Measure 40.4
	Measure 22.2		Measure 34.5	Measure 37.6	Measure 40.5
	Measure 22.3		Measure 35.1		Measure 40.6
	Measure 22.7		Measure 35.2		Commitment 42
			Measure 35.3		Commitment 43
			Measure 35.4		

Legend

- Positive – Compliant
- Positive with Comments – Compliant
- Negative – Partial Compliance and Remediated
- Negative – Partial Compliance
- Negative – Noncompliant
- Disclaimer of Opinion

[1] Sections 1, 2, 3, and 7 are intentionally omitted to align with the structure of the Code of Conduct on Disinformation.

Section 1: Preamble

Section 1 (Preamble) provides introductory context, guiding principles, and background information regarding the objectives and intent of the Code of Conduct on Disinformation. The section does not establish specific commitments, measures, reporting requirements, or other assessable obligations for Signatories and, therefore, does not contain criteria subject to testing.

Section 2: Scrutiny of ad placements

Bing has not elected to subscribe in the commitments associated with Section 2, *Scrutiny of Ad Placements*. Accordingly, these commitments were excluded from the scope of testing. For additional information regarding Bing's subscriptions, please refer to Bing's report available in the Transparency Center (https://disinfocode.eu/).

Section 3: Political advertising

Bing has not elected to subscribe in the commitments associated with Section 3, *Political Advertising*. Accordingly, these commitments were excluded from the scope of testing. For additional information regarding Bing's subscriptions, please refer to Bing's report available in the Transparency Center (https://disinfocode.eu/).

Section 4: Integrity of services

Commitment 16 COCD - Cooperation and transparency

Measure:	Audit criteria:	Materiality threshold:
16.1	**Requirement:** Relevant Signatories will share relevant information about cross-platform information manipulation, foreign interference in information space and incidents that emerge on their respective services for instance via a dedicated sub-group of the permanent Task-force or via existing fora for exchanging such information. **QRE 16.1.1:** Relevant Signatories will disclose the fora they use for information sharing as well as information about learnings derived from this sharing. **SLI 16.1.1:** Relevant Signatories will report on the number of actions taken as a result of the collaboration and information sharing between Signatories. Where they have such information, they will specify which Member States that were affected (including information about the content being detected and acted upon due to this collaboration). **Definitions and Benchmarks:** • **Actions taken:** Actions applied to content, users, or services as a result of collaboration and information-sharing activities; as a search engine, Bing does not host content; therefore, such actions are not applicable to Bing.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains multiple mechanisms to detect, assess, and respond to influence operations, misinformation, and disinformation risks within Bing Search. In addition, Bing collaborates with internal teams and external organizations, including fact-checking organizations, research institutions, and threat intelligence teams, to obtain information relevant to identifying potential information operations. Microsoft also participates in information-sharing initiatives and uses insights received from trusted partners to support monitoring efforts and inform defensive measures designed to protect the integrity of search results.	1. Inspected publicly available disclosures including the "How Bing Delivers Search Results" and "Bing Webmaster Guidelines" webpages and additional documentation to ascertain whether Bing disclosed the fora used for such information sharing. 2. Inspected the Rapid Response System (RRS) process, and related coordination mechanisms and observed that Microsoft Bing has established defined notification, escalation, and communication channels to support information sharing and coordination concerning election-related and cross-platform disinformation incidents. Observed that the process is monitored through established reporting and stakeholder communication channels and observed that, during the period reviewed, no actual election-related or cross-platform disinformation notifications, reports, or information-sharing requests were received through the RRS process.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 16.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Section 5: Empowering users

Commitment 18 COCD - 'Safe design' of the architecture of the services, transparent policies, and accountability of recommender systems

Measure:	Audit criteria:	Materiality threshold:
18.2	**Requirement:** Relevant Signatories will develop and enforce publicly documented, proportionate policies to limit the spread of harmful false or misleading information (as depends on the service, such as prohibiting, downranking, or not recommending harmful false or misleading information, adapted to the severity of the impacts and with due regard to freedom of expression and information); and take action on webpages or actors that persistently violate these policies. **QRE 18.2.1:** Relevant Signatories will report on the policies or terms of service that are relevant to Measure 18.2 and on their approach towards persistent violations of these policies. **SLI 18.2.1:** Relevant Signatories will report on actions taken in response to violations of policies relevant to Measure 18.2, at the Member State level. The metrics shall include: Total number of violations and Meaningful metrics to measure the impact of these actions (such as their impact on the visibility of or the engagement with content that was actioned upon). **Definitions and Benchmarks:** • **Publicly documented:** Able to be accessed by the general public. • **Proportionate:** In a conscientious, balanced manner. • **Persistent violations:** As a Search Engine, Bing does not host content, including user generated content nor does Bing enable user to user communications. Therefore Bing does not experience "persistent violations" of their policies in the same way a Very Large Online Platform does, in which this QRE is generally aimed towards. • **Actions taken:** Actions applied to content, users, or services as a result of collaboration and information-sharing activities; as a search engine, Bing does not host content; therefore, such actions are not applicable to Bing.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains publicly available policies, guidelines, and controls designed through Webmaster Guidelines and How Bing Delivers Search Results to address harmful and misleading information across Bing Search. Bing's ranking systems are designed to promote authoritative and credible sources while reducing the visibility of spam and low-quality content.	1. Inspected the Bing March 2026 Report and ascertained that Bing publicly discloses documented policies describing its approach to delivering search results, including measures designed to promote authoritative information and reduce the visibility of harmful, false, or misleading information. 2. Inspected publicly available disclosures including the "How Bing Delivers Search Results" and "Bing Webmaster Guidelines" webpages and additional documentation to ascertain whether Bing discloses their policies to limit the spread of harmful false or misleading information.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 18.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 19 COCD - 'Safe design' of the architecture of the services, transparent policies, and accountability of recommender systems

Measure:	Audit criteria:	Materiality threshold:
19.1	**Requirement:** Relevant Signatories will make available to their users, including through the Transparency Centre and in their terms and conditions, in a clear, accessible and easily comprehensible manner, information outlining the main parameters their recommender systems employ. **QRE 19.1.1:** Relevant Signatories will provide details of the policies and measures put in place to implement the above-mentioned measures accessible to EU users, especially by publishing information outlining the main parameters their recommender systems employ in this regard. This information should also be included in the Transparency Centre. **Definitions and Benchmarks:** • **Clear, accessible and easily comprehensible:** Clear, and able to be understood broadly by reasonable users of the service, as determined through review by management. • **Recommender systems:** Fully or partially automated systems to suggest or prioritize in online interface specific information to recipients of the service, excluding advertising systems. Article 38 of the DSA requires that those recommender systems that are based on profiling provide at least one option for each of their recommender systems which is not based on profiling. Profiling means any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location, or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. Together this means that those recommender systems that use profiling are in scope. • **Main parameters:** Bing refers to main parameters as defined by management in its published transparency reporting document.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The Bing Compliance and Privacy teams maintain processes to identify and assess recommender systems and associated profiling across the Bing platform through both event-driven and periodic activities. New or updated features are evaluated through the Critical Impact Risk Assessment (CIRA) process to determine whether they materially impact recommender systems. Where such impact is identified, an assessment is performed to determine whether the feature should be included within the	1. Inspected documentation of the CIRA process, including the questionnaire, to ascertain whether evaluation of recommender system impact is captured and documented. 2. Inspected a sample CIRA assessment to ascertain whether consideration of recommender system impact was performed and the outcome was documented. 3. Inspected documentation of the annual review of core and generative features identified within the SRA to ascertain whether each feature was assessed to determine whether they utilize profiling. 4. Examined evidence of management review and approval to ascertain whether the inventory and analysis were reviewed and signed off and segregation of duties was maintained.

scope of recommender systems under Article 38.

On an annual basis, the Bing Compliance and Privacy teams perform a review of all core and generative features on the Bing platform identified within the Systemic Risk Assessment (SRA). Each feature was assessed to determine whether it uses profiling and whether it should be considered a recommender system under Article 38.

The resulting inventory and analysis are documented and tracked and are subject to management review and approval, with segregation of duties maintained between preparation and approval. This annual review, together with the CIRA process, supports the completeness of recommender system identification and management's assessment of the applicability of recommender system-related commitments, including Measure 19.1.

5. Selected samples of identified potential recommender systems and reperformed management's analysis to ascertain whether the features use profiling through observation of feature behavior, and compared the results of testing to management's analysis to ascertain whether the determination of profiling was consistent.
6. Inspected the results of management's annual review of all core and generative features on the Bing platform identified within the SRA and ascertained it supported the conclusion that there were no relevant recommender systems during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 19.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
19.2	**Requirement:** Relevant Signatories will provide options for the recipients of the service to select and to modify at any time their preferred options for relevant recommender systems, including giving users transparency about those options. **SLI 19.2.1:** Relevant Signatories will provide aggregated information on effective user settings, such as the number of times users have actively engaged with these settings within the reporting period or over a sample representative timeframe, and clearly denote shifts in configuration patterns. **Definitions and Benchmarks:** • **Recommender systems:** Fully or partially automated systems to suggest or prioritize in online interface specific information to recipients of the service, excluding advertising systems. Article 38 of the DSA requires that those recommender systems that are based on profiling provide at least one option for each of their recommender systems which is not based on profiling. Profiling means any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location, or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. Together this means that those recommender systems that use profiling are in scope. • **Shifts in configuration patterns:** Tooling changes made to the effective users settings that impact how the aggregated information on effective user settings could be interpreted.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The Bing Compliance and Privacy teams maintain processes to identify and assess recommender systems and associated profiling across the Bing platform through both event-driven and periodic activities. New or updated features are evaluated through the Critical Impact Risk Assessment (CIRA) process to determine whether they materially impact recommender systems. Where such impact is identified, an assessment is performed to determine whether the feature should be included within the scope of recommender systems under Article 38. On an annual basis, the Bing Compliance and Privacy teams perform a review of all core and generative features on the Bing platform identified within the Systemic	1. Inspected documentation of the CIRA process, including the questionnaire, to ascertain whether evaluation of recommender system impact is captured and documented. 2. Inspected a sample CIRA assessment to ascertain whether consideration of recommender system impact was performed and the outcome was documented. 3. Inspected documentation of the annual review of core and generative features identified within the SRA to ascertain whether each feature was assessed to determine whether they utilize profiling. 4. Examined evidence of management review and approval to ascertain whether the inventory and analysis were reviewed and signed off and segregation of duties was maintained. 5. Selected samples of identified potential recommender systems and reperformed management's analysis to ascertain whether the features use profiling through observation of feature behavior, and compared the results of testing to management's analysis to ascertain whether the determination of profiling was consistent. 6. Inspected the results of management's annual review of all core and generative features on the Bing platform identified within the SRA and ascertained it

Risk Assessment (SRA). Each feature was assessed to determine whether it uses profiling and whether it should be considered a recommender system under Article 38. The resulting inventory and analysis are documented and tracked and are subject to management review and approval, with segregation of duties maintained between preparation and approval. This annual review, together with the CIRA process, supports the completeness of recommender system identification and management's assessment of the applicability of recommender system-related commitments, including Measure 19.2.	supported the conclusion that there were no relevant recommender systems during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 19.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 20 COCD - 'Safe design' of the architecture of the services, transparent policies, and accountability of recommender systems

Measure:	Audit criteria:	Materiality threshold:
20.2	**Requirement:** Relevant Signatories will take steps to join/support global initiatives and standards bodies (for instance, C2PA) focused on the development of provenance tools. **QRE 20.2.1:** Relevant Signatories will provide details of global initiatives and standards bodies focused on the development of provenance tools (for instance, C2PA) that signatories have joined, or the support given to relevant organisations, providing links to organisation websites where possible. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing actively participates in and supports global initiatives and standards bodies (e.g., C2PA) to advance the development and adoption of provenance tools. Bing discloses details of global initiatives and standards bodies joined in COCD reports published to the Transparency Centre and on the Microsoft website on a periodic basis.	1. Inspected the Coalition for Content Provenance and Authenticity (C2PA) website to ascertain that Bing participates in or supports global initiatives and standards bodies related to provenance tools. 2. Inspected the identified initiatives to ascertain that they are focused on the development of provenance tools or related authenticity standards. 3. Inspected available information on Bing's involvement in such initiatives to ascertain the nature and extent of its participation. 4. Inspected evidence of Bing's implementation of provenance-related features to ascertain that such features align with initiatives focused on the development of provenance tools. 5. Inspected the Bing March 2026 Report to ascertain that Bing discloses details of global initiatives and standards bodies related to provenance tools that it has joined or supported (e.g., C2PA). 6. Inspected the disclosure within the Bing March 2026 Report and relevant information on Microsoft's public website to ascertain that such disclosure includes sufficient detail on Microsoft's support for such initiatives and where applicable, includes links to relevant organization websites.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 20.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 22 COCD - Better equipping users to identify disinformation

Measure:	Audit criteria:	Materiality threshold:
22.2	**Requirement:** Relevant Signatories will give users the option of having signals relating to the trustworthiness of media sources into the recommender systems or feed such signals into their recommender systems. **QRE 22.2.1:** Relevant Signatories will report on whether and, if relevant, how they feed signals related to the trustworthiness of media sources into their recommender systems, and outline the rationale for their approach. **Definitions and Benchmarks:** • **Recommender systems:** Fully or partially automated systems to suggest or prioritize in online interface specific information to recipients of the service, excluding advertising systems. Article 38 of the DSA requires that those recommender systems that are based on profiling provide at least one option for each of their recommender systems which is not based on profiling. Profiling means any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location, or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. Together this means that those recommender systems that use profiling are in scope.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The Bing Compliance and Privacy teams maintain processes to identify and assess recommender systems and associated profiling across the Bing platform through both event-driven and periodic activities. New or updated features are evaluated through the Critical Impact Risk Assessment (CIRA) process to determine whether they materially impact recommender systems. Where such impact is identified, an assessment is performed to determine whether the feature should be included within the scope of recommender systems under Digital Services Act, Article 38. On an annual basis, the Bing Compliance and Privacy teams perform a review of all core and generative features on the Bing platform identified within the Systemic Risk Assessment (SRA). Each feature was assessed to determine whether it uses	1. Inspected documentation of the CIRA process, including the questionnaire, to ascertain whether evaluation of recommender system impact is captured and documented. 2. Inspected a sample CIRA assessment to ascertain whether consideration of recommender system impact was performed and the outcome was documented. 3. Inspected documentation of the annual review of core and generative features identified within the SRA to ascertain whether each feature was assessed to determine whether they utilize profiling. 4. Examined evidence of management review and approval to ascertain whether the inventory and analysis were reviewed and signed off and segregation of duties was maintained. 5. Selected samples of identified potential recommender systems and reperformed management's analysis to ascertain whether the features use profiling through observation of feature behavior, and compared the results of testing to management's analysis to ascertain whether the determination of profiling was consistent. 6. Inspected the results of management's annual review of all core and generative features on the Bing platform identified within the SRA and ascertained it supported the conclusion that there were no relevant recommender systems during the Examination Period.

profiling and whether it should be considered a recommender system under Digital Services Act, Article 38.

The resulting inventory and analysis are documented and tracked and are subject to management review and approval, with segregation of duties maintained between preparation and approval. This annual review, together with the CIRA process, supports the completeness of recommender system identification and management's assessment of which Bing features are relevant under Digital Services Act, Article 38, including for purposes of Measure 22.2 and QRE 22.2.1.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 22.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
22.3	**Requirement:** Relevant Signatories will make details of the policies and measures put in place to implement the above-mentioned measures accessible to EU users, especially by publishing information outlining the main parameters their recommender systems employ in this regard. This information should be included in the Transparency Centre. **QRE 22.3.1:** Relevant Signatories will provide details of the policies and measures put in place to implement the above mentioned measures to EU users, especially by publishing information outlining the main parameters their recommender systems employ in this regard. This information should also be included in the Transparency Centre. **Definitions and Benchmarks:** • **Recommender systems:** Fully or partially automated systems to suggest or prioritize in online interface specific information to recipients of the service, excluding advertising systems. Article 38 of the DSA requires that those recommender systems that are based on profiling provide at least one option for each of their recommender systems which is not based on profiling. Profiling means any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location, or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. Together this means that those recommender systems that use profiling are in scope.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The Bing Compliance and Privacy teams maintain processes to identify and assess recommender systems and associated profiling across the Bing platform through both event-driven and periodic activities. New or updated features are evaluated through the Critical Impact Risk Assessment (CIRA) process to determine whether they materially impact recommender systems. Where such impact is identified, an assessment is performed to determine whether the feature should be included within the scope of recommender systems under Digital Services Act, Article 38. On an annual basis, the Bing Compliance and Privacy teams perform a review of all core and generative features on the Bing platform identified within the Systemic	1. Inspected documentation of the CIRA process, including the questionnaire, to ascertain whether evaluation of recommender system impact is captured and documented. 2. Inspected a sample CIRA assessment to ascertain whether consideration of recommender system impact was performed and the outcome was documented. 3. Inspected documentation of the annual review of core and generative features identified within the SRA to ascertain whether each feature was assessed to determine whether they utilize profiling. 4. Examined evidence of management review and approval to ascertain whether the inventory and analysis were reviewed and signed off and segregation of duties was maintained. 5. Selected samples of identified potential recommender systems and reperformed management's analysis to ascertain whether the features use profiling through observation of feature behavior, and compared the results of testing to management's analysis to ascertain whether the determination of profiling was consistent. 6. Inspected the results of management's annual review of all core and generative features on the Bing platform identified within the SRA and ascertained it

Risk Assessment (SRA). Each feature was assessed to determine whether it uses profiling and whether it should be considered a recommender system under Digital Services Act, Article 38. The resulting inventory and analysis are documented and tracked and are subject to management review and approval, with segregation of duties maintained between preparation and approval. This annual review, together with the CIRA process, supports the completeness of recommender system identification and management's assessment of which Bing features are relevant under Digital Services Act, Article 38, including for purposes of Measure 22.3 and QRE 22.3.1.	supported the conclusion that there were no relevant recommender systems during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 22.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
22.7	**Requirement:** Relevant Signatories will design and apply products and features (e.g. information panels, banners, pop-ups, maps and prompts, trustworthiness indicators) that lead users to authoritative sources on topics of particular public and societal interest or in crisis situations. **QRE 22.7.1:** Relevant Signatories will outline the products and features they deploy across their services and will specify whether those are available across Member States. **SLI 22.7.1:** Relevant Signatories will report on the reach and/or user interactions with the products or features, at the Member State level, via the metrics of impressions and interactions (clicks, click-through rates (as relevant to the tools and services in question) and shares (as relevant to the tools and services in question). **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing has implemented measures to help counter low authority information and misinformation related to elections, the Russia-Ukraine conflict, the Israel-Hamas conflict, and EU Member State elections. Microsoft participated in the Task-force's Crisis Response Subgroup and Elections Working Group and collaborated with election authorities to promote trusted election-related information. As part of its response, Bing adjusted ranking systems to elevate authoritative content and reduce the visibility of less authoritative information across Bing Search and Copilot Search. Bing also leveraged threat intelligence and resilience signals to identify and respond to information operations, collaborated with trusted third-party organizations including fact-checkers, news publishers, researchers, and nonprofit organizations, and removed autosuggest terms likely to direct users to low authority content. Management has prepared the disclosures under SLI 22.7.1 by reporting Member State-level reach and user interaction metrics associated with Bing	1. Inspected Bing March 2026 Report and ascertained that Bing disclosed products, features, and related measures deployed across Bing Search to direct users toward authoritative sources on topics of public and societal interest and crisis situations, including election-related activities, crisis-reporting initiatives, and measures designed to promote authoritative information and reduce the visibility of low authority information. 2. Inspected supporting documentation for the election-related activities, crisis-reporting initiatives, and products, features, and related measures disclosed in the report, and ascertained that the information included in the disclosure are consistent with the underlying evidence. 3. Inspected Bing March 2026 Report and ascertained that the disclosures include Member State-level reach and user interaction metrics for the relevant products or features, including impressions and defensive interventions.

Search's defensive search interventions related to topics of public and societal interest and crisis situations. The disclosures include quantitative metrics intended to demonstrate the reach and impact of such interventions, including the number of user queries addressed through defensive search interventions and the resulting user impressions during the reporting period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive with Comments – In our opinion, Bing complied with Measure 22.7 during the Examination Period, in all material respects.

Although the audited measure has been met, we noted the following:

- Evidence supporting the completeness and accuracy of reported impressions and interaction metrics under SLI 22.7.1 was not consistently retained.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
D&T recommends Bing enhanced evidence retention practices to ensure sufficient documentation is maintained to demonstrate the completeness and accuracy of reported impressions and interaction metrics under SLI 22.7.1.	By January 31, 2027

Section 6: Empowering the research community

Commitment 26 COCD - Disclosure of and access to signatories' data for research on disinformation

Measure:	Audit criteria:	Materiality threshold:
26.1	**Requirement:** Relevant Signatories will provide public access to non-personal data and anonymised, aggregated or manifestly-made public data pertinent to undertaking research on Disinformation on their services, such as engagement and impressions (views) of content hosted by their services, with reasonable safeguards to address risks of abuse (e.g. API policies prohibiting malicious or commercial uses). **QRE 26.1.1:** Relevant Signatories will describe the tools and processes in place to provide public access to non-personal data and anonymised, aggregated and manifestly-made public data pertinent to undertaking research on Disinformation, as well as the safeguards in place to address risks of abuse. **SLI 26.1.1:** Relevant Signatories will provide quantitative information on the uptake of the tools and processes described in Measure 26.1, such as number of users. **QRE 26.1.2:** Relevant Signatories will publish information related to data points available via Measure 26.1, as well as details regarding the technical protocols to be used to access these data points, in the relevant help centre. This information should also be reachable from the Transparency Centre. At minimum, this information will include definitions of the data points available, technical and methodological information about how they were created, and information about the representativeness of the data. **Definitions and Benchmarks:** • **Research on disinformation:** Research requests submitted through Microsoft's Qualified Researcher Program related to the study of disinformation topics. Whether a request constitutes research on disinformation is assessed by the Qualified Researcher Program based on the information provided by the researcher and applicable program criteria. • **Reasonable safeguards:** Measures and / or precautions taken to prevent misuse or abuse of publicly accessible, non-personal data pursuant to the nature of data to be released. Examples may include, but are not limited to API policies and usage restrictions, data release review processes, and terms and conditions once released. Note, as a Search Engine, Bing does host content, including user generated content nor does Bing enable user to user communications.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains the "Bing Qualified Researcher Program" portal, where researchers can submit information and data access requests to Bing for vetted researchers. Bing reviews these requests and responds within 15 business days	1. Inspected the Bing research resources webpage to ascertain whether Bing provides access to non-personal, anonymized, aggregated, or manifestly public data for disinformation research and whether appropriate safeguards are in place to mitigate risks of misuse. 2. Inspected the Bing March 2026 Report to ascertain whether Microsoft Bing discloses the tools and processes in place to provide public access to non-

with a decision. Once management determines a decision, access will be granted or denied based on the decision.	personal data and public data pertinent to undertaking research on disinformation, as well as the safeguards in place to address risks of abuse. 3. Inspected the bing-researcher@microsoft.com mailbox, email notifications, dashboard of responses, and corresponding entries in the requests tracker, to ascertain whether there is a defined process in place for researchers to request access to data. 4. Inspected the Bing March 2026 Report to ascertain that Bing reported the number of researcher access requests. 5. Obtained the population of researcher access requests from the Requests Tracker along with corresponding approval/denial records and ascertained that there were zero research requests for COCD. 6. Inspected the Bing March 2026 Report available in the Transparency Centre, as well as the publicly available support page for the Bing Qualified Researcher program, to ascertain whether Bing published information related to data points available via Measure 26.1. Ascertained that the published information included the technical protocols to be used to access these data points, definitions of the data points available, technical and methodological information about how they were created, and information about the representativeness of the data.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 26.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
26.3	**Requirement:** Relevant Signatories will implement procedures for reporting the malfunctioning of access systems and for restoring access and repairing faulty functionalities in a reasonable time. **QRE 26.3.1:** Relevant Signatories will describe the reporting procedures in place to comply with Measure 26.3 and provide information about their malfunction response procedure, as well as about malfunctions that would have prevented the use of the systems described above during the reporting period and how long it took to remediate them. **Definitions and Benchmarks:** • **Access systems:** Access to data for disinformation related research provided through Microsoft's Qualified Researcher Program subject to legal, privacy, security, confidentiality, and technical feasibility constraints. • **Reasonable time:** Proceedings are conducted efficiently, fairly and without unnecessary delay.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains the "Bing Qualified Researcher Program" portal, where researchers can submit information and data access requests to Bing for vetted researchers. Microsoft has established a formal process for managing and responding to researcher access issues. Reported issues are centrally managed through a comprehensive issue-tracking mechanism, supported by established channels for reporting access-related issues and technical malfunctions.	1. Inspected publicly available support pages, as well as Bing's Internal Issues Tracker, and ascertained that procedures are in place for reporting the malfunctioning of access systems and for restoring access and repairing faulty functionalities in a reasonable time. 2. Inspected the Bing Researchers Issues Tracker, which records issues received via bing-researcher-form-issues@microsoft.com and bing-researcher@microsoft.com mailboxes, and ascertained that a defined and structured process is in place to identify, track, and address issues related to the malfunctioning of access systems in a timely manner. Per inspection, ascertained that there were no malfunctions reported during the audit period. 3. Verified that reporting procedures for malfunctions are documented in the tracker, including details of the issue, impact on system usage, and malfunction response procedures. 4. Inspected and reviewed Bing's responses within the COCD transparency report and ascertained that Bing described the reporting procedures in place to comply with Measure 26.3 and provided information about their malfunction response procedure. As there were no malfunctions reported during the period, there were no malfunctions for Bing to report on.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 26.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 28 COCD - Cooperation with researchers

Measure:	Audit criteria:	Materiality threshold:
28.2	**Requirement:** Relevant Signatories will be transparent on the data types they currently make available to researchers across Europe. **QRE 28.2.1:** Relevant Signatories will describe what data types European researchers can currently access via their APIs or via dedicated teams, tools, help centres, programs, or events. **Definitions and Benchmarks:** • **Make available to researchers:** Providing a mechanism for researchers to access data for the purposes of disinformation related research through Microsoft's Qualified Researcher Program. • **Dedicated:** Bing considers a "Dedicated" team to be Bing stakeholders that participate in the collection, dissemination, and or review of information in relation to QRE 28.2.1.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft maintains the "Bing Qualified Researcher Program" portal, where Microsoft describes the data types researchers can access via the Qualified Researcher Program.	1. Inspected the Bing March 2026 Report and the Bing Qualified Researcher Program webpage to ascertain whether Bing published information related to data types available to researchers. Ascertained this included the types of data available to researchers, including details such as query text, market (geographic region), date of query, and query frequency.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 28.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
28.3	**Requirement:** Relevant Signatories will not prohibit or discourage genuinely and demonstratively public interest good faith research into Disinformation on their platforms, and will not take adversarial action against researcher users or accounts that undertake or participate in good-faith research into Disinformation. **QRE 28.3.1:** Relevant Signatories will collaborate with EDMO to run an annual consultation of European researchers to assess whether they have experienced adversarial actions or are otherwise prohibited or discouraged to run such research. **Definitions and Benchmarks:** • **Adversarial action:** Action that interferes with or otherwise prohibits good-faith research as it relates to the dissemination of disinformation (managed as information integrity in Bing) in which the requested information is readily available without significant new activity required and not in conflict with key interests in privacy. • **Collaborate:** EDMO conducts an annual consultation of European researchers and may engage online platforms to inform its assessment of adversarial actions affecting the research community. Bing may provide input upon EDMO's request.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft publicly demonstrates its commitment to supporting genuine, good-faith research into disinformation by providing researchers with access to Bing datasets through the Microsoft Support page. Microsoft has established a process to engage with the European Digital Media Observatory (EDMO) in support of its commitments under the Code of Conduct on Disinformation (COCD), including the annual consultation of European researchers. Through ongoing communication and coordination with EDMO, Microsoft demonstrates its intent to collaborate on researcher engagement initiatives and supports EDMO's role in organizing consultations across platform signatories.	1. Inspected the publicly available Microsoft Support page titled "Providing Bing Datasets Access for Researchers" and ascertained that Bing promotes researcher access and participation in good faith research activities, including research related to disinformation, without discouragement or adverse action against participating researchers or accounts. Ascertained there were no COCD research requests or access issues received via the Bing Qualified Researcher Program during the period and no instances of adversarial action against researcher users or accounts. 2. Inspected the Bing March 2026 Report and ascertained that Bing discloses plans to collaborate with relevant signatories and participate in an annual consultation with European researchers under the Code of Conduct on Disinformation. 3. Inspected communications between Bing and EDMO and confirmed that EDMO is responsible for coordinating the annual consultation; however, no annual consultation with European researchers occurred during the examination period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 28.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Section 7: Empowering the fact-checking community

Bing has not elected to subscribe in the commitments associated with Section 7, *Empowering the fact-checking community*. Accordingly, these commitments were excluded from the scope of testing. For additional information regarding Bing's subscriptions, please refer to Bing's report available in the Transparency Center (https://disinfocode.eu/).

Section 8: Transparency Centre

Commitment 34 COCD - Transparency Centre

Measure:	Audit criteria:	Materiality threshold:
34.1	**Requirement:** Signatories will establish and maintain the common Transparency Centre website, which will be operational and available to the public within 6 months from the signature of this Code. **Definitions and Benchmarks:** • **Available to the public:** Able to be accessed by the general public.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
The Transparency Centre website has been developed, launched, and maintained in accordance with the Code's timeline and standards.	1. Inspected the Transparency Centre website and supporting evidence to ascertain the Transparency Centre website existed and was made publicly available within six (6) months of Bing signing the Code. 2. Inspected the Transparency Centre website to ascertain it was publicly available and operational during the Examination Period. 3. Inspected evidence of Bing's ongoing maintenance of the Transparency Centre website to ascertain Bing continues to support the operation and maintenance of the Transparency Centre.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 34.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
34.2	**Requirement:** Signatories will provide appropriate funding, for setting up and operating the Transparency Centre website, including its maintenance, daily operation, management, and regular updating. Funding contribution should be commensurate with the nature of the Signatories' activity, and shall be sufficient for the website's operations and maintenance and proportional to each Signatory's risk profile and economic capacity. **Definitions and Benchmarks:** • **Appropriate funding:** Bing considers the benchmark for this measure to be the arrangement agreed upon between the signatories and the European Commission (EC). Historically, funding contributions for the set up, and operations and (where considered needed) update of the Transparency Centre website has been determined in consultation with the EC and other signatories.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing provides appropriate funding for operating the Transparency Centre website, including maintenance, daily operation, management, and regular updating.	1. Inspected the service agreement between Bing and the Transparency Centre host to ascertain the agreed funding terms and scope of services, including the operation, maintenance, management, and updating of the Transparency Centre website. 2. Inspected evidence of payment from Bing to Transparency Centre host to ascertain whether Bing initiated payment as agreed upon in the service agreement. 3. Inspected evidence from the Transparency Centre host to ascertain that the funding payment was successfully received.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 34.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
34.3	**Requirement:** Relevant Signatories will contribute to the Transparency Centre's information to the extent that the Code is applicable to their services. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing contributes information to the Transparency Centre, to the extent that the Code is applicable to its services, through the publication of its Transparency Reports to the Transparency Centre.	1. Inspected evidence to corroborate Bing uploaded and published its semi-annual reports to the Transparency Centre to demonstrate Bing contributed to the Transparency Centre's information to the extent that the code is applicable to its services. 2. Inspected the Transparency Centre website to ascertain that Bing March 2026 Report and contributions were present and the information posted was accessible and aligned with the measures to which Bing subscribed. 3. Inspected European Commission (EC) press release to corroborate the EC acknowledged Microsoft's report publication to ascertain Bing's contribution to the Transparency Centre.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 34.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
34.4	**Requirement:** Signatories will agree on the functioning and financing of the Transparency Centre within the Task-force, to be recorded and reviewed within the Task-force on an annual basis. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in the Permanent Task-force supporting the implementation and transparency of the Code. As part of this process, Bing contributes to the agreed functioning and funding arrangement supporting the Transparency Centre in accordance with arrangements agreed upon within the Task-force.	1. Inquired with management to understand the funding and payment process supporting the Transparency Centre. 2. Inspected samples of Task-force meeting invitations and agendas to determine whether the topics discussed related to the functioning and financing of the Transparency Centre. 3. Inspected agreements, payment documentation, and supporting evidence to ascertain Bing's contribution to the functioning and financing of the Transparency Centre.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 34.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
34.5	**Requirement:** The Task-force will regularly discuss the Transparency Centre and assess whether adjustments or actions are necessary. Signatories commit to implement the actions and adjustments decided within the Task-force within a reasonable timeline. **Definitions and Benchmarks:** • **Reasonable timeline:** A time period that is proportionate and feasible and without undo delay, taking into account the urgency of the action identified, its complexity, and operational constraints, as determined through consultations within the Task-force and subject to management review and approval.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in the Permanent Task-force supporting the implementation and transparency of the Code. As part of this process, Bing contributes to discussions regarding the Transparency Centre and, where applicable, participates in assessments of whether adjustments or actions are necessary. Bing also supports the implementation of agreed-upon adjustments or actions within a reasonable timeline.	1. Inspected evidence showcasing Bing's participation and contribution in Transparency Centre Sub-group meetings within the audit period. 2. Inspected evidence of an adjustment or action being necessary within the Transparency Centre and assessed timeliness of the implementation of the update. 3. Inspected the Transparency Centre to corroborate that the agreed adjustment or action was implemented as intended.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 34.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 35 COCD - Transparency Centre

Measure:	Audit criteria:	Materiality threshold:
35.1	**Requirement:** Signatories will list in the Transparency Centre, per each commitment and measure that they subscribe to, the terms of service and policies that their service applies to implement these commitments and measures. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing systematically lists and updates the Transparency Centre relevant to each commitment and measure they subscribe to, the terms of service and policies that their service applies to implement these commitments and measures.	1. Inspected the Transparency Centre and the Bing March 2026 Report to identify disclosures related to commitments and associated measures subscribed to by Bing. 2. Assessed whether the Transparency Centre disclosures include information on the terms of service and policies used to implement each commitment and measure, including references to relevant policies. 3. For each subscribed measure, inspected the associated disclosures to determine whether Bing provides policy-related information and descriptions of implementation approaches supporting the requirements of the measure.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 35.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
35.2	**Requirement:** Signatories will provide information on the implementation and enforcement of their policies per service, including geographical and language coverage. **Definitions and Benchmarks:** • **Enforcement:** Enforcement refers to the implementation of Bing's policies through a robust and multi-layered system of mitigations that influence the visibility, prioritization, or accessibility of information in search results. Unlike content-hosting platforms which can action user generated content, Bing operationalizations this through ranking, indexing, and webmaster guideline processes.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing provides information on the implementation and enforcement of its policies per service through the Transparency Center, including geographical and language coverage.	1. Inspected the Bing Transparency Centre and the Bing March 2026 Report to ascertain Bing's disclosures provide information regarding the implementation and enforcement of Bing's policies per service, including references to relevant policies. 2. Inspected the policy referenced in the COCD Report and navigated to the linked webpages to ascertain the links were functional and the policy information was accessible. 3. Inspected the policy-related information and ascertained it provides details regarding policy implementation and enforcement, including geographical and language coverage.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 35.2 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
35.3	**Requirement:** Signatories will ensure that the Transparency Centre contains a repository of their reports assessing the implementation of the Code's commitments. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing has compliance measures in place to regularly update and submit reports in the Transparency Centre, assessing the implementation of the Code's commitments.	1. Inspected the publicly available Transparency Centre and related report links to ascertain whether Bing maintains a repository of reports published during the Examination Period (September 2025 and March 2026) assessing implementation of the Code's commitments.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 35.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
35.4	**Requirement:** In crisis situations, Signatories will use the Transparency Centre to publish information regarding the specific mitigation actions taken related to the crisis. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing maintains a crisis response process that governs the identification and implementation of crisis related mitigation measures and the publication of such measures in the Transparency Centre to promote transparency during crisis situations.	1. Inspected evidence of designated crisis situations from the European Commission (EC) to ascertain the crisis situations for which Bing was required to disclose specific mitigation actions. 2. Inspected the Bing March 2026 Report to ascertain that Bing disclosed each designated crisis situation and the corresponding mitigation actions taken in response.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 35.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Section 9: Permanent Task-force

Commitment 37 COCD - Permanent Task-force

Measure:	Audit criteria:	Materiality threshold:
37.1	**Requirement:** Signatories will participate in the Task-force and contribute to its work. Signatories, in particular smaller or emerging services will contribute to the work of the Task-force proportionately to their resources, size and risk profile. Smaller or emerging services can also agree to pool their resources together and represent each other in the Task-force. The Task-force will meet in plenary sessions as necessary, and at least every 6 months, and, where relevant, in subgroups dedicated to specific issues or workstreams. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in the Permanent Task-force established under the Code of Practice on Disinformation. Participation includes attendance at plenary meetings organized by the European Commission involving relevant stakeholders and experts, as well as participation in working groups and subgroups dedicated to specific issues and workstreams. Bing engages in Task-force coordination activities through communications with the European Commission and participates in relevant subgroup discussions, including election-related working groups. Bing's participation in Task-force activities are supported through meeting attendance, meeting documentation, and communications with relevant stakeholders.	1. Inspected evidence demonstrating Bing's participation and contributions in Task-force plenary meetings within the Examination Period. 2. Inspected evidence to ascertain whether the Task-force met at least every 6 months. 3. Inspected meeting invitations, agendas, and correspondences to ascertain whether Bing participated in the Permanent Task-force plenary meeting and relevant Task-force subgroup activities during the Examination Period. 4. Determined whether Bing's contributions to the Task-force are proportionate to its size, resources, and risk profile by inspecting the Microsoft Bing Subscription Document, reviewing evidence of participation in Task-force meetings, subgroups, and working groups, and assessing whether the focus of these activities aligns with the systemic risks identified in Bing's SRA, including risks relating to civic discourse and electoral processes.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 37.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
37.2	**Requirement:** Signatories agree to work in the Task-force in particular — but not limited to — on the following tasks: • Establishing a risk assessment methodology and a rapid response system to be used in special situations like elections or crises. • Cooperate and coordinate their work in special situations like elections or crisis. • Agree on the harmonised reporting templates for the implementation of the Code's commitments and measures, the refined methodology of the reporting, and the relevant data disclosure for monitoring purposes. • Review the quality and effectiveness of the harmonised reporting templates, as well as the formats and methods of data disclosure for monitoring purposes, throughout future monitoring cycles, and adapt them as needed. • Contribute to the assessment of the quality and effectiveness of Service Level and Structural Indicators and the data points provided to measure these indicators, as well as their relevant adaptation. • Refine, test and adjust Structural Indicators and design mechanisms to measure them at Member State level. • Agree, publish and update a list of TTPs employed by malicious actors, and set down baseline elements, objectives and benchmarks for measures to counter them, in line with the Chapter IV of this Code. • Seek out and discuss research, expert input and up-to-date evidence relevant to the Code's commitments, such as, inter alia, emerging best practices in safe design, retroactive flagging, repository of fact-checks, provenance tools. • Discuss and provide guidance on the adequate quantitative information to be provided by Signatories to fulfil their reporting obligations regarding engagements with fact-checking organisations across different services. • Regularly discuss whether the Code's commitments and measures need updating in view of technological, societal, market and legislative developments, as well as in view of accommodating new Signatories and, where the Task-force agrees to be necessary, carry out such updates. • Review the appropriateness and consistency of adapted measures for smaller or emerging services. • Promote the Code among relevant peers and integrate new Signatories to the Code. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in Permanent Task-force activities relating to special situations such as elections and crises, including engagement with the Elections Rapid Response System (RRS). Bing maintains processes to support participation in election-related RRS	1. Inquired with management regarding Bing's processes for complying with Measure 37.2 and observed Bing's participation in Permanent Task-force meetings, plenary sessions, and relevant subgroups, including the Elections Working Group through December 2025 and the Integrity of Service, Crisis, Elections, and AI subgroups from January 2026. 2. Inquired with management regarding whether the Permanent Task-force had established a risk assessment methodology and a Rapid Response System

activities, including submission mechanisms, internal tracking of RRS activity, restricted access controls, and notification processes for relevant stakeholders.

Bing also participates in Task-force activities relating to harmonised reporting templates, reporting requirements, and discussions regarding potential updates to Code commitments and measures. Relevant stakeholders receive and review communications arising from Permanent Task-force discussions and participate in recurring internal meetings to discuss relevant matters, coordinate responses, and support Bing's contribution to applicable Code-related activities.

("RRS") for special situations such as elections or crises. Inspected Bing's systemic risk assessment documentation and noted that it considers misinformation and disinformation-related risks associated with elections and crises, including mitigants such as the RRS.

3. Inspected communications issued by the European Commission relating to activation of the Elections Rapid Response System ("RRS") during the Examination Period and inspected Transparency Centre disclosures to ascertain whether the RRS had been established and disclosed, including its purpose, timing, and operation.
4. Inspected the Bing March 2026 Report, together with meeting invitations and agendas relating to the Elections and Crisis Response Sub-groups, to ascertain whether Bing disclosed and participated in relevant election- and crisis-related coordination activities.
5. Inspected the harmonised reporting template to ascertain whether it included reporting fields and data disclosure practices for monitoring implementation of the COCD. Inspected Bing's COCD Reports and samples of reports published by other Signatories to ascertain whether the same harmonised reporting template was utilized.
6. Inspected communications and correspondence issued by the European Commission and Permanent Task-force to ascertain whether any changes had been made to, or proposed for, the harmonised reporting template during the Examination Period. Inspected Bing's process documentation to ascertain whether Bing had a defined process for identifying and communicating proposed changes to the harmonised reporting template to the Permanent Task-force.
7. Inspected Bing's Subscription Document, scoping assessment documentation, and Bing March 2026 Report to determine the applicability of the Measure 37.2 requirements relating to Service Level Indicators, Structural Indicators, tactics, techniques and procedures ("TTPs"), and quantitative information relating to agreements with fact-checking organizations. Confirmed that Bing had not subscribed to Commitments 3, 14, 17, 30, and 41 and accordingly determined that these requirements were not applicable to Bing during the Examination Period.
8. Inspected the agenda and invitation for the December 2025 Permanent Task-force plenary meeting to ascertain whether research, expert input, emerging evidence, and broader Code implementation and reporting matters were discussed during the Examination Period. In addition, inspected Bing's process documentation to ascertain whether Bing had a defined process for notifying the Permanent Task-force of any proposed updates to commitments or measures.
9. Inspected evidence relating to the new COCD Signatory acceptance process to ascertain whether Task-force members were provided with the opportunity to review commitments proposed by new Signatories and, where applicable, provide input regarding the appropriateness and consistency of proposed measures.
10. Inspected the Transparency Centre COCD Signatory list and a sample of emails from the Permanent Task-force requesting Signatories' input on the acceptance of new Signatories to ascertain whether Bing was provided with the opportunity

	to review and comment on new Signatory applications as part of the approval process.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive with Comments – In our opinion, Bing complied with Measure 37.2 during the Examination Period, in all material respects.

Although the audited measure has been met, the Task-force representatives did not document and retain evidence showing that all tasks were performed.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
The Task-force representatives should document and retain evidence showing that all tasks were performed during the period.	By January 31, 2027

Measure:	Audit criteria:	Materiality threshold:
37.4	**Requirement:** Signatories agree to set up subgroups dedicated to the specific issues related to the implementation and revision of the Code with the participation of the relevant Signatories. **Definitions and Benchmarks:** • **Specific issues:** Sub-groups set up between signatories whose focus relate to key concerns to which The Code aims to combat. To date, the signatories, in collaboration with the EC, have established the following sub-groups: Ad Scrutiny, Integrity of Services, Crisis, Elections, and AI.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in Task-force subgroups and working groups established under the Code of Conduct on Disinformation to support the implementation of Code commitments and measures. Participation includes engagement in issue-specific working groups and coordination activities facilitated through the Task-force. Bing's participation in Task-force subgroup activities are supported through attendance at relevant meetings and communications with the European Commission and other Task-force participants regarding subgroup initiatives and activities.	1. Developed an understanding of how Task-force subgroups and working groups are established for specific issues related to the implementation and revision of the Code. 2. Inspected evidence for the relevant Task-force subgroups and working groups during the Examination Period, that Bing has participated through its attendance of the meetings. 3. Inspected evidence demonstrating Bing's further commitment to participate in Task-force subgroups and working groups of Integrity of Service, Crisis, Elections, and AI; which have been identified by the Task-force as related to the implementation and revision of the Code.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 37.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
37.5	**Requirement:** When needed, and in any event at least once per year, the Task-force organises meetings with relevant stakeholder groups and experts to inform them about the operation of the Code and gather their views related to important developments in the field of disinformation. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in Permanent Task-force plenary meetings organized by the European Commission involving relevant stakeholders and experts. These meetings provide a forum for participants to discuss the operation of the Code and share views on developments relevant to disinformation. Bing's participation in these activities are supported through attendance at Taskforce plenary meetings and engagement with stakeholders, experts, and other Task-force participants.	1. Inquired with management and obtained evidence to ascertain whether Bing participated in the Permanent Task-force plenary meeting organized by the European Commission during the reporting period. 2. Inspected evidence to ascertain whether the meeting involved relevant stakeholder groups and experts and was held to inform participants about the operation of the Code and gather their views on important developments in the field of disinformation.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 37.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
37.6	**Requirement:** Signatories agree to notify the rest of the Task-force when a commitment or measure would benefit from changes over time as their practices and approaches evolve, in view of technological, societal, market, and legislative developments. Having discussed the changes required, relevant Signatories will update their subscription document accordingly and report on the changes in their next report. **QRE 37.6.1:** Signatories will describe how they engage in the work of the Task-force in the reporting period, including the sub-groups they engaged with. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing maintains governance processes to review developments relating to the Code of Conduct on Disinformation and assess whether updates to commitments, measures or reporting requirements are required. Relevant stakeholders participate in recurring cross-functional Microsoft working group discussions (referred to internally as "V-Teams") relating to Code developments, reporting obligations and potential changes arising from Taskforce activities. Bing maintains documented processes for assessing potential updates and incorporating changes into reporting requirements where applicable. Participation in Taskforce activities and related disclosures are reflected through Bing's Subscription Document and Transparency Reports.	1. Inspected the Bing March 2026 Report to understand how Bing engages with the Task-force and sub-groups. 2. Obtained a flow chart describing Bing's internal process for notifying the Task-force of a proposed update to a COCD commitment or measure. 3. Performed inquiry with management on whether any updates had been proposed to the Task-force during the Examination Period. 4. Inspected Bing's COCD Subscription Document to ascertain that no changes occurred during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 37.6 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Section 10: Monitoring of the Code

Commitment 38 COCD - Monitoring of the Code

Commitment:	Audit criteria:	Materiality threshold:
38	**Requirement:** The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code. **QRE 38.1.1:** Relevant Signatories will outline the teams and internal processes they have in place, per service, to comply with the Code in order to achieve full coverage across the Member States and the languages of the EU. **Definitions and Benchmarks:** • **Adequate financial and human resources:** Resourcing, commensurate with the nature and risk of the service in the EU, to ensure appropriate implementation of Code Commitments. • **Languages of the EU:** The 24 official languages of the EU: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, and Swedish.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Microsoft Bing has implemented a governance and operational framework, supported by a dedicated cross functional team of relevant legal, product, policy, and compliance stakeholders, to oversee compliance and regulatory monitoring, transparency reporting, and implementation of requirements across applicable geographical regions. To facilitate compliance oversight, Bing has implemented an internal tracking process that captures relevant commitments and measures, assigns responsible entities, and identifies accountable personnel for execution of requirements, supported by periodic governance and monitoring activities through recurring cross functional meetings, Task-force discussions, and stakeholder coordination. Bing has also established formal annual investment and strategy review processes to evaluate and approve human and financial resource allocation	1. Inspected the Bing March 2026 Report and corroborating supporting documentation including stakeholder roles and responsibilities, evidence of recurring compliance monitoring and cross-functional coordination meetings, documentation of localization/language coverage processes, and email evidence of investment strategy/resource allocation approvals and also performed management inquiry to verify the governance structure, implementation measures, and teams supporting compliance with Code of Conduct on Disinformation, including legal, product, policy, and compliance teams, and other relevant stakeholders. 2. Inspected stakeholder roles and responsibilities, reviewed the internal compliance tracking process, and verified that commitments, responsible entities, and accountable personnel are documented and monitored to support compliance with commitments obligations. 3. Inspected evidence of recurring governance and compliance monitoring activities, including monthly sync meetings, Task-force discussions, and cross functional coordination meetings, and reviewed documentation supporting geographical and language coverage across applicable EU Member States. 4. Inspected evidence of senior leadership review and approval of Bing's investment strategy and resource allocation for Code of Conduct on Disinformation compliance activities to ascertain whether Bing committed to dedicate adequate financial and human resources to ensure the implementation of their commitments under the Code.

supporting Code of Conduct on Disinformation compliance activities.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Commitment 38 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 40 COCD - Monitoring of the Code

Measure:	Audit criteria:	Materiality threshold:
40.1	**Requirement:** Relevant Signatories that are providers of VLOPSEs, as defined in the DSA, will report every six months on the implementation of the commitments and measures they signed up to under the Code, including on the relevant QREs and SLIs, at service and Member State Level. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing publishes reports every six months detailing its implementation of the commitments and measures subscribed to under the Code, including relevant QREs and SLIs, at the service and Member State level, where applicable.	1. Inspected the publication dates of the identified reports to ascertain that Bing reported on a recurring six-month cadence during the Examination Period. 2. Inspected the most recent report published Bing March 2026 Report and the associated subscription overviews to ascertain that implementation reporting was aligned to Bing's subscribed commitments and measures and included relevant QREs and SLIs, where applicable. 3. Inspected the most recent report's content published in March 2026 to determine whether the relevant QREs and SLIs were presented at the service and Member State level, where applicable.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 40.1 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
40.3	**Requirement:** Signatories will regularly update the Transparency Centre with relevant QREs and SLIs, at least in line with their reporting period under this Code. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing has measures in place to update the Transparency Centre with relevant QREs and SLIs in accordance with its reporting schedule. The Transparency Centre is updated through recurring COCD reporting publications, at least in line with the reporting period required under this Code and reflects current commitment-level reporting disclosures.	1. Inspected COCD reports for two reporting periods (September 2025 and March 2026) to ascertain that the Transparency Centre was maintained and updated in line with the Code reporting cycle. 2. Inspected and compared the QRE and SLI disclosures between the September 2025 and March 2026 COCD reports to ascertain that updated QRE and SLI information was published through the Transparency Centre across reporting periods.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 40.3 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
40.4	**Requirement:** Signatories will develop, within the Task-force, harmonised reporting templates. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in the Permanent Task-force to support the implementation and transparency of the Code. As part of this process, Bing participates in Task-force meetings, including plenary sessions and relevant sub-groups, where it contributes to the development of harmonized reporting templates.	1. Performed inquiry with management and inspected evidence to ascertain whether the harmonised reporting template was created and agreed upon in the Task-force. 2. Inspected evidence to ascertain whether any changes were made to the harmonised reporting templates during the audit period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 40.4 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
40.5	**Requirement:** Signatories will regularly work to improve and optimise the monitoring and reporting framework of the Code, including the SLIs, within the Task-force, building in particular on feedback from the European Commission, ERGA and EDMO. **Definitions and Benchmarks:** • **Regularly work to improve:** For purposes of evaluating its Year 1 controls, Bing used attendance to Task-force Plenary and Sub/Working group meetings (as they are relevant to Bing's subscriptions) for the six-month reporting period as a benchmark. Specifically, meeting attendance is used for determining whether Bing is regularly working to improve the monitoring and reporting framework of The Code as they are discussed in European Commission Task-force meetings.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in the Permanent Task-force to support the implementation and transparency of the Code. As part of this process, Bing participates in Task-force meetings, including plenary sessions and relevant sub-groups, where it contributes to the reporting framework of the Code by developing harmonised reporting templates. Additionally, Bing publishes COCD reports in accordance with these templates on a 6-month cadence.	1. Inquired with management and inspected Task-force communications related to the monitoring and reporting framework of the Code, including the harmonised reporting template. 2. Inspected evidence of Bing's attendance at the relevant Task-force plenary and sub- groups meetings, which management uses as its benchmark for regularly working to improve and optimize the Code's monitoring and reporting framework. 3. Inspected policies, procedures, and reporting disclosures to ascertain Bing's process for reviewing and implementing updates to the monitoring and reporting framework of the Code, including SLIs and feedback from the European Commission, ERGA, and EDMO. 4. Performed inquiry with management and inspected evidence to ascertain that there were no changes to the monitoring and reporting framework of the code, nor feedback received from the EC, ERGA, and EDMO during the audit period on the improvement and optimization of the reporting framework of the code.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 40.5 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Measure:	Audit criteria:	Materiality threshold:
40.6	**Requirement:** Signatories will cooperate with the European Commission, respond to its reasonable requests and provide the European Commission with reasonable information, data and further input necessary to assess the implementation of the Code, allowing for the Code's efficient and thorough monitoring, including at Member State level. **Definitions and Benchmarks:** • **Reasonable information:** Details or data that are responsive to the European Commission's requests and readily available with minimal new activity required and not in conflict with corporate commitments and policies (e.g. privacy), to assess the implementation of The Code.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Upon request from the European Commission for reasonable information, data, or input, Bing reviews and responds to requests for information, data, input that would help to assess the implementation of the Code, and would allow for efficient and thorough monitoring of the code at the Member State level.	1. Inspected policies, procedures, and supporting documentation to ascertain Bing's process for cooperating with the European Commission and responding to requests for reasonable information, data, and further input related to the implementation of the Code. 2. Inquired with management and inspected evidence to ascertain where there any information or data requests received from the European Commission pertaining to measure 40.6 during the Examination Period, determining there were no such requests. 3. Inspected the European Commission's websites to corroborate that there were no such requests received during the Examination Period.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Measure 40.6 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 42 COCD - Monitoring of the Code

Commitment:	Audit criteria:	Materiality threshold:
42	**Requirement:** Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Task-force. **Definitions and Benchmarks:** • **Proportionate and appropriate:** Details or data that are responsive to the European Commission's requests and readily available without significant new activity required and not in conflict with key interests in privacy, to assess the implementation of The Code.	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing Search participates in the Code of Conduct Taskforce Rapid Response System (RRS) for special situations, including elections and crises. Where the European Commission identifies a relevant special situation, operational communications are issued to Code signatories setting out the relevant event, reporting timelines and participation requirements. Bing Search participates in RRS-related discussions and communications associated with the identified special situations. Election- and crisis-related information is subsequently disclosed within Bing Search's Transparency Reports where applicable.	1. Inspected communications issued by the European Commission relating to the activation of the Rapid Response System (RRS) for relevant election events and requesting participation from Code signatories in relation to identified special situations. 2. Inspected email correspondence and Microsoft Teams communications relating to multiple election events to ascertain Bing Search's participation in discussions and communications associated with the Rapid Response System during the Examination Period. 3. Inspected communications issued by the European Commission requesting Code signatories to provide election- and crisis-related information for inclusion within the relevant Transparency Report reporting period. 4. Inspected publicly available information on the European Commission website to identify any crisis declarations or other special situations requiring reporting during the Examination Period and compared the results to the election- and crisis-related events communicated by the European Commission for inclusion within the relevant Transparency Report reporting period. 5. Inspected the Bing March 2026 Report to verify that election- and crisis-related information was disclosed within dedicated reporting sections where applicable.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Commitment 42 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Commitment 43 COCD - Monitoring of the Code

Commitment:	Audit criteria:	Materiality threshold:
43	**Requirement:** Signatories commit to produce reports and provide data following the harmonized reporting templates and refined methodology for reporting and data disclosure, as agreed in the Task-force. **Definitions and Benchmarks:** • N/A	Not applicable

Summary of controls, systems, and processes:	Audit procedures:
Bing participates in the Permanent Task-force to support the implementation and transparency of the Code. As part of this process, Bing participates in Task-force meetings, including plenary sessions and relevant sub-groups, where it contributes to the development and refinement of harmonized reporting templates. Bing produces reports and provides data following the harmonized reporting templates, as agreed in the Task-force.	1. Inquired with management and inspected evidence to ascertain that the harmonized reporting template was not changed during the Examination Period. 2. Inspected and compared COCD reports from other signatories to ascertain that Bing produces reports and provides data following the harmonized reporting templates and refined methodology for reporting and data disclosure, as agreed in the Task-force.

Changes to audit procedures during the examination:

No changes

Conclusion:

Positive – In our opinion, Bing complied with Commitment 43 during the Examination Period, in all material respects.

Recommendations on specific measures:	Recommended timeframe to implement specific measures:
Not applicable	Not applicable

Appendix 2 – Obligations that are out of scope (DSA)

Appendix 2 – Obligations that are Out of Scope (DSA)

Section 1	Section 2	Section 3	Section 4	Section 5	Section 6
13.1 - 13.5	16.1 - 16.6	19.1 – 19.2	29.1 – 29.2	33.1 - 33.6	44.1 - 44.2
14.3	17.1 - 17.5	20.1 - 20.6	30.1 - 30.7	35.2 - 35.3	45.1 - 45.4
15.1. b	18.1 - 18.2	21.1 - 21.2	31.1 - 31.3	36.2 - 36.11	46.1 - 46.4
15.3		21.5		37.7	48.1-40.5
		21.6 - 21.8		40.2	
		21.9		40.8 - 40.11	
		22.1 – 22.8		40.13	
		23.1-23.4		42.2	
		24.1		43.1 – 43.7	
		24.4			
		24.5			
		24.6			
		25.1 - 25.3			
		26.1 - 26.3			
		27.1 – 27.3			
		28.1 – 28.3			
		28.4			

Legend

- Responsibility of the regulatory body and not the VLOSE
- Not applicable until the regulatory body takes action
- Based on Microsoft's legal determination, conditions do not exist for the obligation
- Obligations not relevant for VLOSE

Appendix 3 - Template for the audit report referred to in Article 6 of Delegated Regulation

Section A: General information

1. Audited service:
Bing

2. Audited Provider:
Microsoft Ireland Operations Limited

3. Address of the Audited Provider:
One Microsoft Place, South Country Business Park, Leopardstown, Dublin 18, D18 P521

4. Point of contact of the Audited Provider:
[CONFIDENTIAL]

5. Scope of the audit:	
Does the audit report include an assessment of compliance with all the obligations and commitments referred to in Article 37.1 of Regulation (EU) 2022/2065 applicable to the Audited Provider?	Yes

i. Compliance with Regulation (EU) 2022/2065	
Obligations set out in Chapter III of Regulation (EU) 2022/2065:	
Audited obligation	**Period covered**
A listing of the audited obligations can be found in Appendix 1A, Sections 1-6 (Audit Criteria label) in the Independent Accountant's Report – Digital Services Act.	June 1, 2025 to May 31, 2026

ii. Compliance with codes of conduct and crisis protocols	
Commitments undertaken pursuant to codes of conduct referred to in Articles 45 and 46 of Regulation (EU) 2022/2065 and crisis protocols referred to in Article 48 of Regulation (EU) 2022/2065:	
Audited obligation	**Period covered**
Code of Conduct on Disinformation: A listing of audited commitments and measures can be found in Appendix 1B, Sections 1-10 in the Independent Accountant's Report – Code of Conduct on Disinformation.	July 1, 2025 to May 31, 2026

6a. Audit start date:	b. Audit end date:
DSA: January 2026	DSA: August 2026
COCD: April 2026	COCD: August 2026

Section B: Auditing organization

1. Name of organization constituting the auditing organization:

Deloitte & Touche LLP

2. Information about the auditing team of the auditing organization:

[CONFIDENTIAL] was the overall responsible person from Deloitte & Touche LLP (Contact details: 1015 Second Avenue, Suite 500, Seattle, WA 98104; Deloitte DSA Audit <dsaaudit@deloitte.com>). All members of the auditing team were employees of Deloitte & Touche LLP and its affiliates or related entities.

3. Auditors' qualification:

a. Overview of the professional qualifications of the individuals who performed the audit, including domains of expertise, certifications, as applicable:

The auditing team includes certified professionals (Chartered Accountants, Certified Public Accountants, Certified Information Systems Auditors, Certified Information Systems Security Professionals, Health Information Trust Alliance Certified Common Security Framework Practitioners) and individuals experienced in data science and data privacy regulations.

b. Documents attesting that the auditing organization fulfils the requirements laid down in Article 37.3.b of Regulation (EU) 2022/2065 have been attached as an annex to this report:

See "1. Overview of the professional qualifications of the individuals who performed the audit, including domains of expertise, certifications, as applicable:" above.

4. Auditors' independence:

a. Declaration of interests

D&T performs the audit of Microsoft's annual consolidated financial statements, the review of consolidated financial statements included in Microsoft's quarterly Form 10-Q reports, the audit of internal control over financial reporting, and the services that an independent auditor would customarily provide in connection with subsidiary audits, statutory requirements, regulatory filings, and similar engagements for the fiscal year, such as comfort letters, attest services, consents, and assistance with review of documents filed with the U.S. Securities and Exchange Commission (SEC). In coordination with the consolidated financial statements, D&T performs procedures relating to accounting matters that arise in connection with or as a result of the audit or the review of periodic financial statements and statutory audits that non-U.S. jurisdictions require in addition to audits of Microsoft's employee benefit plans; due diligence related to mergers, acquisitions, and investments; additional revenue and license compliance procedures related to the performance of review or audit of Microsoft's consolidated financial statements; third-party assurance audits for cloud services; accounting consultations about the application of GAAP to proposed transactions; tax compliance and return preparation; and tax planning and advice.

b. References to any standards relevant for the auditing team's independence that the auditing organization(s) adheres to:

As stated in the Independent Accountant's Report under "Our independence and quality management" –

We are required to be independent of Microsoft and its subsidiaries and to meet our other ethical responsibilities, as applicable, for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA and other relevant ethical requirements required for our engagement.

We also applied the International Standard on Quality Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements, and the AICPA's quality management standards, which require that we design, implement, and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Furthermore, Appendix 6 includes our attestation that the auditing organization complies with the obligations laid down in Article 37.3, points (a), (b), and (c).

c. List of documents attesting that the auditing organization complies with the obligations laid down in Article 37.3, points (a) and (c) of Regulation (EU) 2022/2065 attached as annexes to this report.

See "2. References to any standards relevant for the auditing team's independence that the auditing organization(s) adheres to:" above.

5. References to any auditing standards applied in the audit, as applicable:

We conducted our examination in accordance with the International Standard for Assurance Engagements Other Than Audits or Reviews of Historical Financial Information ("ISAE 3000 (Revised)"), the attestation standards established by the American Institute of Certified Public Accountants ("AICPA"), Section III and IV of the Commission Delegated Regulation (EU) supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines ("Delegated Regulation") dated October 20, 2023 and the terms of reference for this examination as agreed with Microsoft on February 13, 2026 for DSA and on May 5, 2026 for COCD. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether Bing complied, in all material respects, with the Specified Requirements referenced in the Independent Accountant's Reports.

6. References to any quality management standards the auditing organization adheres to, as applicable:

Deloitte & Touche LLP applies the International Standard on Quality Management I (ISQM 1) and Statements on Quality Control Standards established by the AICPA. Accordingly, we maintain a comprehensive system of quality control/management including documented policies and procedures regarding compliance with ethical requirements, professional, standards, and applicable legal and regulatory requirements.

Furthermore, Deloitte & Touche LLP is a registered audit firm with the Public Company Accounting Oversight Board ("PCAOB") of the United States and is an American Institute of Certified Public Accountants ("AICPA") member firm. As such, Deloitte & Touche LLP complies with the public accounting profession's technical and ethical standards, including the AICPA's Code of Professional Conduct. In addition to the Code of Professional Conduct, the AICPA publishes standards, which delineate specific requirements that Certified Public Accountants are consistently required to follow during the audit. Refer to Deloitte & Touche LLP Transparency Report 2025 for further background.

Section C: Summary of the main findings

1. Summary of the main findings drawn from the audit (pursuant to paragraph 37.4.e of Regulation (EU) 2022/2065)

DSA: A description of the main findings drawn from the audit can be found in Appendix 1A, Sections 1-6 (Conclusion label) of the Independent Accountant's Report – Digital Services Act.

COCD: A description of the main findings drawn from the audit can be found in Appendix 1B, Sections 1-10 (Conclusion label) of the Independent Accountant's Report – Code of Conduct on Disinformation.

SECTION C.1: Compliance with Regulation (EU) 2022/2065

1. **Audit opinion for compliance with the audited obligations referred to in Article 37.1.a of Regulation (EU) 2022/2065:**
   The audit opinion for compliance with the audited obligations set out in Chapter III of Regulation (EU) 2022/2065 can be found under Opinion section in the Independent Accountant's Report – Digital Services Act.
2. **Audit conclusion for each audited obligation:**
   The audit conclusion for each audited obligation can be found in Appendix 1A, Sections 1-6 (Conclusion label) in the Independent Accountant's Report – Digital Services Act.

SECTION C.2: Compliance with voluntary commitments in codes of conduct and crisis protocols

Repeat section C.2 for each audited code of conduct and crisis protocol referred to in Article 37.1.b of Regulation (EU) 2022/2065:

1. **Audit opinion for compliance with the commitments made under specify the code of conduct or crisis protocol covered by the audit:**
   The audit opinion for compliance with the audited commitments and measures referred to in the Code of Conduct on Disinformation can be found under the Opinion section in the Independent Accountant's Report – Code of Conduct on Disinformation.
2. **Audit conclusion for each audited commitment:**
   The audit conclusion for each audited commitment and measure can be found in Appendix 1B, Sections 1-10 (Conclusion label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

SECTION C.3: Where applicable, explanations of the circumstances and the reasons why an audit opinion could not be expressed:

DSA: Not applicable – The auditing organization was able to obtain sufficient appropriate evidence to express an audit opinion – refer to Appendix 1A, Sections 1-6 (Conclusion label) in the Independent Accountant's Report – Digital Services Act.

COCD: Not applicable - The auditing organization was able to obtain sufficient appropriate evidence to express an audit opinion – refer to Appendix 1B, Sections 1-10 (Conclusion label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

Section D: Description of the findings: compliance with Regulation (EU) 2022/2065

D.1: Audit conclusion for obligation (Digital Services Act)

I. Audit conclusion:

A description of the audit conclusion, justification, and remarks for each audited obligation can be found in Appendix 1A, Sections 1-6 (Conclusion label) in the Independent Accountant's Report – Digital Services Act.

If the conclusion is not 'Positive', operational recommendations on specific measures to achieve compliance (where the conclusion is not positive), including an explanation on the materiality of non-compliance and recommended timeframe to achieve compliance, can be found in Appendix 1A, Sections 1-6 (Recommendations on Specific Measures and Materiality Threshold labels) in the Independent Accountant's Report – Digital Services Act.

II. Audit procedures and their results:

1. **Description of the audit criteria and materiality threshold used by the auditing organization pursuant to Article 10.2.a of this Regulation:**
   A description of the audit criteria and materiality thresholds used can be found in Appendix 1A, Sections 1-6 (Audit Criteria and Materiality Threshold labels) in the Independent Accountant's Report – Digital Services Act.

2. **Audit procedures, methodologies, and results:**
   (a) **Description of the audit procedures performed by the auditing organization, the methodologies used to assess compliance, and justification of the choice of those procedures and methodologies (including, where applicable, a justification for the choices of standards, benchmarks, sample size(s) and sampling method(s)):**

   A description of the audit procedures performed, the methodologies used to assess compliance, and a justification of the choice of those procedures and methodologies can be found in Appendix 1A, Sections 1-6 (Audit Criteria label) in the Independent Accountant's Report – Digital Services Act.

   (b) **Description, explanation, and justification of any changes to the audit procedures during the audit:**

   A description, explanation, and justification of any changes to the audit procedures during the audit can be found in Appendix 1A, Sections 1-6 (Changes to Audit Procedures During the Examination label) in the Independent Accountant's Report – Digital Services Act.

   (c) **Results of the audit procedures, including any test and substantive analytical procedures:**

   The results of the audit procedures, including any test and substantive analytical procedures, can be found in Appendix 1A, Sections 1-6 (Audit Criteria and Conclusion label) in the Independent Accountant's Report – Digital Services Act.

3. **Overview and description of information relied upon as audit evidence, including, as applicable:**
   (a) **description of the type of information and its source;**
   (b) **the period(s) when the evidence was collected;**
   (c) **the period the evidence refers to;**
   (d) **any other relevant information and metadata.**

   Audit evidence is no longer presented as a separate column in Appendix 1A beginning with the current Examination Period. The information relied upon as audit evidence, including its nature, source, applicable period, and other relevant details, is documented in the related test procedures, which can be found in Appendix 1A, Sections 1-6 in the Independent Accountant's Report – Digital Services Act, and supporting workpapers.

4. **Explanation of how the reasonable level of assurance was achieved:**
   An explanation of how the reasonable level of assurance was achieved can be found in Appendix 1 - The specific test procedures we performed, along with the nature, timing, and results of those tests.

5. **In cases when**
   (a) a specific element could not be audited, as referred to in Article 37.5 of Regulation (EU) 2022/2065, or
   (b) an audit conclusion could not be reached with a reasonable level of assurance, as referred to in Article 8.8 of this Regulation, provide an explanation of the circumstances and the reasons:

   Not applicable – The auditing organization was able to obtain sufficient appropriate evidence and reached audit conclusions with reasonable level of assurance – refer to Appendix 1A, Sections 1-6 (Conclusion label) in the Independent Accountant's Report – Digital Services Act.

6. **Notable changes to the systems and functionalities audited during the audited period and explanation of how these changes were taken into account in the performance of the audit.**
   On June 2, 2025, Microsoft launched the release of a new product, Bing Video Creator. D&T planned our procedures accordingly to ensure coverage across all in-scope services and features.

7. **Other relevant observations and findings:**
   Please see Appendix 1A, Sections 1-6 (Conclusion label) in the Independent Accountant's Report – Digital Services Act for any other relevant observations and findings.

SECTION D.2: Additional elements pursuant to Article 16 of this Regulation

1. **An analysis of the compliance of the Audited Provider with Article 37.2 of Regulation (EU) 2022/2065 with respect to the current audit:**
   An analysis of the compliance of the Audited Provider with Article 37.2 of Regulation (EU) 2022/2065 with respect to the current audit can be found in Appendix 1A, Section 5 Obligation 37.2 (Audit Criteria and Conclusion labels) in the Independent Accountant's Report – Digital Services Act.

2. **Description of how the auditing organization ensured its objectivity in the situation described in Article 16.3 of this Regulation:**
   An analysis of how the auditing organization ensured its objectivity in the situation described in Article 16.3 of this Regulation can be found in Appendix 6 in the Independent Accountant's Report – Digital Services Act.

Section E: Description of the findings concerning compliance with codes of conduct and crisis protocol

Section E.1: Audit conclusion for commitment (Code of Conduct on Disinformation)

I. Audit conclusion:

A description of the audit conclusion, justification, and remarks for each audited obligation can be found in Appendix 1B, Sections 1-10 (Conclusion column) in the Independent Accountant's Report – Code of Conduct on Disinformation.

If the conclusion is not 'Positive', operational recommendations on specific measures to achieve compliance (where the conclusion is not positive), including an explanation on the materiality of non-compliance and recommended timeframe to achieve compliance, can be found in Appendix 1B, Sections 1-10 (Recommendations on Specific Measures label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

II. Audit procedures and their results:

1. **Description of the audit criteria and materiality threshold used by the auditing organization pursuant to Article 10.2, point (a) of this Regulation:**

   A description of the audit criteria and materiality thresholds used can be found in Appendix 1B, Sections 1-10 (Audit Criteria and Materiality Threshold labels) in the Independent Accountant's Report – Code of Conduct on Disinformation.

2. **Audit procedures, methodologies, and results:**

   (a) **Description of the audit procedures performed by the auditing organization, the methodologies used to assess compliance, and justification of the choice of those procedures and methodologies (including, where applicable, a justification for the choices of standards, benchmarks, sample size(s) and sampling method(s)):**

   A description of the audit procedures performed, the methodologies used to assess compliance, and a justification of the choice of those procedures and methodologies can be found in Appendix 1B, Sections 1-10 (Audit Criteria label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

   (b) **Description, explanation, and justification of any changes to the audit procedures during the audit:**

   A description, explanation, and justification of any changes to the audit procedures during the audit can be found in Appendix 1B, Sections 1-10 (Changes to Audit Procedures During the Examination label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

   (c) **Results of the audit procedures, including any test and substantive analytical procedures:**

   The results of the audit procedures, including any test and substantive analytical procedures, can be found in Appendix 1B, Sections 1-10 (Audit Criteria and Conclusion label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

3. **Overview and description of information relied upon as audit evidence, including, as applicable:**

   (a) **description of the type of information and its source;**

   (b) **the period(s) when the evidence was collected;**

   (c) **the period the evidence refers to;**

   (d) **any other relevant information and metadata.**

   Audit evidence is no longer presented as a separate column in Appendix 1A beginning with the current Examination Period. The information relied upon as audit evidence, including its nature, source, applicable period, and other relevant details, is documented in the related test procedures, which can be found in Appendix 1B, Sections 1-10 in the Independent Accountant's Report – Code of Conduct on Disinformation, and supporting workpapers.

4. **Explanation of how the reasonable level of assurance was achieved:**
   An explanation of how the reasonable level of assurance was achieved can be found in Appendix 1 - The specific test procedures we performed, along with the nature, timing, and results of those tests.

5. **In cases when:**
   (a) a specific element could not be audited, as referred to in Article 37.5 of Regulation (EU) 2022/2065, or
   (b) an audit conclusion could not be reached with a reasonable level of assurance, as referred to in Article 8.8 of this Regulation, provide an explanation of the circumstances and the reasons:

   Not applicable – The auditing organization was able to obtain sufficient appropriate evidence and reached audit conclusions with reasonable level of assurance – refer to Appendix 1B, Sections 1-10 (Conclusion label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

6. **Notable changes to the systems and functionalities audited during the audited period and explanation of how these changes were taken into account in the performance of the audit.**
   No notable changes to the systems or functionalities subject to audit occurred during the audited period.

7. **Other relevant observations and findings:**
   Please see Appendix 1B, Sections 1-10 (Conclusion label) in the Independent Accountant's Report – Code of Conduct on Disinformation for any other relevant observations and findings.

Section F: Third parties consulted

Not applicable because D&T did not engage or consult with any third parties on any auditing matters throughout the DSA Examination Period from June 1, 2025 to May 31, 2026, or throughout the COCD Examination Period from July 1, 2025 to May 31, 2026.

Section G: Any other information the auditing body wishes to include in the audit report (such as a description of possible inherent limitations)

Please refer to the Independent Accountant's report for additional information.

Date	August 25, 2026	**Signed by**	[CONFIDENTIAL]
Place	1015 Second Avenue, Suite 500, Seattle, WA 98104	**In the name of**	Deloitte & Touche LLP
		Responsible for:	2026 Microsoft Bing Digital Services Act (DSA) Report 2026 Microsoft Bing Code of Conduct on Disinformation (COCD) Report

Appendix 4A – Written agreement between VLOSE and the auditing organization (DSA)

Written agreement between VLOSE and the auditing organization (DSA)

The following pages contain the written agreement between the VLOSE and the auditing organization. Additionally, refer to Appendix 1A for the exhaustive list of audited obligations for DSA, respectively.

Statement of Work
("SOW")

Addresses and contacts for notices

"Microsoft"	"Supplier"
Company Name: Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries	Company Name: Deloitte & Touche LLP
Primary Contact: [CONFIDENTIAL]	Primary Contact: [CONFIDENTIAL]
Address: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Address: 1015 Second Avenue, Suite 500 Seattle, WA 98104
Phone number: N/A	Phone number: [CONFIDENTIAL]
Fax number: N/A	Fax number: [CONFIDENTIAL]
Email (if applicable): [CONFIDENTIAL]	Email (if applicable): [CONFIDENTIAL]
Secondary Contact:	Secondary Contact:
	Microsoft Supplier Number: 1100000

SOW Effective Date:	January 19, 2026
SOW Expiration Date:	October 31, 2026
DealPoint # for Master Agreement	
Budget ID#	

Agreed and accepted

Microsoft, on behalf of itself and its subsidiaries		Supplier
Microsoft Signature: [CONFIDENTIAL]	Microsoft Signature:	Supplier Signature: [CONFIDENTIAL]
Microsoft Name: [CONFIDENTIAL]	Microsoft Name:	Supplier Name: [CONFIDENTIAL]
Microsoft Title: [CONFIDENTIAL]	Microsoft Title:	Supplier Title: [CONFIDENTIAL]
Microsoft Date: 13- Feb-2026 | 4:17:23 PM ET	Microsoft Date:	Supplier Date: 13- Feb-2026 | 2:29:37 PM EST

☒ This SOW (together with the attached appendices, the "Agreement") dated as of January 19, 2026 between Microsoft and the Supplier is entered into by the parties and is effective as of the SOW Effective Date above.

☐ This SOW pursuant to the Microsoft Purchase Order Terms and Conditions is entered into by the parties and effective as of the SOW Effective Date above.

SECTION 1 Purpose

The purpose of this SOW is to set forth the specific services that the Supplier will provide to Microsoft.

SECTION 2 Description of Services and Delivery Schedule

(a) Description of Services. Section 2(b) (Services) describes the details of the independent accountant's examination services, including project expectations and the Supplier activities, the Supplier will perform or deliver to Microsoft under this SOW (collectively, the "Services").

(b) Services. Deloitte & Touche LLP ("D&T" or "we" or "us" or "Supplier") is pleased to serve as independent accountants for Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries (together referred to as "Microsoft" ; the "Company" or "you" or "your") to perform an examination of management of the Company's assertion regarding Microsoft Bing, being designated as a Very Large Online Search Engine (VLOSE) under the Digital Services Act ("DSA" or "Regulation (EU) 2022/2065")[1], service's compliance with the obligations set out in Chapter III of the DSA; for the period June 1, 2025 to May 31, 2026 (the "subject matter") presented in accordance with the criteria defined in Appendix E ("the Criteria") (collectively, "management's assertion"). [CONFIDENTIAL] will be responsible for the services that we perform for the Company hereunder. For purposes of Sections 9, 10 and 11, "Supplier" will mean Deloitte & Touche LLP and its subsidiaries; Deloitte Touche Tohmatsu Limited, its member firms, the affiliates of Deloitte & Touche LLP, Deloitte Touche Tohmatsu Limited and its member firms; and, in all cases, any successor or assignee. Microsoft Ireland Operations Limited represents and warrants that it has the power and authority to execute this agreement on behalf of, and to bind, itself, its affiliates, and its subsidiaries hereto.

(1) Examination of Management's Assertion and the Subject Matter.

Our engagement is to perform an examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) (the "AICPA attestation standards") and International Standard on Assurance Engagements 3000 (Revised) Assurance Engagements Other than Audits or Reviews of Historical Financial Information issued by the International Auditing and Assurance Standards Board (the "ISAE standards"). The objective of an examination conducted in accordance with the AICPA attestation standards and ISAE standards is to:

1. Obtain reasonable assurance about whether the subject matter as measured or evaluated against the Criteria is free from material misstatement.
2. Express an opinion in the form of a written report about whether management's assertion is fairly stated, in all material respects.

An examination includes examining, on a test basis, evidence supporting management's assertion and the subject matter and performing such other procedures as the Supplier considers necessary in the circumstances. An examination conducted in accordance with the AICPA attestation standards and ISAE standards is designed to obtain reasonable, rather than absolute, assurance about management's assertion and the subject matter taken as a whole. Because of the inherent limitations of an examination engagement, together with the inherent limitations of internal control, an unavoidable risk exists that some material misstatements may not be detected, even though the examination is properly planned and performed in accordance with the AICPA attestation standards and ISAE standards.

These professional standards require us to establish whether the required preconditions for an assurance engagement are present. This is based on our preliminary knowledge of the engagement circumstances and discussion with the appropriate parties. If we discover after the engagement has been accepted that one or more preconditions for the services is not present, we will discuss the matter with you and determine whether the matter can be resolved to our satisfaction, whether it is appropriate for us to continue with the engagement and, if so, how to communicate the matter in the report.

(2) Report on Management's Assertion and the Subject Matter.

We expect to issue a written report upon the completion of our examination. Our ability to express any opinion or to issue any report as a result of this engagement and the wording thereof, will, of

[1] The Digital Services Act (DSA) establishes a set of narrowly defined objective criteria to prevent illegal and harmful activities online and the spread of disinformation through VLOP.

course, be dependent on the facts and circumstances at the date of our report. If, for any reason, we are unable to complete our examination or are unable to form, or have not formed, any opinion, we may decline to express any opinion or decline to issue any report as a result of this engagement. If we are unable to complete our examination or if any report to be issued by the Supplier as a result of this engagement requires modification, the reasons for this will be discussed with management.

(c) Locations. Services will be performed remotely and at the following location(s):

Facility	Address
Onsite: Microsoft Redmond Campus	One Microsoft Way Redmond, WA 98052

(d) Hours of Operation. The Supplier will provide Services M-F 8-5 PST. However, the Supplier will operate additional hours as necessary.

(e) Reporting requirements. The Supplier will endeavor to provide the following reports to the Company according to the schedule indicated below.

Report description	Schedule (Anticipated)	Format
Weekly status reports*	February 2026 – August 2026	Excel/PDF
Monthly expense reports*	February 2026 – August 2026	Excel/PDF
Assurance report on the Company's compliance with DSA	August 25, 2026	PDF

* Weekly status updates showing status of walkthroughs, data requests, test execution, and exceptions organized by the Company's DSA requirements.

(f) Deliverables / Delivery Schedule. Subject to the terms hereof, the Supplier will endeavor to complete and deliver all Services to the Company on or before August 25, 2026. The milestone delivery schedule for the Services, if applicable, will be as follows:

Milestone #	Brief Description of Services to be completed by Supplier and delivered to the Company	Estimated Due on or Before
1	Plan examination, including review of draft control matrix and preparation of test plans	January - February 2026
2	Start examination, including walkthroughs of controls and examining evidence	March – May 2026
3	Perform design effectiveness testing	March – May 2026
4	Perform operating effectiveness testing	April – June 2026
5	Provide a draft report to the management	June 2026
6	Issue final report and perform examination wrap-up	July – October 2026

In addition to the deliverables listed above, the Supplier will conduct weekly status meetings with management starting in March 2026.

(1) Inclusion of Supplier Reports or References to Supplier in Other Documents or Electronic Sites.

Nothing in this engagement letter is intended to restrict the ability of the Company to distribute to other parties any of our reports issued hereunder unedited and, in its entirety. In connection with such distribution, to the extent the Company needs to describe the services hereunder or describe any report issued hereunder, the Company agrees only to use the description provided within the applicable report, unedited and in its entirety. Except as described above, if the Company intends to publish or otherwise reproduce in any document any report issued as a result of this engagement, or otherwise make reference to the Supplier in a document that contains other information in addition to management's assertion and the subject matter (e.g., in a periodic filing with a regulator), thereby associating the Supplier with such document, in both instances the Company agrees that its management will provide the Supplier with a draft of

the document to read and obtain our approval for the inclusion or incorporation by reference of any of our reports, or the reference to the Supplier, in such document before the document is printed and distributed. The inclusion or incorporation by reference of any of our reports in any such document would constitute the reissuance of such reports. Except as otherwise required by the European Commission, the Company also agrees that its management will notify us and obtain our approval prior to including any of our reports on an electronic site. For purposes of this paragraph, the Supplier's approval shall be based upon professional standards and facts and circumstances at the time of the request.

Our engagement to perform the services described herein does not constitute our agreement to be associated with any such documents published or reproduced by or on behalf of the Company. Any request by the Company to reissue any report issued as a result of this engagement, to consent to or acknowledge our awareness of any such report's inclusion or incorporation by reference in another document, or to agree to any such report's inclusion on an electronic site will be considered based on the facts and circumstances existing at the time of such request. The estimated fees outlined herein do not include any procedures that would need to be performed in connection with any such request. Should the Supplier agree to perform such procedures, fees for such procedures would be subject to the mutual agreement of the Company and the Supplier.

SECTION 3 Payment

(a) Service fees. The Company will pay Supplier a total fee not to exceed [CONFIDENTIAL] according to the milestone payment schedule below as full and final payment for the Services. The Company will only make payment for Services that Supplier has completed and delivered to the Company, and that the Company has accepted in accordance with the terms of Section 2(c).

Milestone #	Not to exceed payment amount	Delivery/payment date
1	[CONFIDENTIAL]	February 1, 2026
2, 3	[CONFIDENTIAL]	March 1, 2026
2, 3, 4	[CONFIDENTIAL]	April 1, 2026
2, 3, 4	[CONFIDENTIAL]	May 1, 2026
4	[CONFIDENTIAL]	June 1, 2026
5	[CONFIDENTIAL]	July 1, 2026
6	[CONFIDENTIAL]	August 1, 2026
Sub-total	[CONFIDENTIAL]	**-**
Estimated expenses maximum (if agreed to – see Section 3(b)(Expenses), below)	[CONFIDENTIAL]	Expense must be listed separately on any invoices submitted by the Supplier to allow for appropriate visibility.
Total	[CONFIDENTIAL]	-

(b) Expenses. As reflected in Section 3(a) (Services fees), above, the Company will reimburse the Supplier for the actual expenses that Supplier incurs while performing the Service up to a total not to exceed the amount of [CONFIDENTIAL]. The expense must comply with the Company policy. The expenses must also be reasonable and related to the Services. The Supplier must submit appropriate documentation evidencing the expenses to be reimbursed.

(c) Payment of Invoices. [CONFIDENTIAL]

(d) Relationship of the Parties. The Supplier is responsible for and will pay all wages, fringe benefits, payroll taxes, insurance, work schedules, and work conditions with respect to its employees, contractors or other resources performing Services under this SOW.

Each party shall comply with all economic sanctions, export control, and import laws and regulations applicable to it in connection with this engagement letter. The parties recognize that such laws and regulations restrict the export and reexport of the Services to jurisdictions subject to territorial U.S. economic sanctions (currently Crimea, Cuba, Iran, North Korea, Russia, Syria, and the Donetsk and Luhansk National People's Republics in Ukraine).

(e) Compliance with Trade Laws

The parties acknowledge that the Services and Deliverables ("Items") may be subject to applicable trade laws in one or more countries and that the Services may not be exported to Russia or any countries subject to comprehensive sanctions, except in compliance with applicable law. The parties will comply with all relevant laws and regulations applicable to the import or export of the Items, including but not limited to, trade laws such as the U.S. Export Administration Regulations or other end-user, end use, and destination restrictions by the U.S. and other governments, as well as sanctions regulations administered by the U.S. Office of Foreign Assets Control ("Trade Laws"). Either party may suspend or terminate the Agreement immediately to the extent that such party reasonably concludes that continued performance would violate Trade Laws or put it at risk of becoming subject to sanctions or penalties under Trade Laws.

SECTION 4 Term and Termination

(a) **Term**. Unless terminated sooner in accordance with its terms, this SOW will terminate on the completion of the Services.

(b) **Early termination**. This SOW may be terminated by the Company, without cause, at any time by giving written notice to the Supplier not less than thirty (30) days before the effective date of termination, or immediately upon written notice in the event the Supplier notifies the Company of a Conflict under Section 12(d) below. This SOW may be terminated by either party, for cause, at any time by giving written notice to the other party. Either party may also terminate this SOW or performance of any part of the Services, upon written notice to the other party, if it reasonably determines that the performance of any part of the Services would be in conflict with law, or independence or professional rules.

SECTION 5 Additional Obligations

(a) **Staffing requirements.** The Supplier will determine all resource requirements needed to remain in compliance with standards defined within this SOW. The Supplier will be responsible for training its own employees. Training will include, but not be limited to, keeping staff informed of new technology, Microsoft account processes, procedures, standards, customer service, and quality. The Supplier's staff performing Services as outlined in this SOW will keep current on technology, governmental and/or regulatory agencies' guidelines, codes, standards, and regulations for products, methods, and techniques, as appropriate. The Company will provide training to the Supplier's team lead for all technologies and tools that are not commercially available to the Supplier.

(b) **Skillset requirements.** The Supplier will be a Certified Public Accounting firm with the ability to issue the report on management's assertion and the subject matter in addition to the following skills:

(1) Significant experience issuing IT-related reports

(2) Strong project management capabilities

(3) Ability to work flexibly to achieve results within the dynamic Company environment

(4) Excellent interpersonal and task-management skills

(5) Strong written and verbal communication skills

(6) Relevant risk and regulatory knowledge

(c) **Roles and responsibilities.**

Company	Supplier
The Company will provide the Supplier access to the following applications/tools/materials required to perform Services under this SOW: • Exchange • SharePoint • Azure DevOps • Additional tools as necessary	Supplier will provide all Supplier resources with the applications/tools/materials required to perform Services under this SOW, including the following: • MS Office Suite • MS Outlook • MS Word • MS Excel • MS PowerPoint
Responsiveness of the Company team members to the Supplier requests and issues is anticipated to be within reason so delivery schedules are not adversely impacted. If issues do arise, the Supplier will escalate to management according to a mutually agreed upon escalation process.	[CONFIDENTIAL] will be the Engagement Leader and will be responsible for the Supplier's independent auditor's examination, while [CONFIDENTIAL] will continue to coordinate all services we perform for the Company. [CONFIDENTIAL] will serve as the practitioner in charge and will be responsible for directing the day-to-day activities of the Supplier's examination.

(d) **Software and materials.** The Supplier will provide each resource with a laptop (onsite with Supplier-owned licenses for commercially available Company Software described in Section

5(c)). The Company will provide the additional required software, licenses and access to applications required to carry out the Services, also described in Section 5(c). The Company-provided software and applications will be uninstalled/returned to the Company upon completion/expiration/termination of the Services provided under this SOW. The Supplier will be responsible for providing all other software, facilities, tools, and equipment not otherwise described herein.

(e) Additional assumptions. The following assumptions and dependencies are associated with the planning and execution of the Services under this SOW. Specifically, for this SOW, its success will depend on the following:

(1) Supplier will have the ability to understand the Company's approach and model for the requested services.

(2) Supplier will be able to effectively communicate with onshore team(s), if applicable

(3) Supplier will maintain an open communication environment.

(4) Supplier, its employees, and Subcontractor(s), if any, will be required to keep secure all Company products, mail, and equipment in accordance with the obligations set forth in Section 12 clause c.

(5) Supplier will assume the risk of the loss of any Company equipment, or materials while in the care, custody, or control of the Supplier's employees. Supplier's employees will not use the Company facilities and/or any Company equipment, products, or materials to perform Services for any person or entity other than the Company.

(6) All Supplier resources will have valid work permits and necessary visa to work in the United States.

(7) Supplier team resources will have the following access if the Company determines such access is relevant to the Services:

i. Access to the Company engagement management to review priorities, steer the engagement, attend status meetings, and approve project Deliverables;

ii. Access to all engagement documentation, including, but not limited to, standard operating procedures;

iii. Access to information around any issues with applications/projects; and

iv. Supplier will resolve all access and connectivity issues within five business days from the start date; at that time, all Supplier resources will have necessary access to all required resources.

(8) The Company will assign a project manager who will be responsible for:

i. Coordinating interview meetings/walkthroughs with control owners as required

ii. Providing required access to the Supplier personnel involved in this engagement

iii. Assisting in data gathering requests

iv. Overseeing the engagement, working side-by-side with the Supplier and handling escalation of issues and engagement risks to the Company management

(9) The Company will support evidence requests and inquiries as needed by the Supplier to enable their assessments and testing.

(10) To facilitate the collection of data needed for testing, Supplier will work with the Company project manager and supporting Company personnel to provide test procedures and data request lists as early in the project as possible.

(11) To facilitate the scheduling of Company control performers, the Supplier will provide interview request lists and proposed meeting agendas as early in the engagement as possible.

SECTION 6 SOW Changes

Unless specifically described otherwise in this SOW, changes to this SOW will be as follows:

(a) Approved minor or non-substantive changes will be memorialized in writing using the Change Order Form attached as Appendix C. The Change Order Form will become an attachment to and part of this SOW after both parties have signed it.

(b) Substantive or major changes will be addressed in a SOW Amendment.

SECTION 7 Definition of Management's Responsibilities

Appendix A describes management's responsibilities.

SECTION 8 Limitations of an Entity's Internal Control

Because of the inherent limitations of internal control, including the possibility of collusion or improper management override of controls, material misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

SECTION 9 Audit Committee's Responsibility

The Supplier acknowledges that the Audit Committee is directly responsible for the appointment, compensation, and oversight of the Supplier's work and, accordingly, except as otherwise specifically noted, the Supplier will report directly to the Audit Committee. The Company has advised the Supplier that the Services to be performed under this SOW, including, where applicable, the use by the Supplier of affiliates or related entities as subcontractors in connection with this SOW, have been approved by the Audit Committee in accordance with the Audit Committee's established preapproval policies and procedures.

Process for Obtaining Preapproval of Services: The Company's management is responsible for the coordination of obtaining the preapproval of the Audit Committee, in accordance with the Audit Committee's preapproval process, for any services to be provided by the Supplier to the Company.

SECTION 10 Independence Matters Relating to Certain Services

In connection with the Supplier's engagement, the Supplier, the Company's management, and the Audit Committee will assume certain roles and responsibilities in an effort to assist the Supplier in maintaining independence and ensuring compliance with the securities laws and regulations. The Supplier will communicate to its partners, principals, and employees that the Company is an attest client. Management of the Company will ensure that the Company has policies and procedures in place for the purpose of ensuring that the Company will not act to engage the Supplier or accept from the Supplier any service that either has not been subjected to their preapproval process or that under SEC or other applicable rules would impair the Supplier's independence. All potential services are to be discussed with [CONFIDENTIAL], Lead Client Service Partner.

SECTION 11 Independence Matters Relating to Hiring

The Company's management will coordinate with the Supplier to ensure that the Supplier's independence is not impaired by hiring former or current partners, principals, or professional employees of the Supplier for certain positions. Management of the Company will ensure that the Company also has policies and procedures in place for purposes of ensuring that the Supplier's independence will not be impaired by hiring a former or current partner, principal, or professional employee of the Supplier in an accounting role or financial reporting oversight role that would cause a violation of securities laws and regulations. Any employment opportunities with the Company for a former or current partner, principal, or professional employee of the Supplier should be discussed with [CONFIDENTIAL] before entering into substantive employment conversations with the former or current partner, principal, or professional employee of the Supplier, if such opportunity relates to serving (1) as chief executive officer, controller, chief financial officer, chief accounting officer, or any equivalent position for the Company; (2) on the Company's board of directors; (3) as a member of the Audit Committee; or (4) in any other position that would cause a violation of securities laws and regulations.

SECTION 12 General Business Terms

(a) Force majeure. Neither party will be liable or deemed in breach for failure to perform any obligation under this SOW to the extent such failure is caused by a force majeure event (including, without limitation, acts of God, natural disasters, war, civil disturbance, action by governmental entity, strike, and other causes beyond the party's reasonable control). The party affected by the force majeure event will provide notice to the other party within a commercially reasonable time and will use its commercially reasonable efforts to resume performance

promptly after the end of the force majeure event. Obligations not performed due to a force majeure event will be performed as soon as reasonably possible when the force majeure event concludes.

(b) Relationship. The parties are independent contractors. This SOW does not create an exclusive relationship between the parties. The Supplier's employees and subcontractors are not Company employees. The Supplier agrees to discuss and provide the Company with reasonable non-confidential proof of independent contractor status of entities that are not affiliates or related entities of the Supplier upon request.

(c) Confidentiality and Protection of Personal Information.

i. Confidential Information. At all times during the Term, and for five years thereafter, to the extent that in connection with this engagement the Supplier comes into possession of any Company Confidential Information, the Supplier will hold in strictest confidence using at least the same degree of care as it employs in maintaining in confidence its own confidential information, but in no event less than a reasonable degree of care, and will not use or disclose to any third party, any Company Confidential Information except as set forth herein. The Supplier may disclose such information 1) to its subcontractors, whether located within or outside the United States, that are providing services in connection with this engagement and who have agreed to be bound by confidentiality obligations similar to those in this section; 2) as required by law, rule, regulation, applicable professional standards, judicial or regulatory process, to respond to governmental inquiries or in connection with litigation or arbitration relating hereto. The term "*Company Confidential Information*" means all non-public information that the Company designates, either in writing or orally, as being confidential, or which, under the circumstances of disclosure ought to be treated as confidential. The Company Confidential Information includes information relating to:

1. Released or unreleased Company software or hardware products;

2. Company source code;

3. Marketing or promotion of any Company product;

4. Business policies or practices of Company;

5. Customers or suppliers of Company;

6. Information received from others that Company is obligated to treat as confidential;

7. The existence and terms of this Agreement; and

8. Information provided by Company under this Agreement or obtained or created by Supplier in the course of providing the Services, including:

a. Information contained in any reports provided to Company;

b. Any electronic or written correspondence between the parties;

c. Company customer lists, customer information and Personal Information, regardless of the source; and

d. Transactional, sales and marketing information related to the Services.

If the Supplier has any questions as to what comprises Company Confidential Information, the Supplier will consult with Company. Company Confidential Information does not include information that was or becomes known to the Supplier on a non-confidential basis from a third party that the Supplier reasonably believes is not prohibited from disclosing such information to the Supplier by obligation to Company, was known to the Supplier prior to Company's disclosure to the Supplier hereunder, or information that becomes publicly available through no fault of the Supplier in breach hereof.

ii. Security procedures. The Supplier will employ security procedures designed to prevent disclosure of Company Confidential Information (including Personal Information) to unauthorized third parties. The Supplier's security procedures must include risk assessment and controls for:

1. System access;

2. System and application development and maintenance;

3. Change management;

4. Asset classification and control;
5. Incident response, physical and environmental security;
6. Disaster recovery/business continuity; and
7. Employee training.

(d) Privacy and data protection.

i. The Supplier will comply with the privacy and data protection requirements in Appendix D.

(e) Press Releases/Publicity. Except as may be required by law or applicable professional standards, neither party shall issue press releases, public statements or publicity that relates to this Agreement, without the prior written consent or approval of the other. Supplier shall not use the name "Microsoft" or "Microsoft Ireland Operations Limited" in any brochures, advertisements or websites and the Company shall not use the name "Deloitte & Touche" or "Deloitte" in any brochures, advertisements or websites, in such cases as an endorsement or recommendation of a party or its services. Supplier may, however, with the prior written consent of the Company, use the name "Microsoft Ireland Operations Limited" in client presentations and/or in written response to requests for client lists as part of the Request for Proposals, Requests for Information, etc.

(f) Compliance with 201 CMR 17.00. To the extent that any information obtained by the Supplier from or on behalf of the Company or its employees in connection with the performance of services under the statement of work relates to a resident of Massachusetts and constitutes "Personal Information" as defined in 201 CMR 17.02 (as may be amended), the Supplier shall comply with the obligations of 201 CMR 17.00 et. Seq. (as may be amended), entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth," with respect to such information.

(g) Third Party Information Technology Controls Report. Deloitte LLP ("DLLP"), the parent entity of the Supplier, has engaged a third party (the "Service Provider") to conduct an examination in accordance with Service Organization Controls 2 ("SOC 2") standards under the Statement on Standards for Attestation Engagements established by the American Institute of Certified Public Accountants to evaluate the description, suitability of the design, and the operating effectiveness of the security controls of DLLP's Infrastructure Support Services System relevant to security and availability, and to prepare a SOC 2 Type 2 report with respect thereto (the "SOC 2 Infrastructure Report"). Upon written request, the Supplier shall promptly provide the Company with a copy of the most recently available SOC 2 Infrastructure Report. The Company shall not disclose such report, or refer thereto in any communication, to any other person or entity. In the event the Company has any questions regarding such report, the Supplier shall make appropriate personnel reasonably available to discuss the contents thereof.

(h) Conflict of Interest. The Company acknowledges that the Supplier is providing a wide range of services for a large number of clients and may be in a position where it is providing services to companies and organizations which may present actual or potential conflict of interest. The Supplier shall establish commercially reasonably procedures to identify such situations. The Supplier will notify the Company of an actual conflict of interest and the parties will discuss appropriate next steps. The Company shall have the right to terminate this SOW in accordance with Section 4(b) above. The Supplier will neither use Company's Confidential Information obtained hereunder for the advantage of a third party, nor will it use confidential information obtained from any other party for the Company's advantage hereunder.

(i) Survival, Interpretation, and Severability. All provisions which are intended by their nature to survive performance of the Services will survive such performance, or the expiration or termination of this SOW. Each of the provisions of these terms will apply to the fullest extent of the law, whether in contract, statute, tort (such as negligence), or otherwise, notwithstanding the failure of the essential purpose of any remedy. Affiliated and related entities are intended third-party beneficiaries of the terms in this SOW, and may in their own right enforce such terms. If any term of this SOW, including its appendices, is determined to be invalid or unenforceable, such term will not affect the other terms hereof or thereof, but such invalid or unenforceable term will be deemed modified to the extent necessary to render it enforceable, preserving to the fullest extent permissible the intent of the parties set forth herein and therein.

(j) Assignment and Subcontracting. Except as provided below, neither party may assign, transfer, or delegate any of its rights or obligations hereunder (including, without limitation,

interests or Claims). Notwithstanding the foregoing, the Company hereby consents to the Supplier subcontracting any portion of the Services to any affiliate or related entity, whether located within or outside of the United States. Services performed hereunder by the Supplier's subcontractors will be invoiced as professional fees on the same basis as Services performed by the Supplier's personnel, unless otherwise agreed. The Supplier agrees that it will remain responsible to the Company for the Services performed by its subcontractors (including its affiliates and related entities that are acting as subcontractors hereunder) under this SOW to the same extent that the Supplier would be responsible to the Company if it had performed such Services. The parties may only agree to the use of subcontractors, other than the Supplier's affiliates or related entities, by written amendment to this SOW and these terms.

(k) Dispute Resolution. Any controversy or claim between the parties arising out of or relating to the engagement letter or this engagement (a "Dispute") shall be resolved by mediation or binding arbitration as set forth in the Dispute Resolution Provision attached hereto as Appendix B and made a part hereof.

(l) Governing law; Jurisdiction. The laws of the State of Washington govern this SOW. If either the Company or the Supplier employs attorneys to enforce any rights arising out of or relating to this Agreement, the prevailing party will be entitled to seek recovery of its reasonable attorneys' fees, costs, and other expenses, including the costs and fees incurred on appeal or in a bankruptcy or similar action.

(m) Entire Agreement, Amendment, and Notices. These terms, and the Statement of Work, including exhibits and appendices attached, constitute the entire agreement between the parties with respect to this engagement; supersede all other oral and written representations, understandings, or agreements relating to this engagement; and may not be amended except by written agreement signed by the parties. In the event of any conflict, ambiguity, or inconsistency between these terms and the Statement of Work, these terms will govern and control followed by the Statement of Work and then the appendices. All notices hereunder will be (a) in writing, (b) delivered to the representatives of the parties at the addresses first set forth above, unless changed by either party by notice to the other party, and (c) effective upon receipt.

APPENDIX A

This Appendix A is part of the engagement letter dated January 19, 2026 between Deloitte & Touche LLP and Microsoft.

MANAGEMENT'S RESPONSIBILITIES

Management's Assertion and the Subject Matter

Management is responsible for the preparation, presentation, and overall accuracy of management's assertion and the subject matter and its conformity with the Criteria. In this regard, management has the responsibility for, among other things:

(a) Our assertion related to the design, implementation, and maintenance of our systems and processes in place to comply with the Act and our compliance with the Specified Requirements.

(b) Establishing and maintaining effective internal control over compliance.

(c) Determining the applicability of all obligations and each obligation in the Act during the Examination Period, selecting the Specified Requirements, making interpretations of any compliance requirements that have varying interpretations, and developing benchmarks, as needed, to implement the Specified Requirements.

(d) Evaluating and monitoring with our compliance with the Specified Requirements and having reasonable basis for our Assertion. We have performed an evaluation of our compliance with the Specified Requirements.

(e) Preparing and submitting ANNEX II - Template for the audit implementation report referred to in Article 6 of the Delegated Regulation, and ensuring completeness, accuracy, and presentation of the ANNEX II. The content of ANNEX II is beyond the scope of the examination engagement.

(f) Designing, implementing, and maintaining internal control over information relevant to the preparation of the Transparency Report, required under Articles 15, 24, and 42, that is free from material misstatement, whether due to fraud or error.

(g) Determining the Criteria are suitable, will be available to the intended users, and are appropriate for the purpose of the engagement.

(h) We have disclosed any Subsequent Events to the period covered after the period end of the report, May 31, 2026, until the opinion date of your Examination Report, that could have a significant effect on the Subject Matter. We understand that you have no responsibility to perform any procedures regarding the Subject Matter after the date of your Examination Report. However, if after the date of your Examination Report, a material event happens or a fact becomes known to us that, if it had been known to you, may have caused you to have amended your report, then we will disclose this matter to you.

Management's Representations

We will make specific inquiries of management about the representations embodied in management's assertion and the subject matter. In addition, we will request that management provide us with the written representations the Company is required to provide to its independent accountants under the AICPA attestation standards and ISAE standards. The responses to those inquiries and the written representations of management are part of the evidential matter that the Supplier will rely on in forming its opinion on management's assertion and the subject matter.

We confirm, to the best of our knowledge and belief, the following representations made to you during your examination engagement:

(a) We have provided you with all information relevant to the engagement and access as agreed to in the terms of the engagement and reflected all relevant matters in the measurement or evaluation of the Subject Matter.

(b) We have measured or evaluated the Subject Matter against the applicable criteria, including that all relevant matters are reflected in the Subject Matter.

(c) All known matters contradicting the Subject Matter, including any communication from regulatory agencies or others contradicting the Subject Matter, have been disclosed to you, including communications received between the end of the period addressed in the written assertion period ended May 31, 2026, and the date of the practitioner's report.

(d) We have disclosed to you all deficiencies in internal control relevant to the engagement of which we are aware.

(e) We are not aware of any actual, suspected, or alleged fraud affecting the Subject Matter.

(f) We have disclosed any known noncompliance with the Specified Requirements occurring during and subsequent to the period of June 1, 2025 through May 31, 2026.

(g) We are not aware of any cybersecurity incidents that could lead to noncompliance with the Specified Requirements.

(h) We believe that significant assumptions used in our legal determinations are reasonable and have been consistently applied to the Subject Matter. These legal determinations include the scoping of obligations that are subject to the examination.

(i) We acknowledge that the scope of the examination engagement was limited to the subject matter and assertion. All other information presented within the subject matter, including any information relating to periods prior to the beginning period of the examination of June 1, 2025, and post the examination period May 31, 2026, and accordingly, you do not express an opinion or any form of assurance on such information.

(j) We are responsible for the selection or establishment of the Criteria, along with defining terms, benchmarks and other clarifying information, which we believe provide an objective basis for reporting the description of the systems and processes implemented to comply with Regulation (EU) 2022/2065 of the European Parliament and of the Council.

(k) We have responded fully and truthfully to all inquiries made to us by you during your examination engagement.

(l) Your report is intended solely for the information and use of the Company, the European Commission, and the applicable Digital Services Coordinator of establishment as mandated under DSA Article 42(4), (collectively, the "Specified Parties") for assessing the audited provider's compliance with the Specified Requirements, and is not intended to be, and should not be, used by anyone other than these Specified Parties or for other purposes.

(m) We are responsible for the Transparency Report including the assessment of relevant information, and the selection by management of different but acceptable measurement methods, input data, or assumptions may have resulted in materially different amounts, metrics being reported.

APPENDIX B

This Appendix B is part of the statement of work dated as of January 19, 2026 between Deloitte & Touche LLP and Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries (the "Company").

DISPUTE RESOLUTION PROVISION

This Dispute Resolution Provision sets forth the dispute resolution process and procedures applicable to the resolution of Disputes and shall apply to the fullest extent of the law, whether in contract, statute, tort (such as negligence), or otherwise.

Mediation: All Disputes shall be first submitted to nonbinding confidential mediation by written notice to the parties, and shall be treated as compromise and settlement negotiations under the standards set forth in the Federal Rules of Evidence and all applicable state counterparts, together with any applicable statutes protecting the confidentiality of mediations or settlement discussions. If the parties cannot agree on a mediator, the International Institute for Conflict Prevention and Resolution ("CPR"), at the written request of a party, shall designate a mediator.

Arbitration Procedures: If a Dispute has not been resolved within 90 days after the effective date of the written notice beginning the mediation process (or such longer period, if the parties so agree in writing), the mediation shall terminate and the Dispute shall be settled by binding arbitration to be held in Chicago, Illinois. The arbitration shall be solely between the parties and shall be conducted in accordance with the CPR Rules for Non-Administered Arbitration that are in effect at the time of the commencement of the arbitration, except to the extent modified by this Dispute Resolution Provision (the "Rules").

The arbitration shall be conducted before a panel of three arbitrators. Each of the Company and Deloitte & Touche LLP shall designate one arbitrator in accordance with the "screened" appointment procedure provided in the Rules, and the two party-designated arbitrators shall jointly select the third in accordance with the Rules. No arbitrator may serve on the panel unless he or she has agreed in writing to enforce the terms of the statement of work (including its appendices) to which this Dispute Resolution Provision is attached and to abide by the terms of this Dispute Resolution Provision. Except with respect to the interpretation and enforcement of these arbitration procedures (which shall be governed by the Federal Arbitration Act), the arbitrators shall apply the laws of the State of Washington (without giving effect to its choice of law principles) in connection with the Dispute. The arbitrators shall have no power to award punitive, exemplary, or other damages not based on a party's actual damages (and the parties expressly waive their right to receive such damages). The arbitrators may render a summary disposition relative to all or some of the issues, provided that the responding party has had an adequate opportunity to respond to any such application for such disposition. Discovery shall be conducted in accordance with the Rules.

All aspects of the arbitration shall be treated as confidential, as provided in the Rules. Before making any disclosure permitted by the Rules, a party shall give written notice to all other parties and afford such parties a reasonable opportunity to protect their interests. Further, judgment on the arbitrators' award may be entered in any court having jurisdiction.

Costs: Each party shall bear its own costs in both the mediation and the arbitration; however, the parties shall share the fees and expenses of both the mediators and the arbitrators equally.

APPENDIX C

This Appendix D is part of the engagement letter dated January 19, 2026 between Deloitte & Touche LLP and Microsoft.

CHANGE ORDER FORM

Date requested:	[insert details]
Title of request:	[insert details]

Change number:	[insert details]
Requested by:	[insert details]

This Change Order Form amends the Statement of Work between Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries ("*Microsoft*" or "the Company") and Deloitte & Touche LLP ("*Supplier*") dated as of January 19, 2026 (the "*SOW*"). This Change Order Form is entered into between the same parties and is effective on [insert month, date, year] [the "*Change Order Effective Date*"]. This Change Order is subject to all of the terms and conditions in the SOW. The parties agree as follows:

Change requested in: (Check all that apply)

☐ **Specifications** ☐ **Deliverables**

☐ **Schedules** ☐ **Services**

☐ **Other**

Affected Section #s of SOW, or name of other document:

Description of change:

Reason for change:

Change(s) to SOW:

Section #	***Original language:***	***Replacing/supplementing language:***

Supplier approval

Print name/Title _____

Signature_____ Date _____

Microsoft approval: MICROSOFT IRELAND OPERATIONS LIMITED, on behalf of itself, its affiliates, and its subsidiaries

Print name/Title _____

Signature_____ Date _____

APPENDIX D DATA PROTECTION

This Appendix D is part of the engagement letter dated January 19, 2026 between Deloitte & Touche LLP and Microsoft.

SECTION 1 Scope, Order of Precedence, and Term

(a) This Appendix modifies and supplements the terms and conditions in the Agreement as they relate to Supplier's Processing of Personal Data and compliance with Data Protection Law. Supplier is operating as an Independent Controller for the Personal Data it Processes under the Agreement. Notwithstanding anything to the contrary in the Agreement, if there is a conflict between this Appendix and the Agreement, this Appendix will control with respect to its subject matter.

(b) This Appendix applies to the extent that Supplier receives, stores, or Processes Personal Data or Confidential Information in connection with the Services.

SECTION 2 Definitions

(a) All capitalized terms not defined in this Appendix will have the meanings set forth in the Agreement.

(b) The following terms have the definitions given to them in the CCPA: "*Business*," "*Business Purpose,"* "*Sale*," "*Share,"* "*Service Provider*," "*Contractor*," and "*Third Party*."

(c) "*Controller*" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes a Business, Controller (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

(d) "*Data Exporter*" means the party that (1) has a corporate presence or other stable arrangement in a jurisdiction that requires an International Data Transfer Mechanism and (2) transfers Personal Data, or makes Personal Data available to, the Data Importer.

(e) "*Data Importer*" means the party that is (1) located in a jurisdiction that is not the same as the Data Exporter's jurisdiction and (2) receives Personal Data from the Data Exporter or is able to access Personal Data made available by the Data Exporter.

(f) "*Data Protection Law"* means any Law applicable to Supplier, in its performance of the Services, or Microsoft, in its receipt of the Services, relating to data security, data protection, and/or privacy, including, as may be applicable under the circumstances, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and the free movement of that data ("*GDPR*"), and Cal. Civ. Code Title 1.81.5, § 1798.100 et seq. (California Consumer Privacy Act) ("*CCPA*"), and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended, repealed and replaced, or re-enacted, in each case, having the effect of law.

(g) "*Data Subject*" means an identifiable natural person who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(h) *"De-identified Data"* means information that cannot reasonably be linked to an identified or identifiable individual.

(i) "*EEA*" means the European Economic Area.

(j) "*Personal Data*" means any information relating to an identified or identifiable natural person ("*Data Subject*") and any other data or information that constitutes personal data or personal information under any applicable Data Protection Law received from, or on behalf of the Company by Supplier in its performance of the Services. An identifiable natural person is one who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(k) "*Process*" or "*Processing*" means any operation or set of operations that a party performs on

Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

(l) "*Processor*" means an entity that processes Personal Data on behalf of another entity. "Processor" includes Service Provider, Contractor, Processor (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

(m) "*Protected Health Information*" or "*PHI*" means the Company Personal Data that is protected by the Health Information Portability and Accountability Act (HIPAA).

(n) *"Pseudonymous Data"* means information that cannot be attributed to a specific individual without the use of additional information provided that it is kept separately and subject to appropriate technical and organizational measures to ensure that it is not attributed to the individual.

(o) "*Sensitive Data*" means the following types and categories of data: (1) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, immigration or citizenship status, or trade union membership; genetic data; (2) biometric data; (3) data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; (4) data concerning a natural person's sex life or sexual orientation; (5) government identification numbers (e.g., SSNs, driver's license); (6) payment card information; (7) nonpublic personal information governed by the Gramm Leach Bliley Act; (8) an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; (9) personal bank account numbers; (10) data related to children; and (11) precise geolocation.

(p) "*Standard Contractual Clauses*" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

(q) "*Subprocessor*" means a Processor engaged by a party who is acting as a Processor.

SECTION 3 Description of the Parties' Personal Data Processing Activities and Statuses of the Parties

(a) The subject matter and duration of the Processing, and the nature and purpose of the Processing, pertain to the Processing of Personal Data related to the provision of the Services reflected in the Agreement.

(b) Microsoft and Supplier operate as Independent Controllers for Processing of Personal under the Agreement.

(c) To the extent Personal Data has been transferred from the EEA, United Kingdom or Switzerland ("EEA/CH/UK") to a jurisdiction outside the EEA/CH/UK which is not recognized by the European Commission, UK Secretary of State or the relevant Swiss regulator as providing an adequate level of protection for personal data, and such transfer is not covered by an alternative International Data Transfer Mechanism (as such term is defined below), Module 1 of the Standard Contractual Clauses applies to the Processing of Personal Data under the Agreement, subject to the supplemental terms set forth in Schedule 1 hereto.

SECTION 4 International Data Transfer

(a) Some jurisdictions require that an entity transferring Personal Data to a recipient in another jurisdiction take extra measures to ensure that the Personal Data has special protections if the law of the recipient's jurisdiction does not protect Personal Data in a manner equivalent to the transferring entity's jurisdiction (an "*International Data Transfer Mechanism*"). The parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law and that is mutually agreed upon, including the Standard Contractual Clauses.

(b) If the International Data Transfer Mechanism on which the parties rely is invalidated or superseded, the parties will work together in good faith to find a suitable alternative.

(c) The parties agree that by executing this Agreement they also execute the Standard Contractual Clauses, which will be incorporated by reference and form an integral part of this Agreement. The parties agree that, with respect to the elements of the Standard Contractual

Clauses that require the parties' input, Schedule 1 contains information relevant to the Standard Contractual Clauses' Annexes. The parties agree that, for Personal Data of Data Subjects in the United Kingdom, Switzerland, or another country specified in Schedule 1, they adopt the modifications to the Standard Contractual Clauses listed in Schedule 1 to adapt the Standard Contractual Clauses to local law, as applicable.

SECTION 5 Mutual Obligations of the Parties

(a) **Compliance**. The parties will comply with their respective obligations under Data Protection Law and their privacy notices, including by providing the same level of privacy protection that is required of Businesses under the CCPA.

(b) **Information.** Upon request, Supplier will provide reasonably relevant information to Microsoft to enable Microsoft to fulfill its obligations (if any) to conduct data protection assessments or prior consultations with data protection authorities.

(c) **Notification.** Supplier will notify Microsoft if it determines that it can no longer meet its obligations under applicable Data Protection Law.

(d) **Cooperation.** If Supplier receives any type of request or inquiry from a governmental, legislative, judicial, law enforcement, or regulatory authority, or faces an actual claim, inquiry, or complaint in connection with Parties' Processing of Personal Data provided to Supplier by or on behalf of Microsoft, its affiliates, or its respective end users, or obtained or collected by Supplier in connection with the purposes of this Agreement, then Supplier will notify Microsoft without undue delay, but in no event later than ten (10) business days, unless such notification is prohibited by applicable law. Supplier will promptly provide Microsoft with information relevant to the Inquiry reasonably requested by Microsoft, including any information relevant to the defense of a claim, to enable Microsoft to respond to the Inquiry.

(e) **Confidentiality**. Supplier will ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality obligations no less protective than those set forth in the Agreement or are under an appropriate statutory obligation of confidentiality.

(f) **Security Controls**. Supplier will take all measures required by applicable Data Protection Law relating to data security (including pursuant to Article 32 of the GDPR). Supplier will implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk.

SECTION 6 Supplier's Obligations as Independent Controller. As a Controller of Personal Data that is collected, exchanged, or otherwise Processed in connection with Supplier's performance of the Agreement:

(a) Supplier acknowledges and agrees that Supplier is independently responsible for compliance and will comply with applicable Data Protection Law (e.g., obligations of Controllers);

(b) Supplier will not Sell Personal Data;

(c) Supplier agrees to be responsible for providing notice to Data Subjects as may be required by applicable Data Protection Law (e.g., GDPR Articles 13 and 14, as applicable) and responding, as required by Data Protection Laws such as Chapter III of GDPR, to Data Subject's requests to exercise their rights and identifying a lawful basis of Processing (e.g., consent or legitimate interest);

(d) Supplier agrees that will keep Pseudonymous Data separate from any additional information necessary to make such Pseudonymous Data attributable to a specific individual and will subject such Pseudonymous Data to appropriate technical and organizational measures to ensure that it is not attributed to specific individual; and

(e) Supplier agrees that it will take reasonable measures to ensure that De-identified Data cannot be associated with a specific consumer or household, publicly commit to maintain the De-identified Data in de-identified form and not attempt to reidentify it, and contractually commit any Subprocessors to do the same**.**

SECTION 7 Supplier's Obligations as Third Party. If Supplier Processes Personal Data as a Third Party under the CCPA in connection with Supplier's performance of the Agreement, then:

(1) Supplier will Process Personal Data only for the limited and specific business purpose(s) described in the Agreement.

(2) Supplier agrees that the Personal Data is made available only for the limited and specified purpose(s) set forth in the Agreement, and Supplier may use the information only for those purposes.

(3) Supplier will not Sell or Share Personal Data made available to it by Microsoft.

Schedule 1 to Appendix D:

Information for International Transfers

Frequency of Transfer

Continuous for all Personal Data.

Retention Periods

As Controllers, the parties retain Personal Data for as long as they have a business purpose for it or for the longest time allowable by applicable law.

1. *For the purpose of the Standard Contractual Clauses:*
    - Clause 7: The parties do not adopt the optional docking clause.
    - Clause 8.2(c): Before disclosing a copy of the Standard Contractual Clauses, the disclosing party must redact all commercial terms including without limitation liability terms, Annex II, and any other detailed security terms.
    - Clause 11(a): The parties do not select the independent dispute resolution option.
    - Clause 17: The parties select Option 1. The parties agree that the governing jurisdiction is Republic of Ireland.
    - Clause 18: The parties agree that the forum is the High Court in Dublin, Ireland.
    - The Parties agree that the references to local law in the Standard Contractual Clauses include applicable professional standards.
    - For the avoidance of doubt, any limitations of liability, including limitations on indemnities, set forth in the Agreement apply with respect to liability arising under the Standard Contractual Clauses.
    - Nothing herein shall make Supplier responsible for the implementation and maintenance of any controls relating to the equipment or information systems of Microsoft. All such controls shall be the responsibility of Microsoft except as otherwise expressly agreed in an applicable SOW.
    - Annex I(A): The data exporter is the Data Exporter (defined above) and the data importer is the Data Importer (defined above).
    - Annex I(B): The parties agree that Schedule 1 describes the transfer.
    - Annex I(C): The competent supervisory authority is the Irish Data Protection Commission.
    - Annex II: The parties agree that Schedule 2 describes the technical and organizational measures applicable to the transfer.

2. *For the purpose of localizing the Standard Contractual Clauses the terms in Section 1 above shall apply except to the extent modified below:*
    - Switzerland
        - The parties adopt the GDPR standard for all data transfers.
        - Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified above.
        - Clause 17: The parties agree that the governing jurisdiction is Republic of Ireland.
        - Clause 18: The parties agree that the forum is the High Court in Dublin, Ireland. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).
        - The parties agree to interpret the Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.
    - United Kingdom

- "UK SCC Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK's Information Commissioner's Office under S119A(1) Data Protection Act 2018, as modified by the Information Commissioner's office from time to time, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

- For transfers from the United Kingdom that are not subject to an adequacy decision or exception, the parties hereby incorporate the UK SCC Addendum by reference and, by signing this DPA, also enter into and agree to be bound by the Mandatory Clauses of the UK SCC Addendum.
- The parties agree that the following information is relevant to Tables 1 – 4 of the UK SCC Addendum and that by changing the format and content of the Tables neither party intends to reduce the Appropriate Safeguards (as defined in the UK SCC Addendum).
    - Table 1: The parties' details, key contacts, data subject contacts, and signatures are in the signature block of the DPA.
    - Table 2: The selected SCCs, Modules and Selected Clauses are described in Schedule 1.
    - Table 3: The list of parties, description of transfer, and list of sub-processors are described in Schedule 1. The Technical and Organizational measures to ensure the security of the data are described in Schedule 2.
    - Table 4: Neither party may end the UK SCC Addendum when the Approved Addendum changes.
- Clause 17 of the Standard Contractual Clauses: The parties agree that the governing jurisdiction is the United Kingdom.
- Clause 18 of the Standard Contractual Clauses: The parties agree that the forum is the courts of England and Wales. The parties agree that Data Subjects may bring legal proceedings against either party in the courts of any country in the United Kingdom.

Schedule 2 to Appendix D:



DeloitteInformation SecurityStatement.p

APPENDIX E

This Appendix E is part of the engagement letter dated January 19, 2026 between Deloitte & Touche LLP and Microsoft.

INFORMATION SUBJECT TO EXAMINATION

Subject Matter on Which Management's Assertion is Based	*Criteria*
To be mutually agreed upon by the parties during the course of the engagement. Such subject matter and Criteria will be based upon the obligations set out in Chapter III of the DSA combined with Microsoft's benchmarks as required in the Delegated Regulation supplementing Regulation (EU) 2022/2065.	

Appendix 4B – Written agreement between VLOSE and the auditing organization (COCD)

Written agreement between VLOSE and the auditing organization (COCD)

The following pages contain the written agreement between the VLOSE and the auditing organization. Additionally, refer to Appendix 1B for the exhaustive list of audited commitments and measures for COCD, respectively.

Statement of Work
("SOW")

Addresses and contacts for notices

"Microsoft"	"Supplier"
Company Name: Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries	Company Name: Deloitte & Touche LLP
Primary Contact: [CONFIDENTIAL]	Primary Contact: [CONFIDENTIAL]
Address: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Address: 1015 Second Avenue, Suite 500 Seattle, WA 98104
Phone number: N/A	Phone number: [CONFIDENTIAL]
Fax number: N/A	Fax number: [CONFIDENTIAL]
Email (if applicable): [CONFIDENTIAL]	Email (if applicable): [CONFIDENTIAL]
Secondary Contact:	Secondary Contact:
	Microsoft Supplier Number: 1100000

SOW Effective Date:	April 01, 2026
SOW Expiration Date:	October 31, 2026
DealPoint # for Master Agreement	
Budget ID#	

Agreed and accepted

Microsoft, on behalf of itself and its subsidiaries		Supplier
Microsoft Signature: [CONFIDENTIAL]	Microsoft Signature:	Supplier Signature: [CONFIDENTIAL]
Microsoft Name: [CONFIDENTIAL]	Microsoft Name:	Supplier Name: [CONFIDENTIAL]
Microsoft Title: [CONFIDENTIAL]	Microsoft Title:	Supplier Title: [CONFIDENTIAL]
Microsoft Date: 05-May-2026 | 2:03:52 PM PDT	Microsoft Date:	Supplier Date: 04-May-2026 | 1:31:59 PM PDT

☒ This SOW (together with the attached appendices, the "Agreement") dated as of April 01, 2026 between Microsoft and the Supplier is entered into by the parties and is effective as of the SOW Effective Date above.

☐ This SOW pursuant to the Microsoft Purchase Order Terms and Conditions is entered into by the parties and effective as of the SOW Effective Date above.

SECTION 1 Purpose

The purpose of this SOW is to set forth the specific services that the Supplier will provide to Microsoft.

SECTION 2 Description of Services and Delivery Schedule

(a) Description of Services. Section 2(b) (Services) describes the details of the independent accountant's examination services, including project expectations and the Supplier activities, the Supplier will perform or deliver to Microsoft under this SOW (collectively, the "Services").

(b) Services. Deloitte & Touche LLP ("D&T" or "we" or "us" or "Supplier") is pleased to serve as independent accountants for Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries (together referred to as "Microsoft" ; the "Company" or "you" or "your") to perform an examination of management of the Company's assertion regarding Microsoft Bing, being designated as a Very Large Online Search Engine (VLOSE) under the Digital Services I ("DSA" or "Regulation (EU) 2022/2065")[1], service's compliance with Bing's Commitments and Measures ("Specified Measures") under the Code of Conduct on Disinformation ("COCD") [2] for the period July 1, 2025 to May 31, 2026 (collectively, the "subject matter") is presented in accordance with the criteria defined in Appendix E ("the Criteria") (collectively, "management's assertion"). [CONFIDENTIAL] will be responsible for the services that we perform for the Company hereunder. For purposes of Sections 9, 10 and 11, "Supplier" will mean Deloitte & Touche LLP and its subsidiaries; Deloitte Touche Tohmatsu Limited, its member firms, the affiliates of Deloitte & Touche LLP, Deloitte Touche Tohmatsu Limited and its member firms; and, in all cases, any successor or assignee. Microsoft Ireland Operations Limited represents and warrants that it has the power and authority to execute this agreement on behalf of, and to bind, itself, its affiliates, and its subsidiaries hereto.

(1) Examination of Management's Assertion and the Subject Matter.

Our engagement is to perform an examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) (the "AICPA attestation standards") and International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board (the "ISAE standards"). The objectives of an examination conducted in accordance with the AICPA attestation standards and ISAE standards are to:

1. Obtain reasonable assurance about whether the subject matter as measured or evaluated against the Criteria is free from material misstatement.
2. Express an opinion in the form of a written report about whether management's assertion is fairly stated, in all material respects.

An examination includes examining, on a test basis, evidence supporting management's assertion and the subject matter and performing such other procedures as the Supplier considers necessary in the circumstances. An examination conducted in accordance with the AICPA attestation standards and ISAE standards is designed to obtain reasonable, rather than absolute, assurance about management's assertion and the subject matter taken as a whole. Because of the inherent limitations of an examination engagement, together with the inherent limitations of internal control, an unavoidable risk exists that some material misstatements may not be detected, even though the examination is properly planned and performed in accordance with the AICPA attestation standards and ISAE standards.

These professional standards require us to establish whether the required preconditions for an assurance engagement are present. This is based on our preliminary knowledge of the engagement circumstances and discussion with the appropriate parties. If we discover after the

---

[1] The Digital Services Act (DSA) establishes a set of narrowly defined objective criteria to prevent illegal and harmful activities online and the spread of disinformation through VLOSE.

2 The Code of Conduct on Disinformation (COCD) establishes a collaborative framework of commitments and measures aimed at reducing the spread of disinformation online and strengthening platform accountability, transparency, and responsible information practices.

engagement has been accepted that one or more preconditions for the services is not present, we will discuss the matter with you and determine whether the matter can be resolved to our satisfaction, whether it is appropriate for us to continue with the engagement and, if so, how to communicate the matter in the report.

(2) Report on Management's Assertion and the Subject Matter.

We expect to issue a written report upon the completion of our examination. Our ability to express any opinion or to issue any report as a result of this engagement and the wording thereof, will, of course, be dependent on the facts and circumstances at the date of our report. If, for any reason, we are unable to complete our examination or are unable to form, or have not formed, any opinion, we may decline to express any opinion or decline to issue any report as a result of this engagement. If we are unable to complete our examination or if any report to be issued by the Supplier as a result of this engagement requires modification, the reasons for this will be discussed with management.

(c) Locations. Services will be performed remotely and at the following location(s):

Facility	Address
Onsite: Microsoft Redmond Campus	One Microsoft Way Redmond, WA 98052

(d) Hours of Operation. The Supplier will provide Services M-F 8-5 PST. However, the Supplier will operate additional hours as necessary.

(e) Reporting requirements. The Supplier will endeavor to provide the following reports to the Company according to the schedule indicated below.

Report description	Schedule (Anticipated)	Format
Weekly status reports*	April 2026 – August 2026	Excel/PDF
Monthly expense reports*	April 2026 – August 2026	Excel/PDF
Assurance report on the Company's compliance with COCD of DSA	August 25, 2026	PDF

* Weekly status updates showing status of walkthroughs, data requests, test execution, and exceptions organized by the Company's COCD requirements.

(f) Deliverables / Delivery Schedule. Subject to the terms hereof, the Supplier will endeavor to complete and deliver all Services to the Company on or before August 25, 2026. The milestone delivery schedule for the Services, if applicable, will be as follows:

Milestone #	Brief Description of Services to be completed by Supplier and delivered to the Company	Estimated Due on or Before
1	Plan examination, including review of draft control matrix and preparation of test plans	April 2026
2	Start examination, including walkthroughs of controls and examining evidence	April – June 2026
3	Perform design effectiveness testing	April – June 2026
4	Perform operating effectiveness testing	May – July 2026
5	Provide a draft report to the management	July 2026
6	Issue final report and perform examination wrap-up	July – October 2026

In addition to the deliverables listed above, the Supplier will conduct weekly status meetings with management starting in April 2026.

(1) Inclusion of Supplier Reports or References to Supplier in Other Documents or Electronic Sites.

Nothing in this engagement letter is intended to restrict the ability of the Company to distribute to other parties any of our reports issued hereunder unedited and, in its entirety. In connection

with such distribution, to the extent the Company needs to describe the services hereunder or describe any report issued hereunder, the Company agrees only to use the description provided within the applicable report, unedited and in its entirety. Except as described above, if the Company intends to publish or otherwise reproduce in any document any report issued as a result of this engagement, or otherwise make reference to the Supplier in a document that contains other information in addition to management's assertion and the subject matter (e.g., in a periodic filing with a regulator), thereby associating the Supplier with such document, in both instances the Company agrees that its management will provide the Supplier with a draft of the document to read and obtain our approval for the inclusion or incorporation by reference of any of our reports, or the reference to the Supplier, in such document before the document is printed and distributed. The inclusion or incorporation by reference of any of our reports in any such document would constitute the reissuance of such reports. Except as otherwise required by the European Commission, the Company also agrees that its management will notify us and obtain our approval prior to including any of our reports on an electronic site. For purposes of this paragraph, the Supplier's approval shall be based upon professional standards and facts and circumstances at the time of the request.

Our engagement to perform the services described herein does not constitute our agreement to be associated with any such documents published or reproduced by or on behalf of the Company. Any request by the Company to reissue any report issued as a result of this engagement, to consent to or acknowledge our awareness of any such report's inclusion or incorporation by reference in another document, or to agree to any such report's inclusion on an electronic site will be considered based on the facts and circumstances existing at the time of such request. The estimated fees outlined herein do not include any procedures that would need to be performed in connection with any such request. Should the Supplier agree to perform such procedures, fees for such procedures would be subject to the mutual agreement of the Company and the Supplier.

SECTION 3 Payment

(a) **Service fees.** The Company will pay Supplier a total fee not to exceed [CONFIDENTIAL] according to the milestone payment schedule below as full and final payment for the Services. The Company will only make payment for Services that Supplier has completed and delivered to the Company, and that the Company has accepted in accordance with the terms of Section 2(c).

Milestone #	Not to exceed payment amount	Delivery/payment date
1	[CONFIDENTIAL]	April 1, 2026
2, 3	[CONFIDENTIAL]	May 1, 2026
2, 3, 4	[CONFIDENTIAL]	June 1, 2026
4	[CONFIDENTIAL]	July 1, 2026
5, 6	[CONFIDENTIAL]	August 1, 2026
Sub-total	[CONFIDENTIAL]	**-**
Estimated expenses maximum (if agreed to – see Section 3(b)(Expenses), below)	[CONFIDENTIAL]	Expense must be listed separately on any invoices submitted by the Supplier to allow for appropriate visibility.
Total	[CONFIDENTIAL]	-

(b) **Expenses**. As reflected in Section 3(a) (Services fees), above, the Company will reimburse the Supplier for the actual expenses that Supplier incurs while performing the Service up to a total not to exceed the amount of [CONFIDENTIAL]. The expense must comply with the Company policy. The expenses must also be reasonable and related to the Services. The Supplier must submit appropriate documentation evidencing the expenses to be reimbursed.

(c) Payment of Invoices. [CONFIDENTIAL]

(d) Relationship of the Parties. The Supplier is responsible for and will pay all wages, fringe benefits, payroll taxes, insurance, work schedules, and work conditions with respect to its employees, contractors or other resources performing Services under this SOW.

Each party shall comply with all economic sanctions, export control, and import laws and regulations applicable to it in connection with this engagement letter. The parties recognize that such laws and regulations restrict the export and reexport of the Services to jurisdictions subject to territorial U.S. economic sanctions (currently Crimea, Cuba, Iran, North Korea, Russia, Syria, and the Donetsk and Luhansk National People's Republics in Ukraine).

(e) Compliance with Trade Laws

The parties acknowledge that the Services and Deliverables ("Items") may be subject to applicable trade laws in one or more countries and that the Services may not be exported to Russia or any countries subject to comprehensive sanctions, except in compliance with applicable law. The parties will comply with all relevant laws and regulations applicable to the import or export of the Items, including but not limited to, trade laws such as the U.S. Export Administration Regulations or other end-user, end use, and destination restrictions by the U.S. and other governments, as well as sanctions regulations administered by the U.S. Office of Foreign Assets Control ("Trade Laws"). Either party may suspend or terminate the Agreement immediately to the extent that such party reasonably concludes that continued performance would violate Trade Laws or put it at risk of becoming subject to sanctions or penalties under Trade Laws.

SECTION 4 Term and Termination

(a) **Term**. Unless terminated sooner in accordance with its terms, this SOW will terminate on the completion of the Services.

(b) **Early termination**. This SOW may be terminated by the Company, without cause, at any time by giving written notice to the Supplier not less than thirty (30) days before the effective date of termination, or immediately upon written notice in the event the Supplier notifies the Company of a Conflict under Section 12(d) below. This SOW may be terminated by either party, for cause, at any time by giving written notice to the other party. Either party may also terminate this SOW or performance of any part of the Services, upon written notice to the other party, if it reasonably determines that the performance of any part of the Services would be in conflict with law, or independence or professional rules.

SECTION 5 Additional Obligations

(a) **Staffing requirements.** The Supplier will determine all resource requirements needed to remain in compliance with standards defined within this SOW. The Supplier will be responsible for training its own employees. Training will include, but not be limited to, keeping staff informed of new technology, Microsoft account processes, procedures, standards, customer service, and quality. The Supplier's staff performing Services as outlined in this SOW will keep current on technology, governmental and/or regulatory agencies' guidelines, codes, standards, and regulations for products, methods, and techniques, as appropriate. The Company will provide training to the Supplier's team lead for all technologies and tools that are not commercially available to the Supplier.

(b) **Skillset requirements.** The Supplier will be a Certified Public Accounting firm with the ability to issue the report on management's assertion and the subject matter in addition to the following skills:

(1) Significant experience issuing IT-related reports

(2) Strong project management capabilities

(3) Ability to work flexibly to achieve results within the dynamic Company environment

(4) Excellent interpersonal and task-management skills

(5) Strong written and verbal communication skills

(6) Relevant risk and regulatory knowledge

(c) **Roles and responsibilities.**

Company	Supplier
The Company will provide the Supplier access to the following applications/tools/materials required to perform Services under this SOW: • Exchange • SharePoint • Azure DevOps • Additional tools as necessary	The Supplier will provide all Supplier resources with the applications/tools/materials required to perform Services under this SOW, including the following: • MS Office Suite • MS Outlook • MS Word • MS Excel • MS PowerPoint
Responsiveness of the Company team members to the Supplier requests and issues is anticipated to be within reason so delivery schedules are not adversely impacted. If issues do arise, the Supplier will escalate to management according to a mutually agreed upon escalation process.	[CONFIDENTIAL] will be the Engagement Leader and will be responsible for the Supplier's independent auditor's examination, while [CONFIDENTIAL] will continue to coordinate all services we perform for Microsoft. [CONFIDENTIAL] will serve as the practitioner-in-charge and will be responsible for directing the day-to-day activities of the Supplier's examination.

(d) **Software and materials.** The Supplier will provide each resource with a laptop (onsite with Supplier-owned licenses for commercially available Company Software described in Section

5(c)). The Company will provide the additional required software, licenses and access to applications required to carry out the Services, also described in Section 5(c). The Company-provided software and applications will be uninstalled/returned to the Company upon completion/expiration/termination of the Services provided under this SOW. The Supplier will be responsible for providing all other software, facilities, tools, and equipment not otherwise described herein.

(e) Additional assumptions. The following assumptions and dependencies are associated with the planning and execution of the Services under this SOW. Specifically, for this SOW, its success will depend on the following:

(1) Supplier will have the ability to understand the Company's approach and model for the requested services.

(2) Supplier will be able to effectively communicate with onshore team(s), if applicable

(3) Supplier will maintain an open communication environment.

(4) Supplier, its employees, and Subcontractor(s), if any, will be required to keep secure all Company products, mail, and equipment in accordance with the obligations set forth in Section 12 clause c.

(5) Supplier will assume the risk of the loss of any Company equipment, or materials while in the care, custody, or control of the Supplier's employees. Supplier's employees will not use the Company facilities and/or any Company equipment, products, or materials to perform Services for any person or entity other than the Company.

(6) All Supplier resources will have valid work permits and necessary visa to work in the United States.

(7) Supplier team resources will have the following access if the Company determines such access is relevant to the Services:

i. Access to the Company engagement management to review priorities, steer the engagement, attend status meetings, and approve project Deliverables;

ii. Access to all engagement documentation, including, but not limited to, standard operating procedures;

iii. Access to information around any issues with applications/projects; and

iv. Supplier will resolve all access and connectivity issues within five business days from the start date; at that time, all Supplier resources will have necessary access to all required resources.

(8) The Company will assign a project manager who will be responsible for:

i. Coordinating interview meetings/walkthroughs with control owners as required

ii. Providing required access to the Supplier personnel involved in this engagement

iii. Assisting in data gathering requests

iv. Overseeing the engagement, working side-by-side with the Supplier and handling escalation of issues and engagement risks to the Company management

(9) The Company will support evidence requests and inquiries as needed by the Supplier to enable their assessments and testing.

(10) To facilitate the collection of data needed for testing, Supplier will work with the Company project manager and supporting Company personnel to provide test procedures and data request lists as early in the project as possible.

(11) To facilitate the scheduling of Company control performers, the Supplier will provide interview request lists and proposed meeting agendas as early in the engagement as possible.

SECTION 6 SOW Changes

Unless specifically described otherwise in this SOW, changes to this SOW will be as follows:

(a) Approved minor or non-substantive changes will be memorialized in writing using the Change Order Form attached as Appendix C. The Change Order Form will become an attachment to and part of this SOW after both parties have signed it.

(b) Substantive or major changes will be addressed in a SOW Amendment.

SECTION 7 Definition of Management's Responsibilities

Appendix A describes management's responsibilities.

SECTION 8 Limitations of an Entity's Internal Control

Because of the inherent limitations of internal control, including the possibility of collusion or improper management override of controls, material misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

SECTION 9 Audit Committee's Responsibility

The Supplier acknowledges that the Audit Committee is directly responsible for the appointment, compensation, and oversight of the Supplier's work and, accordingly, except as otherwise specifically noted, the Supplier will report directly to the Audit Committee. The Company has advised the Supplier that the Services to be performed under this SOW, including, where applicable, the use by the Supplier of affiliates or related entities as subcontractors in connection with this SOW, have been approved by the Audit Committee in accordance with the Audit Committee's established preapproval policies and procedures.

Process for Obtaining Preapproval of Services: The Company's management is responsible for the coordination of obtaining the preapproval of the Audit Committee, in accordance with the Audit Committee's preapproval process, for any services to be provided by the Supplier to the Company.

SECTION 10 Independence Matters Relating to Certain Services

In connection with the Supplier's engagement, the Supplier, the Company's management, and the Audit Committee will assume certain roles and responsibilities in an effort to assist the Supplier in maintaining independence and ensuring compliance with the securities laws and regulations. The Supplier will communicate to its partners, principals, and employees that the Company is an attest client. Management of the Company will ensure that the Company has policies and procedures in place for the purpose of ensuring that the Company will not act to engage the Supplier or accept from the Supplier any service that either has not been subjected to their preapproval process or that under SEC or other applicable rules would impair the Supplier's independence. All potential services are to be discussed with [CONFIDENTIAL], Lead Client Service Partner.

SECTION 11 Independence Matters Relating to Hiring

The Company's management will coordinate with the Supplier to ensure that the Supplier's independence is not impaired by hiring former or current partners, principals, or professional employees of the Supplier for certain positions. Management of the Company will ensure that the Company also has policies and procedures in place for purposes of ensuring that the Supplier's independence will not be impaired by hiring a former or current partner, principal, or professional employee of the Supplier in an accounting role or financial reporting oversight role that would cause a violation of securities laws and regulations. Any employment opportunities with the Company for a former or current partner, principal, or professional employee of the Supplier should be discussed with [CONFIDENTIAL] before entering into substantive employment conversations with the former or current partner, principal, or professional employee of the Supplier, if such opportunity relates to serving (1) as chief executive officer, controller, chief financial officer, chief accounting officer, or any equivalent position for the Company; (2) on the Company's board of directors; (3) as a member of the Audit Committee; or (4) in any other position that would cause a violation of securities laws and regulations.

SECTION 12 General Business Terms

(a) Force majeure. Neither party will be liable or deemed in breach for failure to perform any obligation under this SOW to the extent such failure is caused by a force majeure event (including, without limitation, acts of God, natural disasters, war, civil disturbance, action by governmental entity, strike, and other causes beyond the party's reasonable control). The party affected by the force majeure event will provide notice to the other party within a commercially reasonable time and will use its commercially reasonable efforts to resume performance

promptly after the end of the force majeure event. Obligations not performed due to a force majeure event will be performed as soon as reasonably possible when the force majeure event concludes.

(b) Relationship. The parties are independent contractors. This SOW does not create an exclusive relationship between the parties. The Supplier's employees and subcontractors are not Company employees. The Supplier agrees to discuss and provide the Company with reasonable non-confidential proof of independent contractor status of entities that are not affiliates or related entities of the Supplier upon request.

(c) Confidentiality and Protection of Personal Information.

i. Confidential Information. At all times during the Term, and for five years thereafter, to the extent that in connection with this engagement the Supplier comes into possession of any Company Confidential Information, the Supplier will hold in strictest confidence using at least the same degree of care as it employs in maintaining in confidence its own confidential information, but in no event less than a reasonable degree of care, and will not use or disclose to any third party, any Company Confidential Information except as set forth herein. The Supplier may disclose such information 1) to its subcontractors, whether located within or outside the United States, that are providing services in connection with this engagement and who have agreed to be bound by confidentiality obligations similar to those in this section; 2) as required by law, rule, regulation, applicable professional standards, judicial or regulatory process, to respond to governmental inquiries or in connection with litigation or arbitration relating hereto. The term "*Company Confidential Information*" means all non-public information that the Company designates, either in writing or orally, as being confidential, or which, under the circumstances of disclosure ought to be treated as confidential. The Company Confidential Information includes information relating to:

1. Released or unreleased Company software or hardware products;

2. Company source code;

3. Marketing or promotion of any Company product;

4. Business policies or practices of the Company;

5. Customers or suppliers of the Company;

6. Information received from others that Company is obligated to treat as confidential;

7. The existence and terms of this Agreement; and

8. Information provided by the Company under this Agreement or obtained or created by Supplier in the course of providing the Services, including:

a. Information contained in any reports provided to the Company;

b. Any electronic or written correspondence between the parties;

c. The Company customer lists, customer information and Personal Information, regardless of the source; and

d. Transactional, sales and marketing information related to the Services.

If the Supplier has any questions as to what comprises Company Confidential Information, the Supplier will consult with the Company. Company Confidential Information does not include information that was or becomes known to the Supplier on a non-confidential basis from a third party that the Supplier reasonably believes is not prohibited from disclosing such information to the Supplier by obligation to the Company, was known to the Supplier prior to the Company's disclosure to the Supplier hereunder, or information that becomes publicly available through no fault of the Supplier in breach hereof.

ii. Security procedures. The Supplier will employ security procedures designed to prevent disclosure of Company Confidential Information (including Personal Information) to unauthorized third parties. The Supplier's security procedures must include risk assessment and controls for:

1. System access;

2. System and application development and maintenance;

3. Change management;

4. Asset classification and control;
5. Incident response, physical and environmental security;
6. Disaster recovery/business continuity; and
7. Employee training.

(d) Privacy and data protection.

i. The Supplier will comply with the privacy and data protection requirements in Appendix D.

(e) Press Releases/Publicity. Except as may be required by law or applicable professional standards, neither party shall issue press releases, public statements or publicity that relates to this Agreement, without the prior written consent or approval of the other. Supplier shall not use the name "Microsoft" or "Microsoft Ireland Operations Limited" in any brochures, advertisements or websites and the Company shall not use the name "Deloitte & Touche" or "Deloitte" in any brochures, advertisements or websites, in such cases as an endorsement or recommendation of a party or its services. Supplier may, however, with the prior written consent of the Company, use the name "Microsoft Ireland Operations Limited" in client presentations and/or in written response to requests for client lists as part of the Request for Proposals, Requests for Information, etc.

(f) Compliance with 201 CMR 17.00. To the extent that any information obtained by the Supplier from or on behalf of the Company or its employees in connection with the performance of services under the statement of work relates to a resident of Massachusetts and constitutes "Personal Information" as defined in 201 CMR 17.02 (as may be amended), the Supplier shall comply with the obligations of 201 CMR 17.00 et. Seq. (as may be amended), entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth," with respect to such information.

(g) Third Party Information Technology Controls Report. Deloitte LLP ("DLLP"), the parent entity of the Supplier, has engaged a third party (the "Service Provider") to conduct an examination in accordance with Service Organization Controls 2 ("SOC 2") standards under the Statement on Standards for Attestation Engagements established by the American Institute of Certified Public Accountants to evaluate the description, suitability of the design, and the operating effectiveness of the security controls of DLLP's Infrastructure Support Services System relevant to security and availability, and to prepare a SOC 2 Type 2 report with respect thereto (the "SOC 2 Infrastructure Report"). Upon written request, the Supplier shall promptly provide the Company with a copy of the most recently available SOC 2 Infrastructure Report. The Company shall not disclose such report, or refer thereto in any communication, to any other person or entity. In the event the Company has any questions regarding such report, the Supplier shall make appropriate personnel reasonably available to discuss the contents thereof.

(h) Conflict of Interest. The Company acknowledges that the Supplier is providing a wide range of services for a large number of clients and may be in a position where it is providing services to companies and organizations which may present actual or potential conflict of interest. The Supplier shall establish commercially reasonably procedures to identify such situations. The Supplier will notify the Company of an actual conflict of interest and the parties will discuss appropriate next steps. The Company shall have the right to terminate this SOW in accordance with Section 4(b) above. The Supplier will neither use Company's Confidential Information obtained hereunder for the advantage of a third party, nor will it use confidential information obtained from any other party for the Company's advantage hereunder.

(i) Survival, Interpretation, and Severability. All provisions which are intended by their nature to survive performance of the Services will survive such performance, or the expiration or termination of this SOW. Each of the provisions of these terms will apply to the fullest extent of the law, whether in contract, statute, tort (such as negligence), or otherwise, notwithstanding the failure of the essential purpose of any remedy. Affiliated and related entities are intended third-party beneficiaries of the terms in this SOW, and may in their own right enforce such terms. If any term of this SOW, including its appendices, is determined to be invalid or unenforceable, such term will not affect the other terms hereof or thereof, but such invalid or unenforceable term will be deemed modified to the extent necessary to render it enforceable, preserving to the fullest extent permissible the intent of the parties set forth herein and therein.

(j) Assignment and Subcontracting. Except as provided below, neither party may assign, transfer, or delegate any of its rights or obligations hereunder (including, without limitation,

interests or Claims). Notwithstanding the foregoing, the Company hereby consents to the Supplier subcontracting any portion of the Services to any affiliate or related entity, whether located within or outside of the United States. Services performed hereunder by the Supplier's subcontractors will be invoiced as professional fees on the same basis as Services performed by the Supplier's personnel, unless otherwise agreed. The Supplier agrees that it will remain responsible to the Company for the Services performed by its subcontractors (including its affiliates and related entities that are acting as subcontractors hereunder) under this SOW to the same extent that the Supplier would be responsible to the Company if it had performed such Services. The parties may only agree to the use of subcontractors, other than the Supplier's affiliates or related entities, by written amendment to this SOW and these terms.

(k) Dispute Resolution. Any controversy or claim between the parties arising out of or relating to the engagement letter or this engagement (a "Dispute") shall be resolved by mediation or binding arbitration as set forth in the Dispute Resolution Provision attached hereto as Appendix B and made a part hereof.

(l) Governing law; Jurisdiction. The laws of the State of Washington govern this SOW. If either the Company or the Supplier employs attorneys to enforce any rights arising out of or relating to this Agreement, the prevailing party will be entitled to seek recovery of its reasonable attorneys' fees, costs, and other expenses, including the costs and fees incurred on appeal or in a bankruptcy or similar action.

(m) Entire Agreement, Amendment, and Notices. These terms, and the Statement of Work, including exhibits and appendices attached, constitute the entire agreement between the parties with respect to this engagement; supersede all other oral and written representations, understandings, or agreements relating to this engagement; and may not be amended except by written agreement signed by the parties. In the event of any conflict, ambiguity, or inconsistency between these terms and the Statement of Work, these terms will govern and control followed by the Statement of Work and then the appendices. All notices hereunder will be (a) in writing, (b) delivered to the representatives of the parties at the addresses first set forth above, unless changed by either party by notice to the other party, and (c) effective upon receipt.

APPENDIX A

This Appendix A is part of the engagement letter dated April 01, 2026 between Deloitte & Touche LLP and Microsoft.

MANAGEMENT'S RESPONSIBILITIES

Management's Assertion and the Subject Matter

Management is responsible for the preparation, presentation, and overall accuracy of management's assertion and the subject matter and its conformity with the Criteria. In this regard, management has the responsibility for, among other things:

- Our assertion related to the design, implementation, and maintenance of our systems and processes in place to comply with the Code of Conduct on Disinformation and our compliance with the Specified Measures.
- Preparation and fair presentation of the Subject Matter, in accordance with the Criteria.
- Establishing and maintaining effective internal control over compliance.
- Determining the applicability of all measures and each measure in the Code of Conduct on Disinformation during the Examination Period, selecting the Measures, making interpretations of any compliance requirements that have varying interpretations, and developing benchmarks, as needed, to implement the Specified Measures.
- Evaluating and monitoring with our compliance with the Specified Measure and having a reasonable basis for our Assertion. We have performed an evaluation of our compliance with the Specified Measures.
- Determining the Criteria are suitable, will be available to the intended users, and are appropriate for the purpose of the engagement.

Management's Representations

We will make specific inquiries of management about the representations embodied in management's assertion and the subject matter. In addition, we will request that management provide us with the written representations the Company is required to provide to its independent accountants under the AICPA attestation standards and ISAE standards. The responses to those inquiries and the written representations of management are part of the evidential matter that the Supplier will rely on in forming its opinion on management's assertion and the subject matter.

We confirm, to the best of our knowledge and belief, the following representations made to you during your examination engagement:

(a) We have provided you with all information relevant to the engagement and access as agreed to in the terms of the engagement and reflected all relevant matters in the measurement or evaluation of the Subject Matter.

(b) We have measured or evaluated the Subject Matter against the applicable criteria, including that all relevant matters are reflected in the Subject Matter.

(c) All known matters contradicting the Subject Matter, including any communication from regulatory agencies or others contradicting the Subject Matter, have been disclosed to you, including communications received between the end of the period addressed in the written assertion period ended May 31, 2026, and the date of the practitioner's report.

(d) We have disclosed to you all deficiencies in internal control relevant to the engagement of which we are aware.

(e) We are not aware of any actual, suspected, or alleged fraud affecting the Subject Matter.

(f) We have disclosed any known noncompliance with the Specified Requirements occurring during and subsequent to the period of July 1, 2025 through May 31, 2026.

(g) We are not aware of any cybersecurity incidents that could lead to noncompliance with the Specified Requirements.

(h) We believe that significant assumptions used in our legal determinations are reasonable and have been consistently applied to the Subject Matter. These legal determinations include the scoping of obligations that are subject to the examination.

(i) We acknowledge that the scope of the examination engagement was limited to the subject matter and assertion. All other information presented within the subject matter, including any information relating to periods prior to the beginning period of the examination of July 1, 2025, and post the examination period May 31, 2026, including information related to forward- looking statements, targets, goals, progress against goals, and linked information, were not subject to your procedures, and accordingly, you do not express an opinion or any form of assurance on such information.

(j) We are responsible for the selection or establishment of the Criteria, along with defining terms, benchmarks and other clarifying information, which we believe provide an objective basis for reporting the description of the systems and processes implemented to comply with Regulation (EU) 2022/2065 of the European Parliament and of the Council.

(k) We have responded fully and truthfully to all inquiries made to us by you during your examination engagement.

(l) Your report is intended solely for the information and use of the Company, the European Commission, and the applicable Digital Services Coordinator of establishment as mandated under DSA Article 42(4), (collectively, the "Specified Parties") for assessing the audited provider's compliance with the Specified Requirements, and is not intended to be, and should not be, used by anyone other than these Specified Parties or for other purposes.

(m) We are responsible for the Transparency Report including the assessment of relevant information, and the selection by management of different but acceptable measurement methods, input data, or assumptions may have resulted in materially different amounts, metrics being reported.

(n) We have disclosed any Subsequent Events to the period covered after the period end of the report, May 31, 2026, until the opinion date of your Examination Report, that could have a significant effect on the subject matter. We understand that you have no responsibility to perform any procedures regarding the subject matter after the date of your Examination Report. However, if after the date of your Examination Report, a material event happens or a fact becomes known to us that, if it had been known to you, may have caused you to have amended your report, then we will disclose this matter to you.

APPENDIX B

This Appendix B is part of the engagement letter dated as of April 01, 2026 between Deloitte & Touche LLP and Microsoft.

DISPUTE RESOLUTION PROVISION

This Dispute Resolution Provision sets forth the dispute resolution process and procedures applicable to the resolution of Disputes and shall apply to the fullest extent of the law, whether in contract, statute, tort (such as negligence), or otherwise.

Mediation: All Disputes shall be first submitted to nonbinding confidential mediation by written notice to the parties, and shall be treated as compromise and settlement negotiations under the standards set forth in the Federal Rules of Evidence and all applicable state counterparts, together with any applicable statutes protecting the confidentiality of mediations or settlement discussions. If the parties cannot agree on a mediator, the International Institute for Conflict Prevention and Resolution ("CPR"), at the written request of a party, shall designate a mediator.

Arbitration Procedures: If a Dispute has not been resolved within 90 days after the effective date of the written notice beginning the mediation process (or such longer period, if the parties so agree in writing), the mediation shall terminate and the Dispute shall be settled by binding arbitration to be held in Chicago, Illinois. The arbitration shall be solely between the parties and shall be conducted in accordance with the CPR Rules for Non-Administered Arbitration that are in effect at the time of the commencement of the arbitration, except to the extent modified by this Dispute Resolution Provision (the "Rules").

The arbitration shall be conducted before a panel of three arbitrators. Each of the Company and Deloitte & Touche LLP shall designate one arbitrator in accordance with the "screened" appointment procedure provided in the Rules, and the two party-designated arbitrators shall jointly select the third in accordance with the Rules. No arbitrator may serve on the panel unless he or she has agreed in writing to enforce the terms of the statement of work (including its appendices) to which this Dispute Resolution Provision is attached and to abide by the terms of this Dispute Resolution Provision. Except with respect to the interpretation and enforcement of these arbitration procedures (which shall be governed by the Federal Arbitration Act), the arbitrators shall apply the laws of the State of Washington (without giving effect to its choice of law principles) in connection with the Dispute. The arbitrators shall have no power to award punitive, exemplary, or other damages not based on a party's actual damages (and the parties expressly waive their right to receive such damages). The arbitrators may render a summary disposition relative to all or some of the issues, provided that the responding party has had an adequate opportunity to respond to any such application for such disposition. Discovery shall be conducted in accordance with the Rules.

All aspects of the arbitration shall be treated as confidential, as provided in the Rules. Before making any disclosure permitted by the Rules, a party shall give written notice to all other parties and afford such parties a reasonable opportunity to protect their interests. Further, judgment on the arbitrators' award may be entered in any court having jurisdiction.

Costs: Each party shall bear its own costs in both the mediation and the arbitration; however, the parties shall share the fees and expenses of both the mediators and the arbitrators equally.

APPENDIX C

This Appendix C is part of the engagement letter dated April 01, 2026 between Deloitte & Touche LLP and Microsoft.

CHANGE ORDER FORM

Date requested:	[insert details]
Title of request:	[insert details]

Change number:	[insert details]
Requested by:	[insert details]

This Change Order Form amends the Statement of Work between Microsoft Ireland Operations Limited, its affiliates, and its subsidiaries ("*Microsoft*" or "the Company") and Deloitte & Touche LLP ("*Supplier*") dated as of April 01, 2026 (the "*SOW*"). This Change Order Form is entered into between the same parties and is effective on [insert month, date, year] [the "*Change Order Effective Date*"]. This Change Order is subject to all of the terms and conditions in the SOW. The parties agree as follows:

Change requested in: (Check all that apply) ☐ **Specifications** ☐ **Deliverables** ☐ **Schedules** ☐ **Services** ☐ **Other**	**Affected Section #s of SOW, or name of other document:**

Description of change:

Reason for change:

Change(s) to SOW:

Section #	***Original language:***	***Replacing/supplementing language:***

Supplier approval

Print name/Title _____

Signature_____ Date _____

Microsoft approval: MICROSOFT IRELAND OPERATIONS LIMITED, on behalf of itself, its affiliates, and its subsidiaries

Print name/Title _____

Signature_____ Date _____

APPENDIX D

This Appendix D is part of the engagement letter dated April 01, 2026 between Deloitte & Touche LLP and Microsoft.

DATA PROTECTION

SECTION 1 Scope, Order of Precedence, and Term

(a) This Appendix modifies and supplements the terms and conditions in the Agreement as they relate to Supplier's Processing of Personal Data and compliance with Data Protection Law. Supplier is operating as an Independent Controller for the Personal Data it Processes under the Agreement. Notwithstanding anything to the contrary in the Agreement, if there is a conflict between this Appendix and the Agreement, this Appendix will control with respect to its subject matter.

(b) This Appendix applies to the extent that Supplier receives, stores, or Processes Personal Data or Confidential Information in connection with the Services.

SECTION 2 Definitions

(a) All capitalized terms not defined in this Appendix will have the meanings set forth in the Agreement.

(b) The following terms have the definitions given to them in the CCPA: "*Business*," "*Business Purpose,"* "*Sale*," "*Share,"* "*Service Provider*," "*Contractor*," and "*Third Party*."

(c) "*Controller*" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes a Business, Controller (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

(d) "*Data Exporter*" means the party that (1) has a corporate presence or other stable arrangement in a jurisdiction that requires an International Data Transfer Mechanism and (2) transfers Personal Data, or makes Personal Data available to, the Data Importer.

(e) "*Data Importer*" means the party that is (1) located in a jurisdiction that is not the same as the Data Exporter's jurisdiction and (2) receives Personal Data from the Data Exporter or is able to access Personal Data made available by the Data Exporter.

(f) "*Data Protection Law"* means any Law applicable to Supplier, in its performance of the Services, or Microsoft, in its receipt of the Services, relating to data security, data protection, and/or privacy, including, as may be applicable under the circumstances, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and the free movement of that data ("*GDPR*"), and Cal. Civ. Code Title 1.81.5, § 1798.100 et seq. (California Consumer Privacy Act) ("*CCPA*"), and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended, repealed and replaced, or re-enacted, in each case, having the effect of law.

(g) "*Data Subject*" means an identifiable natural person who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(h) *"De-identified Data"* means information that cannot reasonably be linked to an identified or identifiable individual.

(i) "*EEA*" means the European Economic Area.

(j) "*Personal Data*" means any information relating to an identified or identifiable natural person ("*Data Subject*") and any other data or information that constitutes personal data or personal information under any applicable Data Protection Law received from, or on behalf of the Company by Supplier in its performance of the Services. An identifiable natural person is one who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of

that natural person.

(k) "*Process*" or "*Processing*" means any operation or set of operations that a party performs on Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

(l) "*Processor*" means an entity that processes Personal Data on behalf of another entity. "Processor" includes Service Provider, Contractor, Processor (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

(m) "*Protected Health Information*" or "*PHI*" means the Company Personal Data that is protected by the Health Information Portability and Accountability Act (HIPAA).

(n) *"Pseudonymous Data"* means information that cannot be attributed to a specific individual without the use of additional information provided that it is kept separately and subject to appropriate technical and organizational measures to ensure that it is not attributed to the individual.

(o) "*Sensitive Data*" means the following types and categories of data: (1) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, immigration or citizenship status, or trade union membership; genetic data; (2) biometric data; (3) data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; (4) data concerning a natural person's sex life or sexual orientation; (5) government identification numbers (e.g., SSNs, driver's license); (6) payment card information; (7) nonpublic personal information governed by the Gramm Leach Bliley Act; (8) an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; (9) personal bank account numbers; (10) data related to children; and (11) precise geolocation.

(p) "*Standard Contractual Clauses*" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

(q) "*Subprocessor*" means a Processor engaged by a party who is acting as a Processor.

SECTION 3 Description of the Parties' Personal Data Processing Activities and Statuses of the Parties

(a) The subject matter and duration of the Processing, and the nature and purpose of the Processing, pertain to the Processing of Personal Data related to the provision of the Services reflected in the Agreement.

(b) Microsoft and Supplier operate as Independent Controllers for Processing of Personal under the Agreement.

(c) To the extent Personal Data has been transferred from the EEA, United Kingdom or Switzerland ("EEA/CH/UK") to a jurisdiction outside the EEA/CH/UK which is not recognized by the European Commission, UK Secretary of State or the relevant Swiss regulator as providing an adequate level of protection for personal data, and such transfer is not covered by an alternative International Data Transfer Mechanism (as such term is defined below), Module 1 of the Standard Contractual Clauses applies to the Processing of Personal Data under the Agreement, subject to the supplemental terms set forth in Schedule 1 hereto.

SECTION 4 International Data Transfer

(a) Some jurisdictions require that an entity transferring Personal Data to a recipient in another jurisdiction take extra measures to ensure that the Personal Data has special protections if the law of the recipient's jurisdiction does not protect Personal Data in a manner equivalent to the transferring entity's jurisdiction (an "*International Data Transfer Mechanism*"). The parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law and that is mutually agreed upon, including the Standard Contractual Clauses.

(b) If the International Data Transfer Mechanism on which the parties rely is invalidated or superseded, the parties will work together in good faith to find a suitable alternative.

(c) The parties agree that by executing this Agreement they also execute the Standard Contractual Clauses, which will be incorporated by reference and form an integral part of this Agreement. The parties agree that, with respect to the elements of the Standard Contractual Clauses that require the parties' input, Schedule 1 contains information relevant to the Standard Contractual Clauses' Annexes. The parties agree that, for Personal Data of Data Subjects in the United Kingdom, Switzerland, or another country specified in Schedule 1, they adopt the modifications to the Standard Contractual Clauses listed in Schedule 1 to adapt the Standard Contractual Clauses to local law, as applicable.

SECTION 5 Mutual Obligations of the Parties

(a) **Compliance**. The parties will comply with their respective obligations under Data Protection Law and their privacy notices, including by providing the same level of privacy protection that is required of Businesses under the CCPA.

(b) **Information.** Upon request, Supplier will provide reasonably relevant information to Microsoft to enable Microsoft to fulfill its obligations (if any) to conduct data protection assessments or prior consultations with data protection authorities.

(c) **Notification.** Supplier will notify Microsoft if it determines that it can no longer meet its obligations under applicable Data Protection Law.

(d) **Cooperation.** If Supplier receives any type of request or inquiry from a governmental, legislative, judicial, law enforcement, or regulatory authority, or faces an actual claim, inquiry, or complaint in connection with Parties' Processing of Personal Data provided to Supplier by or on behalf of Microsoft, its affiliates, or its respective end users, or obtained or collected by Supplier in connection with the purposes of this Agreement, then Supplier will notify Microsoft without undue delay, but in no event later than ten (10) business days, unless such notification is prohibited by applicable law. Supplier will promptly provide Microsoft with information relevant to the Inquiry reasonably requested by Microsoft, including any information relevant to the defense of a claim, to enable Microsoft to respond to the Inquiry.

(e) **Confidentiality**. Supplier will ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality obligations no less protective than those set forth in the Agreement or are under an appropriate statutory obligation of confidentiality.

(f) **Security Controls**. Supplier will take all measures required by applicable Data Protection Law relating to data security (including pursuant to Article 32 of the GDPR). Supplier will implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk.

SECTION 6 Supplier's Obligations as Independent Controller. As a Controller of Personal Data that is collected, exchanged, or otherwise Processed in connection with Supplier's performance of the Agreement:

(a) Supplier acknowledges and agrees that Supplier is independently responsible for compliance and will comply with applicable Data Protection Law (e.g., obligations of Controllers);

(b) Supplier will not Sell Personal Data;

(c) Supplier agrees to be responsible for providing notice to Data Subjects as may be required by applicable Data Protection Law (e.g., GDPR Articles 13 and 14, as applicable) and responding, as required by Data Protection Laws such as Chapter III of GDPR, to Data Subject's requests to exercise their rights and identifying a lawful basis of Processing (e.g., consent or legitimate interest);

(d) Supplier agrees that will keep Pseudonymous Data separate from any additional information necessary to make such Pseudonymous Data attributable to a specific individual and will subject such Pseudonymous Data to appropriate technical and organizational measures to ensure that it is not attributed to specific individual; and

(e) Supplier agrees that it will take reasonable measures to ensure that De-identified Data cannot be associated with a specific consumer or household, publicly commit to maintain the De-identified Data in de-identified form and not attempt to reidentify it, and contractually commit any Subprocessors to do the same**.**

SECTION 7 Supplier's Obligations as Third Party. If Supplier Processes Personal Data as a Third Party under the CCPA in connection with Supplier's performance of the Agreement, then:

(1) Supplier will Process Personal Data only for the limited and specific business purpose(s) described in the Agreement.

(2) Supplier agrees that the Personal Data is made available only for the limited and specified purpose(s) set forth in the Agreement, and Supplier may use the information only for those purposes.

(3) Supplier will not Sell or Share Personal Data made available to it by Microsoft.

Schedule 1 to Appendix D:

Information for International Transfers

Frequency of Transfer

Continuous for all Personal Data.

Retention Periods

As Controllers, the parties retain Personal Data for as long as they have a business purpose for it or for the longest time allowable by applicable law.

1. *For the purpose of the Standard Contractual Clauses:*
    - Clause 7: The parties do not adopt the optional docking clause.
    - Clause 8.2(c): Before disclosing a copy of the Standard Contractual Clauses, the disclosing party must redact all commercial terms including without limitation liability terms, Annex II, and any other detailed security terms.
    - Clause 11(a): The parties do not select the independent dispute resolution option.
    - Clause 17: The parties select Option 1. The parties agree that the governing jurisdiction is Republic of Ireland.
    - Clause 18: The parties agree that the forum is the High Court in Dublin, Ireland.
    - The Parties agree that the references to local law in the Standard Contractual Clauses include applicable professional standards.
    - For the avoidance of doubt, any limitations of liability, including limitations on indemnities, set forth in the Agreement apply with respect to liability arising under the Standard Contractual Clauses.
    - Nothing herein shall make Supplier responsible for the implementation and maintenance of any controls relating to the equipment or information systems of Microsoft. All such controls shall be the responsibility of Microsoft except as otherwise expressly agreed in an applicable SOW.
    - Annex I(A): The data exporter is the Data Exporter (defined above) and the data importer is the Data Importer (defined above).
    - Annex I(B): The parties agree that Schedule 1 describes the transfer.
    - Annex I(C): The competent supervisory authority is the Irish Data Protection Commission.
    - Annex II: The parties agree that Schedule 2 describes the technical and organizational measures applicable to the transfer.

2. *For the purpose of localizing the Standard Contractual Clauses the terms in Section 1 above shall apply except to the extent modified below:*
    - Switzerland
        - The parties adopt the GDPR standard for all data transfers.
        - Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified above.
        - Clause 17: The parties agree that the governing jurisdiction is Republic of Ireland.
        - Clause 18: The parties agree that the forum is the High Court in Dublin, Ireland. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).
        - The parties agree to interpret the Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.
    - United Kingdom

- "UK SCC Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK's Information Commissioner's Office under S119A(1) Data Protection Act 2018, as modified by the Information Commissioner's office from time to time, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

- For transfers from the United Kingdom that are not subject to an adequacy decision or exception, the parties hereby incorporate the UK SCC Addendum by reference and, by signing this DPA, also enter into and agree to be bound by the Mandatory Clauses of the UK SCC Addendum.
- The parties agree that the following information is relevant to Tables 1 – 4 of the UK SCC Addendum and that by changing the format and content of the Tables neither party intends to reduce the Appropriate Safeguards (as defined in the UK SCC Addendum).
    - Table 1: The parties' details, key contacts, data subject contacts, and signatures are in the signature block of the DPA.
    - Table 2: The selected SCCs, Modules and Selected Clauses are described in Schedule 1.
    - Table 3: The list of parties, description of transfer, and list of sub-processors are described in Schedule 1. The Technical and Organizational measures to ensure the security of the data are described in Schedule 2.
    - Table 4: Neither party may end the UK SCC Addendum when the Approved Addendum changes.
- Clause 17 of the Standard Contractual Clauses: The parties agree that the governing jurisdiction is the United Kingdom.
- Clause 18 of the Standard Contractual Clauses: The parties agree that the forum is the courts of England and Wales. The parties agree that Data Subjects may bring legal proceedings against either party in the courts of any country in the United Kingdom.

Schedule 2 to Appendix D:



DeloitteInformation SecurityStatement.p

APPENDIX E

This Appendix E is part of the engagement letter dated April 01, 2026, between Deloitte & Touche LLP and Microsoft.

INFORMATION SUBJECT TO EXAMINATION

Subject Matter on Which Management's Assertion is Based	*Criteria*
To be mutually agreed upon by the parties during the course of the engagement. Such subject matter and Criteria will be based upon the measures set out in Chapter III Articles 45 and 46 of the DSA and the crisis protocols referred to in Article 48, and Microsoft's commitments and measures under the Code of Conduct on Disinformation (COCD), combined with Microsoft's benchmarks as required in the Delegated Regulation supplementing Regulation (EU) 2022/2065.	

Appendix 5 – Documents relating to the audit risk analysis

Purpose

This document summarizes the risk assessment performed for the assessment of compliance with each audited obligation or commitment, including the assessment of inherent risks, control risks, and detection risks for each audited obligation and commitment (i.e., each sub-article).

DSA and Code of Conduct Risk Assessment Requirements

1) The audit report shall include a substantiated audit risk analysis performed by the auditing organization for the assessment of the Audited Provider's compliance with each audited obligation or commitment.
2) The audit risk analysis shall be carried out prior to the performance of audit procedures and shall be updated during the performance of the audit, in the light of any new audit evidence which, according to the professional judgement of the auditing organization, materially modifies the assessment of the audit risk.
3) The audit risk analysis shall consider:
    a. Inherent risks
    b. Control risks
    c. Detection risks

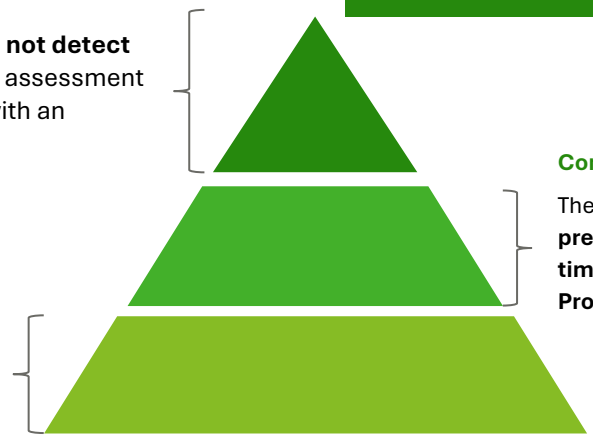
Misstatement – an intentional or unintentional omission, misrepresentation, or error in the declarations or data Reported or provided by the Audited Provider to the audit provider, or in the testing environment made available by the Audited Provider to the audit provider.

Detection Risk

The risk that the **auditor provider does not detect a misstatement** that is relevant for the assessment of the Audited Provider's compliance with an audited obligation or commitment.

Inherent Risk

The risk of **non-compliance intrinsically related to the nature, the design, the activity, and the use of the audited service,** as well as the context in which it is operated, and the risk of non-compliance related to the nature of the audited obligation or commitment.



Control Risk

The risk that a **misstatement is not prevented, detected, and corrected in a timely manner** by **means of the Audited Provider's internal controls.**

4) The audit risk analysis shall be conducted considering:
    a. the nature of the audited service and the societal and economic context in which the audited service is operated, including probability and severity of exposure to crisis situations and unexpected events.
    b. the nature of the obligations and commitments.
    c. other appropriate information, including:
        - where applicable, information from previous audits to which the audited service was subjected.

- where applicable, information from reports issued by the European Board for Digital Services or guidance from the Commission, including guidelines issued pursuant to Article 35.2 and 35.3 of Regulation (EU) 2022/2065, and any other relevant guidance issued by the Commission with respect to the application of Regulation (EU) 2022/2065.
- where applicable, information from audit reports published pursuant to Article 42.4 of Regulation (EU) 2022/2065 by other providers of very large online platforms or of very large online search engines operating in similar conditions or providing similar services to the audited service.

Overview

Risk assessment procedures were performed to help identify risks of material misstatement and plan out the nature, timing, and extent of our audit procedures.

Risk Assessment Steps performed:

1. **We obtained an understanding of the systems and processes (and related controls) put in place to comply with the Specified Requirements and other engagement circumstances.**

Understanding the subject matter is key to planning and executing an effective engagement. We obtain our understanding during planning and update it throughout the performance of the engagement to the extent that changes affect our overall engagement strategy or the nature, timing, and extent of our procedures.

We obtained an understanding sufficient to:

- Enable us to identify and assess the risks of material misstatement.
- Provide a basis for designing and performing procedures to respond to the assessed risks and to obtain reasonable assurance to support our opinion.

Information obtained to inform the audit risk analysis:

Described in Article 9	Information obtained, included, but not limited to:
The nature of the audited service and the societal and economic context in which the audited service is operated, including probability and severity of exposure to crisis situations and unexpected events.	• The transparency reports • Systemic Risk Assessment • Information from Audited Provider (website, voice-over, annual report, trust, and safety reports) • Microsoft Bing Reports from COCD Transparency Centre
The nature of the obligations and commitments in Chapter 3 of the DSA	Any documentation by the Audited Provider concerning the scope including: • Systemic Risk Assessment • Data flowcharts • The audit risk and control framework • COCD Subscription Document
Other appropriate information, including, where applicable, information from previous audits to which the audited service was subjected.	Any documentation from previous audits to which the audited service was subjected: • Internal audit reports concerning the DSA or COCD or covering topics in the DSA or COCD • 2025 Microsoft Bing DSA Audit Report • 2025 Microsoft Bing DSA Audit Report - Redacted • 2025 Bing Systemic Risk Assessment Report • 2025 Bing DSA Audit Implementation Report (AIR)

Other appropriate information, including, where applicable, information from reports issued by the European Board for Digital Services or guidance from the Commission, including guidelines issued pursuant to Article 35.2 and 35.3 of Regulation (EU) 2022/2065, and any other relevant guidance issued by the Commission with respect to the application of Regulation (EU) 2022/2065.	None identified
Other appropriate information, including, where applicable, information from audit reports published pursuant to Article 42.4 of Regulation (EU) 2022/2065 by other providers of very large online platforms or of very large online search engines operating in similar conditions or providing similar services to the audited service.	• 2025 Microsoft Bing DSA Audit Report • 2025 Microsoft Bing DSA Audit Report - Redacted • 2025 Bing Systemic Risk Assessment Report • 2025 Bing DSA Audit Implementation Report (AIR)

2. We determined whether the risk factors we identify are inherent risks that may give rise to risks of material misstatement associated with the subject matter. We obtained an understanding by performing procedures, including reviews of relevant information, inquiries, data analytics, observations, and inspections.

We obtained an understanding of how management prepares certain information, such as their risk assessment to comply with Article 34. We also obtained an understanding of management's process for determining the risks that would prevent the Specified Requirements from being achieved, and for designing and implementing processes and controls to address those risks. The Audited Provider has a formal risk assessment process to comply with Article 34, and other requirements.

We obtained an understanding of the components of the system of internal control at the entity level is an important step in performing our risk assessment procedures, as it helped us identify events and conditions that may have a pervasive effect on the susceptibility of the subject matters of our report to misstatement, either due to fraud or error. We obtained an understanding how Bing's system of internal controls operates at the entity level, including:

- Control environment
- Monitoring activities
- Managements risk assessment process

3. For each obligation and commitment, we assessed inherent, control and detection risks

See below for the determination of inherent, control and detection risks.

4. Revision of Risk Assessment

In some instances, our assessment of the risks of material misstatement changed during the engagement as additional evidence is obtained. In circumstances in which we obtain evidence from performing further procedures, or when new information is obtained, either of which is inconsistent with the evidence on which we originally based the assessment, we revised the assessment and modified the planned procedures accordingly.

Determination and assessment of inherent, control and detection risks for each obligation (i.e., sub article):

Digital Services Act: Overview of risk assessment during the initial and final phases, unless otherwise specified:

Obligations	Inherent risk	Control risk	Testing strategy[2]	Detection risk
11.1	Low	Low	Controls and substantive procedures	Low
11.2	Low	Low	Controls and substantive procedures	Low
11.3	Low	Low	Controls and substantive procedures	Low
12.1	Low	Low	Controls and substantive procedures	Low
12.2	Low	Low	Controls and substantive procedures	Low
14.1	Low	Low	Controls and substantive procedures	Low
14.2	Low	Low	Controls and substantive procedures	Low
14.4	Medium	High	Controls and substantive procedures	Medium
14.5	Low	Low	Controls and substantive procedures	Low
14.6	Low	Low	Controls and substantive procedures	Low
15.1 – Initial	Medium	High	Controls and substantive procedures	Medium
15.1 – Final	High	High	Substantive procedures only	High
24.2 – Initial	Medium	High	Controls and substantive procedures	Medium
24.2 – Final	Medium	High	Substantive procedures only	Medium
24.3	Medium	High	Substantive procedures only	Medium
34.1	Medium	High	Controls and substantive procedures	Medium
34.2	Medium	High	Controls and substantive procedures	Medium
34.3	Low	Low	Controls and substantive procedures	Low
35.1	Medium	High	Controls and substantive procedures	Medium
36.1	Medium	Low	Controls and substantive procedures	Low
37.1	Low	Low	Substantive procedures only	Low

[2] D&T evaluated the controls to assess their design and implementation, as well as to support the risk assessment process.

Obligations	Inherent risk	Control risk	Testing strategy[2]	Detection risk
37.2	Low	Low	Substantive procedures only	Low
37.3	Low	Low	Substantive procedures only	Low
37.4	Low	Low	Substantive procedures only	Low
37.5	Low	Low	Substantive procedures only	Low
37.6	Low	Low	Substantive procedures only	Low
38	High	Medium	Controls and substantive procedures	Medium
39.1	Medium	High	Controls and substantive procedures	Medium
39.2	Medium	High	Controls and substantive procedures	Medium
39.3 – Initial	High	High	Controls and substantive procedures	High
39.3 – Final	Medium	High	Controls and substantive procedures	Medium
40.1	Low	Medium	Controls and substantive procedures	Low
40.3	Low	Medium	Controls and substantive procedures	Low
40.4	Low	Medium	Controls and substantive procedures	Medium
40.5	Low	Medium	Controls and substantive procedures	Medium
40.6	Low	Medium	Controls and substantive procedures	Medium
40.7	Low	Medium	Controls and substantive procedures	Medium
40.12	Low	Medium	Controls and substantive procedures	Low
41.1	Medium	Low	Controls and substantive procedures	Low
41.2	Medium	Low	Controls and substantive procedures	Low
41.3 – Initial	Medium	Low	Controls and substantive procedures	Low
41.3 – Final	Medium	Medium	Controls and substantive procedures	Low
41.4	Medium	Low	Controls and substantive procedures	Low
41.5	Medium	Low	Controls and substantive procedures	Low
41.6	Medium	Low	Controls and substantive procedures	Low
41.7	Medium	Low	Controls and substantive procedures	Low
42.1 – Initial	Medium	Low	Controls and substantive procedures	Low

Obligations	Inherent risk	Control risk	Testing strategy[2]	Detection risk
42.1 – Final	Medium	Low	Substantive procedures only	Low
42.3 – Initial	Medium	High	Controls and substantive procedures	Medium
42.3 – Final	Medium	High	Substantive procedures only	Medium
42.4	Medium	Medium	Substantive procedures only	Medium
42.5	Medium	Medium	Substantive procedures only	Low

Code of Conduct on Disinformation: Overview of risk assessment during the initial and final phases, unless otherwise specified:

Commitments / Measures	Inherent risk	Control risk	Testing strategy[3]	Detection risk
Measure 16.1	Medium	Medium	Substantive procedures only	Medium
Measure 18.2	Medium	Medium	Substantive procedures only	Medium
Measure 19.1	High	Medium	Controls and substantive procedures	Medium
Measure 19.2	High	Medium	Controls and substantive procedures	Medium
Measure 20.2	Low	Low	Substantive procedures only	Low
Measure 22.2	High	Medium	Controls and substantive procedures	Medium
Measure 22.3	High	Medium	Controls and substantive procedures	Medium
Measure 22.7	Medium	Medium	Controls and substantive procedures	Medium
Measure 26.1	Medium	Medium	Controls and substantive procedures	Medium
Measure 26.3	Medium	Medium	Controls and substantive procedures	Medium
Measure 28.2	Low	Medium	Controls and substantive procedures	Medium
Measure 28.3	Low	Medium	Controls and substantive procedures	Medium
Measure 34.1	Low	Low	Substantive procedures only	Low
Measure 34.2	Low	Low	Substantive procedures only	Low
Measure 34.3	Low	Low	Substantive procedures only	Low
Measure 34.4	Medium	Medium	Substantive procedures only	Low
Measure 34.5	Medium	Medium	Substantive procedures only	Low
Measure 35.1	Low	Medium	Substantive procedures only	Low
Measure 35.2	Low	Medium	Substantive procedures only	Low
Measure 35.3	Low	Medium	Substantive procedures only	Low

[3] D&T evaluated the controls to assess their design and implementation, as well as to support the risk assessment process.

Commitments / Measures	Inherent risk	Control risk	Testing strategy[3]	Detection risk
Measure 35.4	Low	Medium	Substantive procedures only	Low
Measure 37.1	Low	Low	Substantive procedures only	Low
Measure 37.2	Medium	Medium	Substantive procedures only	Medium
Measure 37.4	Low	Low	Substantive procedures only	Low
Measure 37.5	Low	Low	Substantive procedures only	Low
Measure 37.6	Low	Low	Substantive procedures only	Low
Commitment 38	Low	Low	Controls and substantive procedures	Low
Measure 40.1	Medium	Medium	Substantive procedures only	Medium
Measure 40.3	Medium	Medium	Substantive procedures only	Medium
Measure 40.4	Low	Low	Substantive procedures only	Low
Measure 40.5	Low	Low	Substantive procedures only	Low
Measure 40.6	Low	Low	Substantive procedures only	Low
Commitment 42	Medium	Medium	Substantive procedures only	Medium
Commitment 43	Low	Low	Substantive procedures only	Low

Appendix 6 – Documents attesting that the auditing organization complies with the obligations laid down in Article 37.3 point (a), (b), (c)

DSA and COCD Annex	Response
Documents attesting that the auditing organization complies with the obligations laid down in Article 37.3.a of Regulation (EU) 2022/2065.	We are required to be independent and to meet other ethical responsibilities in accordance with the Code of Professional Conduct established by the American Institute of Certified Public Accountants ("AICPA") and the International Ethics Standards Board of Accountants' Code of Ethics for Professional Accountants (including International Independence Standards). We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control. Additionally, pursuant to Article 37.3.a, we confirm that we have not performed non-audit services related to the subject matter of this engagement. Further, we have been Microsoft's DSA auditor since 2024; additionally, we were engaged as the auditor for Microsoft's first COCD audit during this Examination Period. Lastly, we confirm that we are not receiving a contingent fee based on the outcome of this audit.
Documents attesting that the auditing organization complies with the obligations laid down in Article 37.3.b of Regulation (EU) 2022/2065.	In compliance with Article 37.3.b, we confirm that our team possesses the necessary knowledge, skills, and professional diligence under ISAE/AICPA standards, which were applied throughout the engagement. The team includes certified professionals (Chartered Accountants, Certified Public Accountants, Certified Information Systems Auditors, Certified Information Systems Security Professionals, Health Information Trust Alliance Certified Common Security Framework Practitioners) and individuals experienced in data science and data privacy regulations.
Documents attesting that the auditing organization complies with the obligations laid down in Article 37.3.c of Regulation (EU) 2022/2065.	We maintain independence and met ethical responsibilities in line with the American Institute of Certified Public Accountants "AICPA" Code of Professional Conduct and the International Ethics Standards Board for Accountants' Code (including International Independence Standards). We also applied International Standard on Quality Management I "ISQM 1", AICPA Statements on Quality Control Standards, and IAASB International Standards on Quality Management, maintaining a comprehensive quality control system with documented policies and procedures for compliance with ethical, professional, legal, and regulatory requirements.

Appendix 7 – Documentation and results of any tests performed by the auditing organization, including as regards algorithmic systems of the Audited Provider

Documentation and results of any tests performed by the auditing organization, including as regards algorithmic systems of the Audited Provider	
Documentation and results of any tests performed by the auditing organization, including as regards algorithmic systems of the Audited Provider.	A description of the audit procedures performed, the methodologies used to assess compliance, and a justification of the choice of those procedures and methodologies can be found in Appendix 1A, Sections 1-6 (Audit Criteria label) in the Independent Accountant's Report - Digital Services Act and Appendix 1B, Sections 1-10 (Audit Criteria label) in the Independent Accountant's Report – Code of Conduct on Disinformation.

Appendix 8 – Definitions

For purposes of this assurance report the following terms have meanings attributed below:	
Assurance Engagement	An engagement in which a practitioner aims to obtain sufficient appropriate evidence to express a conclusion designed to enhance the degree of confidence of the intended users other than the VLOSE about the subject matter information (that is, the outcome of the measurement or evaluation of an underlying subject matter against criteria).
Audit Criteria	The benchmarks used to measure or evaluate the underlying subject matter.
Audited Obligation or Commitment	An obligation or commitment referred to in Obligation 37.1 of Regulation (EU) 2022/2065 which forms the subject matter of the audit. Unless noted otherwise, each sub article is an audited obligation or commitment.
Auditing Organization	An individual organization, a consortium or other combination of organizations, including any sub-contractors, that the audited provider has contracted to perform an independent audit in accordance with Article 37 of Regulation (EU) 2022/2065.
Auditing Procedure	Any technique applied by the auditing organization in the performance of the audit, including data collection, the choice and application of methodologies, such as tests and substantive analytical procedures, and any other action taken to collect and analyze information to collect audit evidence and formulate audit conclusions, not including the issuing of an audit opinion or of the audit report.
Audited Provider	The provider of an audited service which is subject to independent audits pursuant to obligation 37.1 of that Regulation.
Audit Risk	The risk that the auditing organization issues an incorrect audit opinion or reaches an incorrect conclusion concerning the Audited Provider's compliance with an audited obligation or commitment, considering detection risks, inherent risks and control risks with respect to that audited obligation or commitment.
Audited Service	A very large online platform or a very large online search engine designated in accordance with Article 33 of Regulation (EU) 2022/2065.
Evidence	Information used by the practitioner in arriving at the practitioner's conclusion. Evidence includes both information contained in relevant information systems, if any, and other information.
Intended Users	The individual(s) or organization(s), or group(s) thereof that the practitioner expects will use the assurance report.
Internal Control	Any measures, including processes and tests, that are designed, implemented and maintained by the Audited Provider, including its compliance officers and management body, to monitor and ensure the Audited Provider's compliance with the audited obligation or commitment.
Materiality Threshold	The threshold beyond which deviations or misstatements by the Audited Provider, individually or aggregated, would reasonably affect the audit findings, conclusions and opinions.
Measure	A defined implementation activity prescribed by the Code of Conduct on Disinformation and subscribed to by a Signatory, designed to operationalize and support the achievement of a Commitment.

Professional Judgement	The application of relevant training, knowledge, and experience, within the context provided by assurance and ethical standards, in making informed decisions about the courses of action that are appropriate in the circumstances of the engagement.
Qualitative Reporting Element (QRE)	A prescribed qualitative reporting requirement under the Code of Conduct on Disinformation intended to provide information regarding the design, implementation, or operation of a Measure.
Service Level Indicator (SLI)	A prescribed quantitative metric intended to provide information regarding the implementation, performance, reach, or effectiveness of a Measure in the Code of Conduct on Disinformation.
Substantive Analytical Procedure	An audit methodology used by the auditing organization to assess information to infer audit risks or compliance with the audited obligation or commitment.

Sources used: ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information, Commission Delegated Regulation (EU), Article 2, Code of Conduct on Disinformation