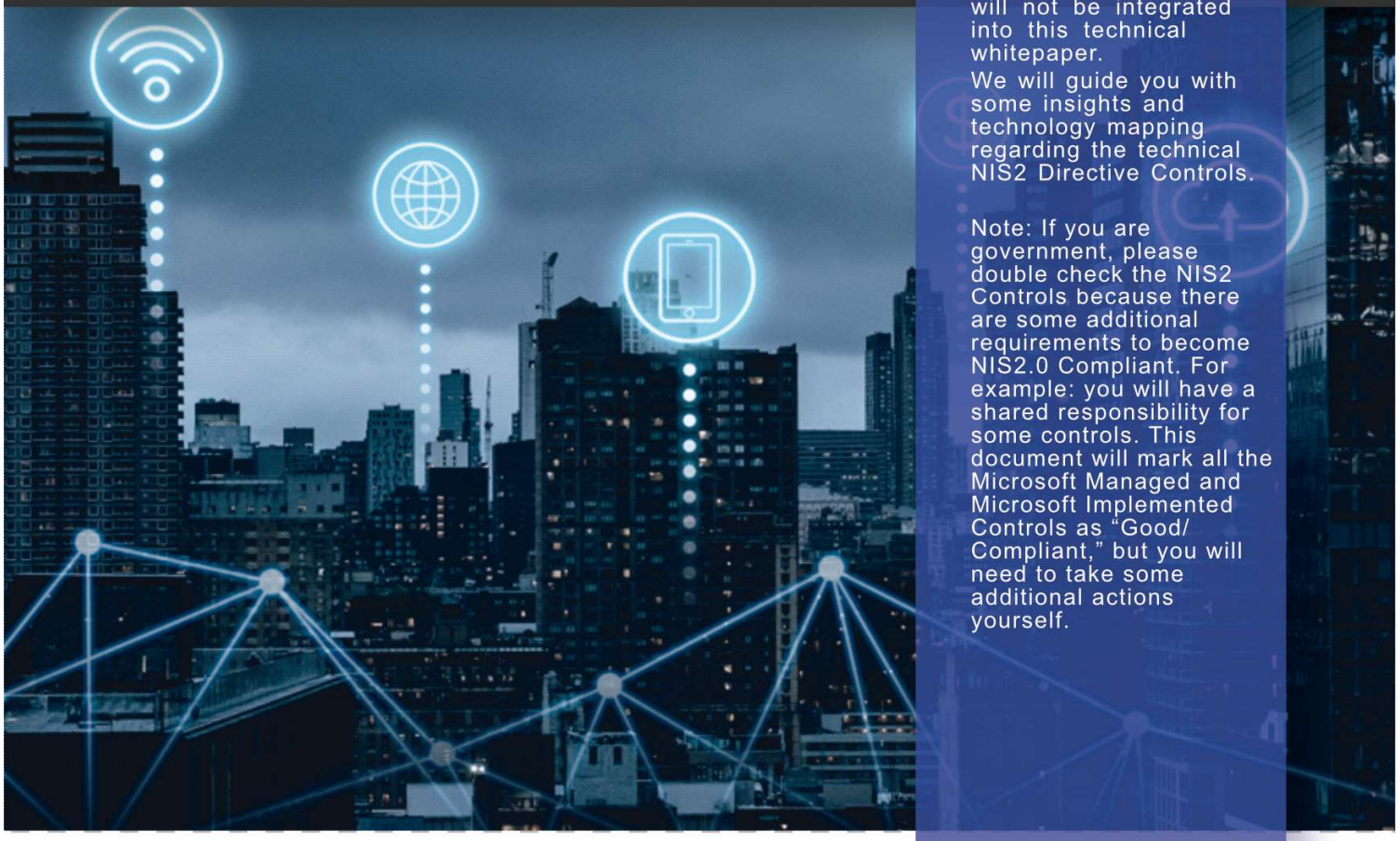
2024

Publication 1.0

NIS2 for Microsoft 365

Technical Whitepaper



OFFICIAL RELEASE

This Document designed based on the Microsoft Purview NIS2 Directive (EU) 2022/2555 Assessment as of the 1st of March 2024. All changes after this date will not be integrated into this technical whitepaper.

We will guide you with some insights and technology mapping regarding the technical NIS2 Directive Controls.

Note: If you are government, please double check the NIS2 Controls because there are some additional requirements to become NIS2.0 Compliant. For example: you will have a shared responsibility for some controls. This document will mark all the Microsoft Managed and Microsoft Implemented Controls as “Good/ Compliant,” but you will need to take some additional actions yourself.

BY ITCOWBOYS.NL

Disclaimer

This document is provided to you as an example of how you can meet the technical requirements from the NIS2 Directive to your Microsoft 365 Tenant.

This document does not provide you with any legal rights or official compliance for NIS2 Standard, please make sure all your processes and other information is also NIS2 Compliant. We do not give any guarantees about passing NIS2 Compliance audits when implemented this Whitepaper.

TABLE OF CONTENTS

INTRODUCTION

This Document designed based on the Microsoft Purview NIS2 Directive (EU) 2022/2555 Assessment as of the 1st of March 2024. All changes after this date will not be integrated into this technical whitepaper.

We will guide you with some insights and technology mapping regarding the technical NIS2 Directive Controls. **Note:** If you are government, please double check the NIS2 Controls because there are some additional requirements to become NIS2.0 Compliant. For example: you will have a shared responsibility for some controls. This document will mark all the Microsoft Managed and Microsoft Implemented Controls as "Good/Compliant," but you will need to take some additional actions yourself.

We also highly recommend having a nice and secure Microsoft Tenant configuration that will exceed the limits of the NIS2 Directive. Just follow the known Zero Trust principals and you should have a good technical base to work with!

To get started please make sure you have common knowledge about Microsoft Defender XDR and SIEM (Sentinel) and layer the recommendations/actions from this Technical Whitepaper on top of these products!

Who are the ITCowboys?

ITCowboys consists of two highly enthusiastic and technically skilled professionals who love to share and inspire knowledge and Best Practices to everyone who follows our community. ITCowboys was born on the 1st of January 2024, and brought to life by Jordy Herber and Paul Erlings.

We consistently Blog on our Website and LinkedIn, provide you with a bi-weekly Podcast and now also provide you with some in depth information, how-to's, Best Practices and Code Examples on GitHub!

The ITCowboys consist of two members: Paul Erlings and Jordy Herber

Jordy Herber: Jordy is an exceptional hands-on Microsoft Cloud & Security Architect and a Technical Expert. His main area is the Modern Workspace with a focus on Microsoft Defender XDR.

You can find Jordy on his LinkedIn Page.

Paul Erlings: Paul is a Principal Consultant for Security & Compliance and a Security Architect. He loves everything within the Microsoft ecosystem and is a true expert.

You can find Paul on his LinkedIn Page

What is the NIS2 Directive?

Introduced in 2020, and recently coming into effect on January 16, 2023, the NIS2 Directive is a continuation and expansion of the previous EU cybersecurity directive, NIS. It was proposed by the European Commission to build upon and rectify the deficiencies of the original NIS directive.

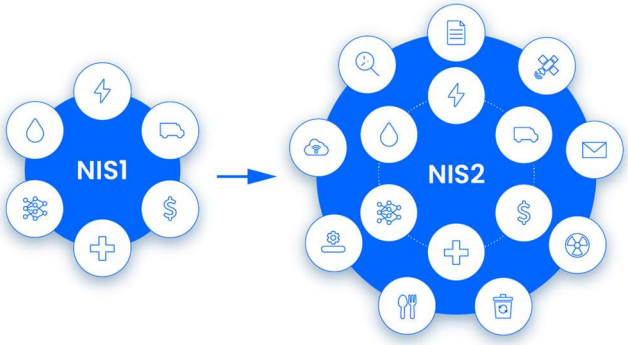
NIS2 aims to enhance the security of network and information systems within the EU by requiring operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities.

Compared to NIS, NIS2 expands its EU-wide security requirements and scope of covered organizations and sectors to improve the security of supply chains, simplify reporting obligations, and enforce more stringent measures and sanctions throughout Europe.

To bolster Europe's resilience against current and future cyberthreats, the NIS2 Directive introduces new requirements and obligations for organizations in four overarching areas: risk management, corporate accountability, reporting obligations, and business continuity.

Risk Management

To comply with the new Directive, organizations must take measures to minimize cyber risks. These measures include incident management, stronger supply chain security, enhanced network security, better access control, and encryption.



Corporate Accountability

NIS2 requires corporate management to oversee, approve, and be trained on the entity's cybersecurity measures and to address cyber risks. Breaches may result in penalties for management, including liability and a potential temporary ban from management roles.

Reporting Obligations

Essential and important entities must have processes in place for prompt reporting of security incidents with significant impact on their service provision or recipients. NIS2 sets specific notification deadlines, such as a 24-hour "early warning".

Business Continuity

Organizations must plan for how they intend to ensure business continuity in the case of major cyber incidents. This plan should include considerations about system recovery, emergency procedures, and setting up a crisis response team.

10 Minimum Measures

In addition to the four overarching areas of requirement, NIS2 mandates that essential and important entities implement baseline security measures to address specific forms of cyberthreats. These include:

- Risk assessments and security policies for information systems
- Policies and procedures for evaluating the effectiveness of security measures.
- Policies and procedures for the use of cryptography and, when relevant, encryption.
- A plan for handling security incidents
- Security around the procurement of systems and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.
- Cybersecurity training and a practice for basic computer hygiene.
- Security procedures for employees with access to sensitive or important data, including policies for data access. Affected organizations must also have an overview of all relevant assets and ensure that they are properly utilized and handled.
- A plan for managing business operations during and after a security incident. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.
- The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.
- Security around supply chains and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.

Organizations Affected by NIS2

NIS2 affects all entities that provide essential or important services to the European economy and society, including companies and suppliers. We highly recommend you to carefully assess the following categories to determine if NIS2 is applicable to your organization.

The Official NIS2 release Date

The deadline for Member States to transpose the NIS2 Directive into applicable, national law is 17 October 2024.

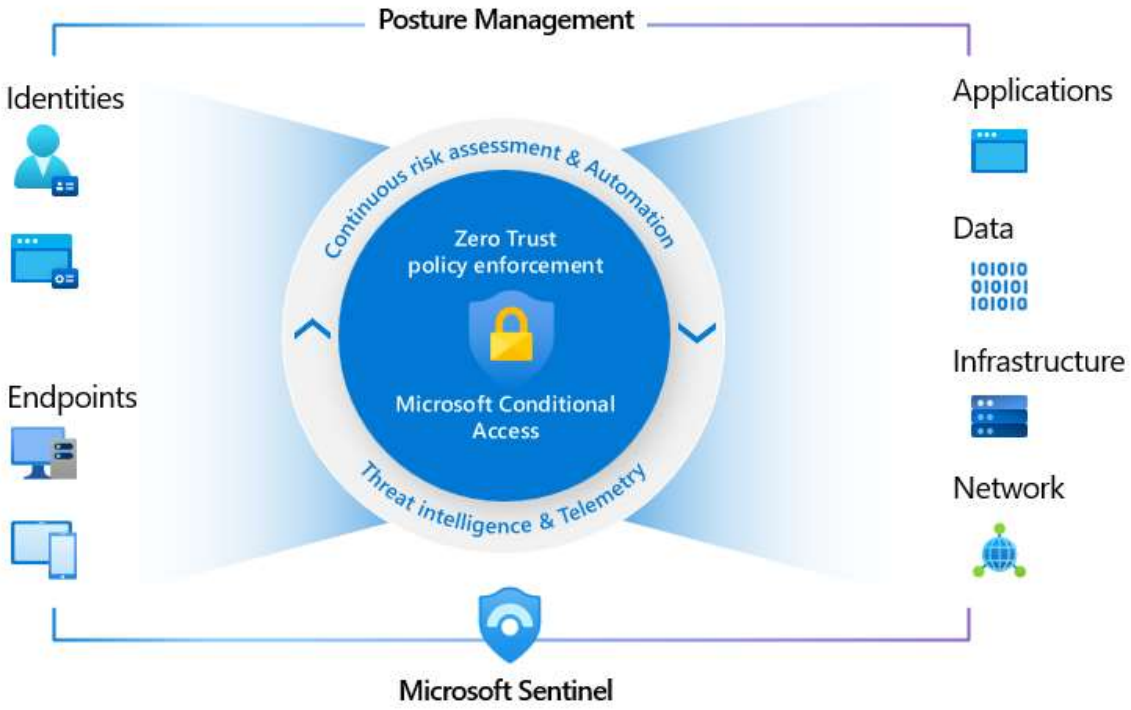
This is a crucial deadline for businesses, as failure to comply with the NIS2 directive can result in severe consequences, including financial penalties and damage to reputation. It is therefore essential that companies are fully prepared and compliant before the deadline date.

Technology mapping

In the NIS 2.0 there are ten duties defined that organizations that are subject to the NIS 2.0 directive will have to implement.

In this document we focus only on these duties and what an organization with Microsoft 365 and/or Microsoft Azure can start with today. The purpose of this document is to visualize the technology components towards the NIS2 but is not exhaustive. We have selected technologies and features that can help with the duties, but other solutions or features may be available.

We will map the different duties on the Microsoft Zero Trust model, as shown on below:



NIS 2.0 Duties:

(a) policies on risk analysis and information system security.

(b) incident handling.

(c) business continuity, such as backup management and disaster recovery, and crisis management.

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

(e) security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure.

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

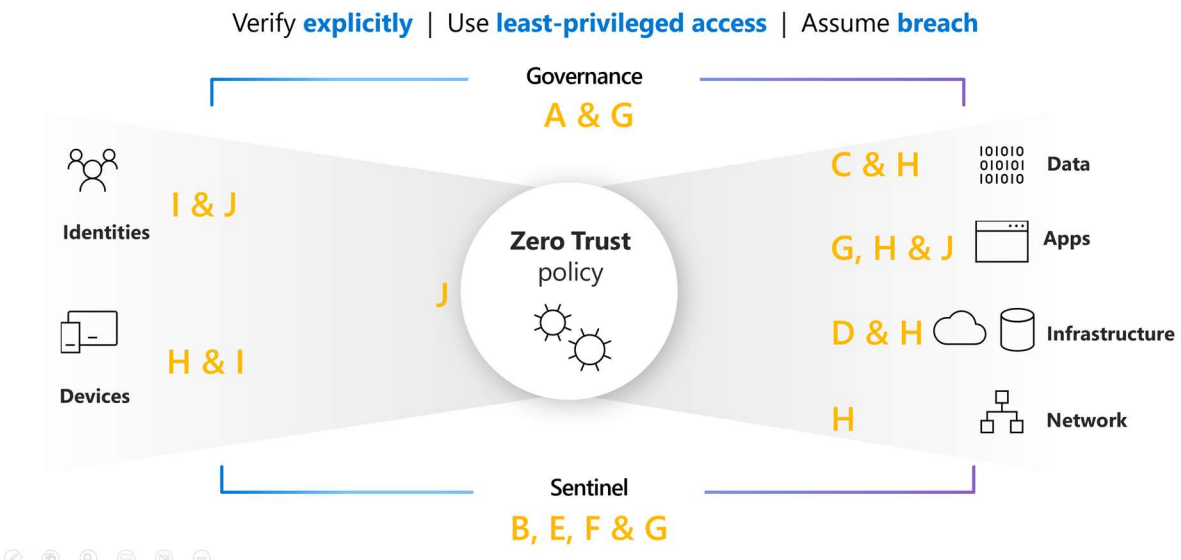
(g) basic cyber hygiene practices and cybersecurity training.

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption.

(i) human resources security, access control policies and asset management.

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Mapping NIS 2.0 Duties to the Microsoft Zero Trust

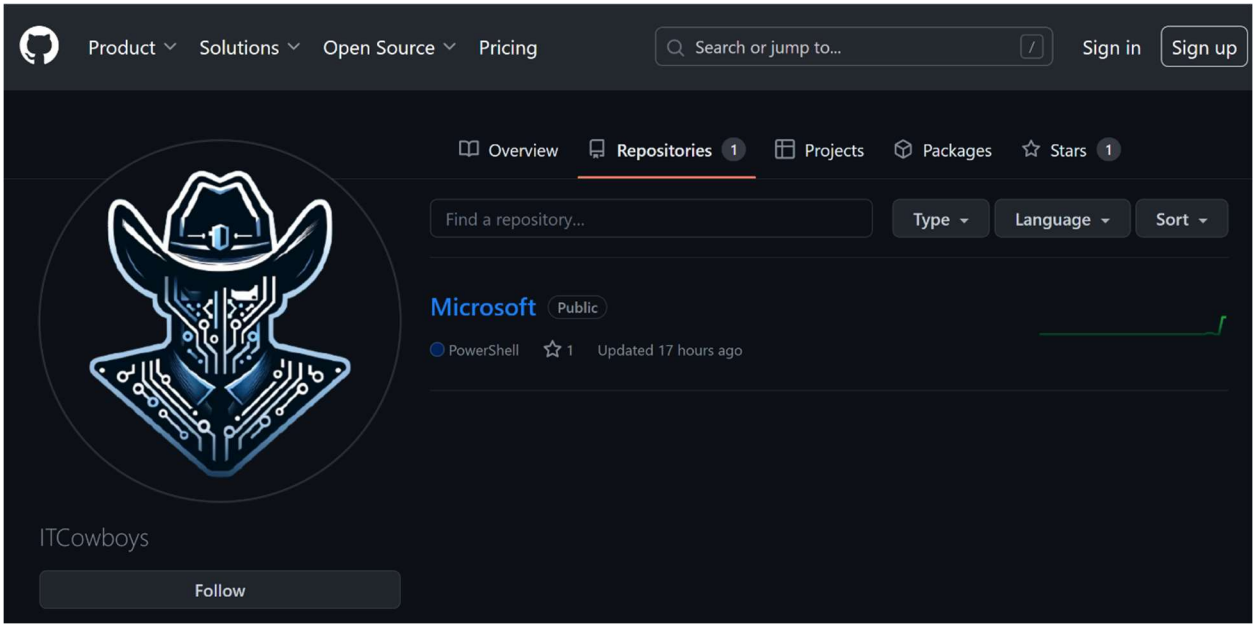


Additional Resources

Next to this document we want to provide you with some ready to go guides for implementing the right technologies as shown in the previous Technology Mapping. All the technologies that applicable to be used based on the NIS2 Duties are shown below:

On GitHub have the following technical best practices

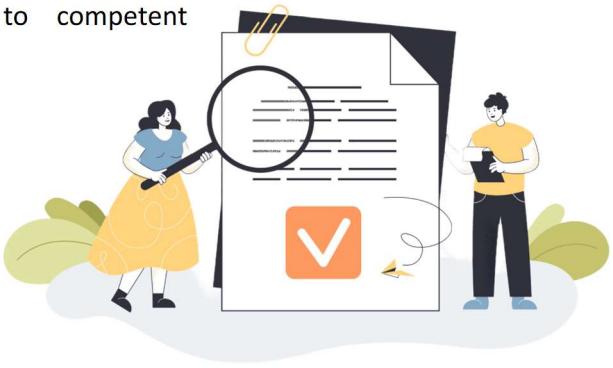
- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft Defender XDR Tenant Settings
- Microsoft Sentinel
- Microsoft Intune (Coming Soon)
- Microsoft Defender Vulnerability Management (Coming Soon)
- Microsoft Defender for DevOps (Coming Soon)
- Microsoft Defender for Identity (Coming Soon)
- Purview Information Protection
- Bring Your Own Key
- Data Lifecycle Management (Coming Soon)
- Customer Key
- Cloud Security Posture Management (Coming Soon)
- Microsoft 365 & Azure Backup (Coming Soon)
- Microsoft 365 Archiving (Coming Soon)
- Disaster Recovery - Azure Site Recovery & Microsoft365DSC (Coming Soon)
- Microsoft Entra Lifecyle Management (Coming Soon)
- Microsoft Entra Entitlement Management (Coming Soon)
- Microsoft Entra Access Reviews
- Privileged Identity Management
- Conditional Access (Coming Soon)



NIS2 DIRECTIVE CUSTOMER ACTIONS

There are 15 Controls that need to be fulfilled by the Customer themselves (Based on the Microsoft Purview NIS2 Directive (EU) 2022/2555 Assessment) The Customer Actions state the following:

- Liaison function for cross-border and cross-sectoral cooperation
- Risk management measures for essential and important entities
- Require regular cybersecurity training for management and employees.
- Identify crisis response capabilities.
- Required information submission by entities to competent authorities.
- ENISAs Biennial Cybersecurity Report
- Policy Recommendations in ENISAs Report
- Methodology for Aggregated Assessments by ENISA
- Reporting Mechanism for Significant Incidents by Entities
- Criteria for Significant Incidents
- Promotion of European and international standards
- Enforcement powers over essential entities



These Actions translate in the following technical Improvement actions:

- **Assign trainings and send reminders.**

Microsoft recommends that your organization assign training to the user and send training reminders when training completion is due. This functionality makes sure that users in your organization complete their trainings on regular basis before deadlines. It allows administrators to assign trainings to users as well as send reminders on precautionary steps of attack like phishing, social engineering etc.

How to Use Microsoft Solutions to Implement Your organization can use Attack Simulation Training via "Microsoft 365 Defender" portal for assigning training and sending reminders when training is due for completion. Select Launch Now to visit the portal. Navigate to "Email & collaboration" > "Attack simulation training" > "Simulations". Select "Launch a simulation" to start the new simulation wizard. Configure the relevant settings, then to assign trainings, on the "Assign training page", configure "Select training content preference", "Redirect to a custom URL" and "No training". When you are finished on the "Assign training page", select "Next".

- **Automate alert notifications.**

Microsoft recommends that your organization implement mechanisms to identify and set alerts for organization-defined activities, such as privileged permissions abuse, malware detection, and potential external and internal threats. This will help strengthen the security of the organization against any potential threat loss.

How to Use Microsoft Solutions to Implement Your organization can use Audit via the "Microsoft Purview" portal to create and view alert policies and to send notifications on activities that may indicate a potential security incident or data breach. Select Launch Now to visit the portal. Navigate to "Policies" > "Alert" > "Alert policies". To create alert policies, you must be assigned the "Manage Alerts role" or the "Organization Configuration role" in the Microsoft 365 compliance center.

- **Collect and analyze information about cyber threats.**

Microsoft recommends that your organization use a threat intelligence tool to collect and analyze information about indicators of past, current, and future cyber threats. Threat intelligence enables your organization to take a proactive approach to managing threats.

How to Use Microsoft Solutions to Implement Your organization can use Microsoft Defender for Office 365 via "Microsoft 365 Defender" to track threats for threat intelligence. Your threat intelligence could include the addition of Microsoft Defender for Office 365 and the use of ATP Threat Trackers to provide intelligence on different cybersecurity issues that might impact your company. Select Launch Now to visit the portal. Navigate to "Email & collaboration" > "Threat Tracker" within the portal.

- **Create an Insider Risk Management Policy**

Microsoft recommends that your organization create a new insider risk management policy to manage security and compliance. Insider Risk Management correlates various notifications, alerts, or signals to identify potentially malicious or inadvertent insider risks, such as IP theft, data leakage and security violations.

How to Use Microsoft Solutions to Implement Your organization can use Insider Risk Management via "Microsoft Purview" to create a new insider risk management policy. Select Launch Now and go to "Insider Risk Management" and select the "Policies" tab. Select "Create Policy" to open the policy wizard. Complete all the steps to create a new policy.

- **Create data transfer policies to support privacy goals.**

Microsoft recommends that your organization create automated policies to detect and handle situations in which data is transferred across departments or regional borders.

How to Use Microsoft Solutions to Implement Your organization can use Priva Privacy Risk Management to create a privacy management policy for data overexposure. Select Launch Now to access the "Policies" dashboard. From there select "Create a policy" and select the "Data transfer" default policy. You can View and Edit settings to customize the policy before testing or enabling it. You can also set user email notifications to send users direct notifications about policy matches and important tasks to complete. The recipients will receive email digests that summarize data to be reviewed and actions, such as making documents private, keeping them on file, reporting any false-positive matches, and adding notes for future reference. These emails also include links for training recipients on how to handle these cases. Providing these links is required when initially setting up notifications and should point to your own internal documentation on processes and best practices.

- **Manage contact information.**

Microsoft recommends your organization to manage the contact information to keep it updated. It might take up to 24 hours to take effect across all services. In case of any changes the information must be kept updated by the organization for right information display.

How to Use Microsoft Solutions to Implement Your organization can use Microsoft 365 admin center to Remove a guest user. Select Launch Now to visit the portal. Go to the "Users > Active users" page. Select the user from the list of active users. Select "Manage contact information". Change the display name and select "Save changes".

- **Manage security related incidents.**

Microsoft recommends that your organization view and manage security related incidents.

How to Use Microsoft Solutions to Implement Your organization can manage Microsoft Defender for Endpoint incidents via Microsoft 365 Defender Portal. Select Launch Now, to go to the Incidents page, select an incident in the "Incidents queue" which will bring up the "Incident management pane" where you can open the incident page for details. The Incidents queue shows a collection of incidents that were flagged from devices in your network. It helps you sort through incidents to prioritize and create an informed cybersecurity response decision.

- **Prioritize incident response using Sensitivity Labels**

Microsoft recommends that your organization use sensitivity labels to prioritize incident response.

How to Use Microsoft Solutions to Implement. Your organization can use Microsoft Defender for Endpoint to Prioritize incident response using sensitivity labels. Select Launch Now and click on "Incidents & Alerts" > "Incidents". Scroll to the right to see the "Data sensitivity" column and open incident page to further investigate. Select the "Devices" tab to identify devices storing files with sensitivity labels. Select the devices that store sensitive data and search through the timeline to identify which files are impacted to take appropriate action to ensure that data is protected.

- **Review audit data**

Microsoft recommends that your organization regularly review and search the compliance audit log for any signs of a breach or malicious activity. Regularly consuming and reviewing audit records makes it less likely that an attacker can operate in your tenant undetected for long periods of time.

How to Use Microsoft Solutions to Implement Your organization can use the Microsoft Purview solution to review and search the audit log. Select Launch Now to access the Audit solution to search and review audit log data and look for any signs of a breach or malicious activity.

- **Run simulation attacks.**

Microsoft recommends that your organization simulate realistic attack scenarios to help identify vulnerabilities before a real attack impacts your bottom line. It is also recommended that your organization form a red team and perform attack simulations manually. Your organization should consider participating in cyber drills conducted by recognized expert computer emergency response/readiness team (CERT) or computer incident response team (CIRT) groups.

How to Use Microsoft Solutions to Implement. Your organization can use Microsoft 365 Defender "Attack Simulation training" in the Microsoft 365 Defender to run realistic attack scenarios in your organization. Select Launch Now to access "Attack simulation training", where you can run realistic phishing attempts such as spear phishing and password attacks.

- **View incident summary**

Microsoft recommends that your organization display the summary of an incidents that shows the full scope of the attack, how the attack spread through your network over time, where it started, and how far the attacker went. This is helpful to view all details regarding summary of attacks happened over the network more effectively.

How to Use Microsoft Solutions to Implement. Your organization may use Microsoft 365 Defender to view incident summary. Select Launch Now then go to the "Incidents" under "incidents & alerts". Selecting an incident name displays the entire attack story of the incident, including Alert page within incident Graph You can view the entity details directly from the graph and act on them. The additional tab for an incident "Summary" contains a quick overview of the impacted assets associated with alerts

NIS2 DIRECTIVE MICROSOFT ACTIONS

There are 84 Controls that are fulfilled by Microsoft (Based on the Microsoft Purview NIS2 Directive (EU) 2022/2555 Assessment) The Microsoft Actions state the following:

- Account Management - Conditions for Group/Role Membership
- Account Management - Notification of Need-To-Know Change
- Alternate Work Site - Employee Communication with Security Personnel
- Audit and Accountability Policy and Procedures - Creating Policy
- Audit Events - Capability to Audit
- Audit Events - Coordination
- Audit Events - Rational for Adequacy
- Audit Review, Analysis, and Reporting - Integration / Scanning and Monitoring
- Audit Review, Analysis, and Reporting - Reporting
- Authenticator Management - In-Person or Trusted Third-Party Registration
- Contingency Plan - Coordinate with Related Plans
- Contingency Plan - Coordination of Activities
- Contingency Plan - Recovery Objectives, Restoration Priorities, Metrics
- Contingency Plan Testing - Coordinate with Related Plans
- Continuous Monitoring - Response Actions
- Continuous Monitoring - Security Status Reporting
- Controlled Maintenance - Security Control Check
- Correlation with External Organizations
- Development Process, Standards, and Tools
- External Information System Services - Monitor Compliance by External Service Providers
- External Information Systems - Processing, Storage, and Service Location
- External Information Systems - Risk Assessments/ Organizational Approvals - Conduct Risk Assessment
- Flaw Remediation - Remediates Flaws
- Incident Handling - Automated Incident Handling Processes
- Incident Handling - Continuity of Operations
- Incident Monitoring
- Incident Reporting - Authority
- Incident Reporting - Automated Reporting
- Incident Reporting - Required Timeframe
- Incident Response Assistance
- Incident Response Assistance - Coordination with External Providers - Identification of Team Members
- Incident Response Assistance - Coordination with External Providers - Relationship with External Providers
- Incident Response Plan - Communication of Plan Changes
- Incident Response Plan - Component of Overall Organization
- Incident Response Plan - Organizational Requirements

- Incident Response Plan - Plan Distribution
- Incident Response Plan - Reportable Incidents
- Incident Response Plan - Resources and Management Support
- Incident Response Plan - Roadmap for Implementation
- Incident Response Plan - Structure and Organization
- Incident Response Policy and Procedures - Creating Policy
- Incident Response Policy and Procedures - Creating Procedures
- Incident Response Policy and Procedures - Reviewing Policy
- Incident Response Policy and Procedures - Reviewing Procedures
- Information in Shared Resources
- Information Sharing - Assisting Sharing Decision Making
- Information Sharing - User Discretion
- Information System Documentation - Documentation Protection
- Physical Access Control - Audit Logs
- Position Risk Designation - Criteria for Filling These Positions
- Resource Availability
- Response to Audit Processing Failures - Additional Actions
- Risk Assessment - Conduct Risk Assessment
- Risk Assessment - Disseminate Results to Defined Personnel
- Risk Assessment - Document Assessment Results
- Risk Assessment - Review Results
- Risk Assessment - Update Assessments: Changes, Impacting Conditions
- Risk Assessment Policy and Procedures - Creating Policy
- Risk Assessment Policy and Procedures - Creating Procedures
- Risk Assessment Policy and Procedures - Reviewing Policy
- System and Information Integrity Policy and Procedures - Creating Policy
- System Security Plan - Plan/ Coordinate with Other Organizational Entities
- System Security Plan - Update Plan to Address Changes
- Transmission Confidentiality and Integrity
- Vulnerability Scanning - Share Vulnerability Information with Defined Personnel to Help Other Systems

NIS2 DIRECTIVE (EU) CONTROLS

Below you will find an overview of all the 142 Controls which are covered by the NIS2.0 Detective. These Controls might be Implemented and Managed by Microsoft or Managed/Need to be Implemented by the Customer.

We divided the controls with two colors:

Out of Scope	Implemented/Good

Please check if the implementation requirements meet your organization's vertical. For example: Government needs additional implementation requirements.

Competent authorities and single points of contact

Designate competent cybersecurity authorities.

Article	8.1
Description	Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities)
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Designate single points of contact.

Article	8.3
Description	Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Endure adequate resources for authorities.

Article	8.5
Description	Member States shall ensure that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 servers are configured to limit the use of processor and memory resources by process priority. This is a built-in feature of the Windows OS. Additionally, service teams monitor processor and memory utilization spikes and initiate the incident response process if spikes threaten the health of Office 365. Also, process and memory resources are capped per tenant, which prevents any single tenant from interfering with the availability of other tenant's services. Resource caps are "soft caps" meaning that under non-duress operation the processes can use whatever resources they need. Under duress (system is at >=97% CPU or <3% available mem) a service called PUMA applies a system enforced throttle per process. This is evaluated every hour and removed once the system is out of the duress state. The per process throttle is based on past usage and agreement with the component team owners. If a tenant has hit the process and / or memory cap usage is throttled back to acceptable level. The intent of the soft caps is to maintain critical customer facing operations at all costs. Processor and memory resources management are inherited from pre-existing FedRAMP Authorization for Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).

Liaison function for cross-border and cross-sectoral cooperation

Article	8.4
Description	Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Computer security incident response teams (CSIRTs)

Designate and establish computer security incident response teams (CSIRTs)

Article	10.1
Description	Each Member State shall designate or establish one or more CSIRTs. The CSIRTs may be designated or established within a competent authority. The CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Enable CSIRT cooperation with entities.

Article	10.4
Description	The CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 29 with sectoral or cross-sectoral communities of essential and important entities.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for only sharing government customer content with properly authenticated government customer users. There are two mechanisms by which government customers could potentially share government customer content with non-authorized users i.e. guest access to SFB meetings and SharePoint Online Guest access. Guest access to SFB meetings, if enabled, allows anyone with a meeting invite to access the meeting lobby. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting. Government customers are responsible for disabling guest access to SFB meetings to remain compliant with FedRAMP standards as advised in “Office 365 MT Government Compliance Considerations v2 00 . Non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see: https://docs.microsoft.com/en-us/powershell/module/skype/Set-CsMeetingConfiguration SharePoint Online guest invitations allow external users to access an organization’s SharePoint site(s). Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online, as an account type, should be allowed for their organization. Government customers are responsible for disabling guest access to SharePoint Online to remain compliant with FedRAMP standards. The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers. For more information, see the Microsoft 365 Solution and Architecture Center: https://docs.microsoft.com/en-us/microsoft-365/solutions Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365. O365: A detailed list of specific technical mechanisms implemented within Office 365 to prevent unauthorized and unintended information transfer via shared system resources is documented in "Tenant Isolation in Office 365". Shared resources in Office 365 require each Office 365 user (including Office 365 service team administrators, customer administrators, and customer users) to hold a unique Active Directory (AD) identifier. Access to shared resources is governed by explicit access allocation, and information is segregated between Office 365 user sessions through AD and Azure Active Directory (AAD).

Enable CSIRTs to provide international assistance.

Article	10.8
Description	The CSIRTs may cooperate with third countries’ national computer security incident response teams or equivalent third-country bodies, for the purpose of providing them with cybersecurity assistance.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 SIR team coordinates with peer teams inside MSIT and Azure as required for incidents internal to Microsoft. Coordination with third party entities is addressed in the ISAs with those groups for incidents that may cross organizational boundaries. The Office 365 SIR team coordinates with customers as required consistent with the reporting timeframes outlined. The Office 365 SIR team tracks all coordinated incidents.

Ensure adequate resources for CSIRTs.

Article	10.2
Description	Member States shall ensure that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3).
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Establish international CSIRT cooperation.

Article	10.7
Description	The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers who choose to share their information/content are responsible for employing automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. O365: Office 365 employees are not allowed to share Office 365 data or customer content outside the security boundary and thus do not make discretionary sharing decisions.

Facilitate effective CSIRT network cooperation.

Article	10.6
Description	The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 Security Incident & Response (SIR) team maintains a list of incident response contacts for all partner organizations, including: organizations internal to Microsoft, incident response POCs within partner organizations covered via ISAs, and customer incident response contacts. These partner organizations are also provided direct contact information for the Office 365 SIR team.

Mandate CSIRT participation in peer reviews

Article	10.5
Description	Rules of Behavior - Review/Update Rules
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for ensuring that government customer users acknowledge and sign the government customer's rules of behavior for Office 365 MT. O365: Microsoft and Office 365 review and update the Employee Handbook, the NDA, and the Office 365 Rules of Behavior annually.

Notify commission of the identity and tasks of the CSIRT

Article	10.9
Description	Each Member State shall notify the Commission without undue delay of the identity of the CSIRT referred to in paragraph 1 of this Article and the CSIRT designated as coordinator pursuant to Article 12(1), of their respective tasks in relation to essential and important entities, and of any subsequent changes thereto.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Updates are made to the Office 365 System Security Plan as changes are made to the system or the operating environment to ensure the plan represents an accurate depiction of the Office 365 security posture.

Provide secure communication infrastructure for CSIRTS.

Article	10.3
Description	The organization develops an incident response plan that describes the structure and organization of the incident response capability.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Request assistance from ENISA for CSIRT development

Article	10.10
Description	The organization develops an incident response plan that meets the unique requirements of the organization, which relate to mission, size, structure, and functions.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Cooperation at national level

Coordinate with various national and EU bodies

Article	13.4
Description	In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Ensure computer security incident response teams (CSIRTs) receive notifications of significant incidents.

Article	13.2
Description	Member States shall ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats and near misses pursuant to Article 30.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams utilize alternate processing site agreements in accordance with the organization's availability requirements. Recovery Time Objectives (RTO) are established for services and are detailed as part of the Business Continuity Management (BCM) process. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Office 365 service.

Ensure intra-state cooperation among authorities.

Article	13.1
Description	The organization develops, documents, and disseminates to [Assignment: organization-defined personnel or roles] procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Exchange information between competent authorities

Article	13.5
Description	Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including about relevant incidents and cyber threats.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Inform single points of contact about incidents.

Article	13.3
Description	The organization develops an incident response plan that defines reportable incidents.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams utilize alternate processing site agreements in accordance with the organization's availability requirements. Recovery Time Objectives (RTO) are established for services and are detailed as part of the Business Continuity Management (BCM) process. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Office 365 service.

Simplify mandatory and voluntary reporting systems.

Article	13.6
Description	Member States shall simplify the reporting through technical means for notifications referred to in Articles 23 and 30.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 SIR team reports incidents to designated authorities (including US-CERT) consistently with NIST SP 800-61 as documented in the Office 365 SIR Plan.

Cooperation Group

Allow technical reports requests by Cooperation Group

Article	14.6
Description	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Any new deficiencies that are identified from the security control assessments are documented in the POA&M. The POA&M is continuously updated and used to report on the security state of the information system as part of monthly Office 365 operational service readiness reviews. POA&M updates are provided to customers monthly.

Annual meeting with Critical Entities Resilience Group

Article	14.9
Description	The Cooperation Group shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group established under Directive (EU) 2022/2557 to promote and facilitate strategic cooperation and the exchange of information.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for only sharing government customer content with properly authenticated government customer users. There are two mechanisms by which government customers could potentially share government customer content with non-authorized users i.e. guest access to SFB meetings and SharePoint Online Guest access. Guest access to SFB meetings, if enabled, allows anyone with a meeting invite to access the meeting lobby. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting. Government customers are responsible for disabling guest access to SFB meetings to remain compliant with FedRAMP standards as advised in “Office 365 MT Government Compliance Considerations v2 00 . Non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see: https://docs.microsoft.com/en-us/powershell/module/skype/Set-CsMeetingConfiguration SharePoint Online guest invitations allow external users to access an organization’s SharePoint site(s). Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online, as an account type, should be allowed for their organization. Government customers are responsible for disabling guest access to SharePoint Online to remain compliant with FedRAMP standards. The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers. For more information, see the Microsoft 365 Solution and Architecture Center: https://docs.microsoft.com/en-us/microsoft-365/solutions Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365

Biennial work program establishment by Cooperation Group

Article	14.7
Description	By 1 February 2024 and every two years thereafter, the Cooperation Group shall establish a work program in respect of actions to be undertaken to implement its objectives and tasks.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for ensuring that government customer users acknowledge and sign the government customer's rules of behavior for Office 365. Non-government customers may not be required to have rules of behavior. O365: All full-time employees and contingent staff must sign appropriate agreements to acknowledge the terms and conditions of their employment and their understanding and acceptance of the Microsoft corporate employment policies. All Office 365 staff are required to sign confidentiality and non-disclosure agreements (NDA), as well as the Microsoft Employee Handbook, at the time of hire as a condition for employment. A signed confirmation from Microsoft users indicating understanding and agreement of the NDA is required of all staff upon hire to Microsoft. Office 365 service team administrators are provided with all of these documents as part of annual security awareness training. Completion of the training constitutes employee acknowledgement and understanding of these documents and is used in place of a signature. Additionally, the training ends with a test to verify the user's understanding; passing the test is required and results are tracked by Office 365.

Biennial work programs for Cooperation Group

Article	14.2
Description	The Cooperation Group shall carry out its tasks on the basis of biennial work programs referred to in paragraph 7.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Business Continuity Management (BCM) teams coordinate with the Office 365 Security Incident & Response (SIR) team when determining plan requirements. Each plan includes instructions for coordinating plan execution with the incident handling process.

Composition of the Cooperation Group

Article	14.3
Description	The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation. Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work. The Commission shall provide the secretariat.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: All customers, including government and non-government customers, are responsible for establishing conditions for group/role membership for their organization in compliance with their organizational policies. Government and non-government customers using ADFS will configure their groups/roles in their existing Active Directory infrastructure. Non-government customers not using ADFS will configure groups in AAD via SUE. For more information on managing customer groups/roles in AAD via the SUE portal, see the following link: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/user-account-management O365: Service teams establish conditions for group/role membership by defining and enforcing conditions for each group/role in account management tools. In addition, service teams use JIT Tools to enforce additional, more granular conditions for privilege escalation and approval for interactive sessions. Office 365 establishes conditions for group and role membership based on least privilege necessary for a user to perform their assigned duties. Predetermined conditions are established when groups are created.

Define Tasks of the Cooperation Group

Article	14.4
Description	Separation of Duties - Role Definition The organization defines information system access authorization to support separation of duties.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Access authorization to support separation of duties is implemented through authorized role membership. Role membership is managed using account management tools.

Ensure Cooperation in the Cooperation Group

Article	14.5
Description	Member States shall ensure effective, efficient, and secure cooperation of their representatives in the Cooperation Group.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: All customers, including government and non-government customers, are responsible for establishing conditions for group/role membership for their organization in compliance with their organizational policies. Government and non-government customers using ADFS will configure their groups/roles in their existing Active Directory infrastructure. Non-government customers not using ADFS will configure groups in AAD via SUE. For more information on managing customer groups/roles in AAD via the SUE portal, see the following link: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/user-account-management O365: Service teams establish conditions for group/role membership by defining and enforcing conditions for each group/role in account management tools. In addition, service teams use JIT Tools to enforce additional, more granular conditions for privilege escalation and approval for interactive sessions. Office 365 establishes conditions for group and role membership based on least privilege necessary for a user to perform their assigned duties. Predetermined conditions are established when groups are created.

Establish the Cooperation Group

Article	14.1
Description	To support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: All customers, including government and non-government customers, are responsible for establishing conditions for group/role membership for their organization in compliance with their organizational policies. Government and non-government customers using ADFS will configure their groups/roles in their existing Active Directory infrastructure. Non-government customers not using ADFS will configure groups in AAD via SUE. For more information on managing customer groups/roles in AAD via the SUE portal, see the following link: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/user-account-management O365: Service teams establish conditions for group/role membership by defining and enforcing conditions for each group/role in account management tools. In addition, service teams use JIT Tools to enforce additional, more granular conditions for privilege escalation and approval for interactive sessions. Office 365 establishes conditions for group and role membership based on least privilege necessary for a user to perform their assigned duties. Predetermined conditions are established when groups are created.

Coordinated vulnerability disclosure and a European vulnerability database.

Create European vulnerability database.

Article	12.2
Description	The organization develops, documents, and disseminates to [Assignment: organization-defined personnel or roles] a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Designate CSIRT as vulnerability disclosure coordinator

Article	12.1
Description	The organization shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 Security provides a reporting interface to allow authorized Office 365 personnel to see the details of vulnerabilities associated with the environment. The reporting interface provides high-level / technical reports (covering information such as servers, vulnerabilities, CVE IDs, breakdowns of vulnerable hosts, and remediation steps, etc.). Vulnerability reporting to government customers is accomplished through continuous monitoring reporting processes identified in CA-7.

CSIRTs network

Biennial assessment by network of CSIRTs

Article	15.4
Description	By 17 January 2025, and every two years thereafter, the CSIRTs network shall, for the purpose of the review referred to in Article 40, assess the progress made about the operational cooperation and adopt a report. The report shall draw up conclusions and recommendations based on the outcome of the peer reviews referred to in Article 19, which are carried out in relation to the national CSIRTs. That report shall be submitted to the Cooperation Group.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Microsoft employs a FedRAMP-approved 3PAO as an independent assessor to conduct a security control assessment of Office 365 and its components.

Composition of the CSIRTs Network

Article	15.2
Description	The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for only sharing government customer content with properly authenticated government customer users. There are two mechanisms by which government customers could potentially share government customer content with non-authorized users i.e., guest access to SFB meetings and SharePoint Online Guest access. non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. Government and non-government customers can configure this setting. For more information, see: https://docs.microsoft.com/en-us/powershell/module/skype/Set-CsMeetingConfiguration O365: A detailed list of specific technical mechanisms implemented within Office 365 to prevent unauthorized and unintended information transfer via shared system resources is documented in "Tenant Isolation in Office 365". Shared resources in Office 365 require each Office 365 user (including Office 365 service team administrators, customer administrators, and customer users) to hold a unique Active Directory (AD) identifier. Access to shared resources is governed by explicit access allocation, and information is segregated between Office 365 user sessions through AD and Azure Active Directory (AAD).

Define Tasks of the CSIRTs Network

Article	15.3
Description	The organization develops an incident response plan that describes the structure and organization of the incident response capability.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Establish national network of CSIRTs.

Article	15.1
Description	To contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 Security Incident & Response (SIR) team maintains a list of incident response contacts for all partner organizations, including: organizations internal to Microsoft, incident response POCs within partner organizations covered via ISAs, and customer incident response contacts. These partner organizations are also provided direct contact information for the Office 365 SIR team.

Procedural arrangements between CSIRTs network and EU-CyCLONe

Article	15.2
Description	The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for only sharing government customer content with properly authenticated government customer users. There are two mechanisms by which government customers could potentially share government customer content with non-authorized users i.e., guest access to SFB meetings and SharePoint Online Guest access. non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. Government and non-government customers can configure this setting. For more information, see: https://docs.microsoft.com/en-us/powershell/module/skype/Set-CsMeetingConfiguration The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers. For more information, see the Microsoft 365 Solution and Architecture Center: https://docs.microsoft.com/en-us/microsoft-365/solutions Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365. O365: A detailed list of specific technical mechanisms implemented within Office 365 to prevent unauthorized and unintended information transfer via shared system resources is documented in "Tenant Isolation in Office 365". Shared resources in Office 365 require each Office 365 user (including Office 365 service team administrators, customer administrators, and customer users) to hold a unique Active Directory (AD) identifier. Access to shared resources is governed by explicit access allocation, and information is segregated between Office 365 user sessions through AD and Azure Active Directory (AAD).

Cybersecurity information-sharing arrangements

ENISAs Assistance in Information-Sharing Arrangements

Article	29.5
Description	ENISA shall aid with the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers may choose to share their information/content in accordance with their security policies and are responsible for enabling authorized customer users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information being shared. O365: Office 365 employees are not allowed to share Office 365 data or customer content outside the security boundary.

Establishment of cybersecurity information-sharing arrangements

Article	29.3
Description	The information system prevents unauthorized and unintended information transfer via shared system resources.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers may choose to share their information/content in accordance with their security policies and are responsible for enabling authorized customer users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information being shared. O365: Office 365 employees are not allowed to share Office 365 data or customer content outside the security boundary.

Information Exchange Within Communities of Entities

Article	29.2
Description	Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers may choose to share their information/content in accordance with their security policies and are responsible for enabling authorized customer users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information being shared. O365: Office 365 employees are not allowed to share Office 365 data or customer content outside the security boundary.

Notification requirements for participation in information-sharing

Article	29.4
Description	Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering such arrangements, or, as applicable, of their withdrawal from such arrangements once the withdrawal takes effect.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for only sharing government customer content with properly authenticated government customer users. There are two mechanisms by which government customers could potentially share government customer content with non-authorized users i.e., guest access to SFB meetings and SharePoint Online Guest access. non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. Government and non-government customers can configure this setting. For more information, see: https://docs.microsoft.com/en-us/powershell/module/skype/Set-CsMeetingConfiguration The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers. For more information, see the Microsoft 365 Solution and Architecture Center: https://docs.microsoft.com/en-us/microsoft-365/solutions Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365. O365: A detailed list of specific technical mechanisms implemented within Office 365 to prevent unauthorized and unintended information transfer via shared system resources is documented in "Tenant Isolation in Office 365". Shared resources in Office 365 require each Office 365 user (including Office 365 service team administrators, customer administrators, and customer users) to hold a unique Active Directory (AD) identifier. Access to shared resources is governed by explicit access allocation, and information is segregated between Office 365 user sessions through AD and Azure Active Directory (AAD).

Voluntary Exchange of Cybersecurity Information

Article	29.1
Description	The organization employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers who choose to share their information/content are responsible for employing automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. O365: Office 365 employees are not allowed to share Office 365 data or customer content outside the security boundary and thus do not make discretionary sharing decisions.

Commissions implementing acts on technical requirements.

Article	21.5
Description	The organization requires the developer of the information system, system component, or information system service to follow a documented development process that explicitly addresses security requirements.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: All development in Microsoft Office 365 must follow the SDL process detailed in SA-03 for all engineering and development projects. The SDL process includes the following: Addressing security requirements: The Requirements phase of the SDL includes the project inception—when the organization considers security and privacy at a foundational level—and a cost analysis—when determining if development and support costs for improving security and privacy are consistent with business needs. Identifying standards and tools/documents tools and configurations: The Implementation phase is when the organization creates the documentation and tools the customer uses to make informed decisions about how to deploy the software securely. To this end, the Implementation phase is when the organization establishes development best practices to detect and remove security and privacy issues early in the development cycle. Documents, manages, and ensures the integrity of changes: During the Verification phase, the organization ensures that the code meets the security and privacy tenets established in the previous phases. This is done through security and privacy testing, and a security push—which is a team-wide focus on threat model updates, code review, testing, and thorough documentation review and edit. A public release privacy review is also completed during the Verification phase. O365: Microsoft Office 365 reviews the SDL process on an ongoing basis to ensure that the process, standards, and tools selected and employed provide sufficient security for all systems and software developed and released by Microsoft.

Consideration of supplier and service provider vulnerabilities

Article	21.3
Description	The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Corrective measures for non-compliance

Article	21.4
Description	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for ensuring that customer users are using secure browsers and properly patched information systems to access Office 365. Customer Responsibility (W365): Government customers utilizing W365 services are responsible for identifying, reporting, and correcting information system flaws on their own VMs. O365: Office 365 identifies, reports, and corrects information system flaws through vulnerability management, incident response management, and patch/configuration management processes. The Office 365 Security Incident Response Program assists with identifying and reporting of information system flaws. Office 365 receives vulnerability-related data from multiple sources of information which include: Microsoft Security Resource Center (MSRC), vendor Web sites, other third-party services (e.g., Internet Security Systems) and internal/external vulnerability scanning of services. Office 365 Security will determine which updates are applicable within the Office 365 environment. Potential changes are tested in advance. Patching schedules are defined by Office 365 Security to install security-relevant software and firmware updates within 30 days for high vulnerabilities, 90 days for moderate vulnerabilities. Office 365 inherits firmware changes from Azure, which is responsible for firmware updates to the Office 365 infrastructure. Services with inherited compute also inherit this control from Azure. Azure has a FedRAMP IaaS P-ATO (package ID F1209051525). For containers, when patches are available, a new container image is pulled from Microsoft Container Registry (MCR) and prepped for use. A new build is also created when components added to the MCR container image need to be patched.

Risk management measures for essential and important entities

Article	21.1
Description	The organization documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]].
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 documents risk assessment results in an annual risk assessment report.

Specific areas of risk management measures

Article	21.2
Description	The organization develops, documents, and disseminates to [Assignment: organization-defined personnel or roles] an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Database of domain name registration data

Access to specific domain name data for legitimate seekers

Article	28.5
Description	Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures about the disclosure of such data to be made publicly available.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Avoidance of data duplication in domain name registration

Article	28.6
Description	Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Database requirements for DNS and domain name registration

Article	28.1
Description	For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Information to be included in domain name database.

Article	28.2
Description	For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include: (a) the domain name;; (b) the date of registration;; (c) the registrant's name, contact email address and telephone number;; (d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Policies for accurate and complete domain name databases

Article	28.3
Description	Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Public availability of non-personal domain name data

Article	28.4
Description	Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Adopt EU-CyCLONe rules of procedure.

Article	16.8
Description	EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer. ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information. Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Composition of EU-CyCLONe

Article	16.2
Description	EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer. ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information. Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Cooperation between EU-CyCLONe and CSIRTs Network

Article	16.6
Description	EU-CyCLONe shall cooperate with the CSIRTs network based on agreed procedural arrangements provided for in Article 15(6)
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Define tasks of EU-CyCLONe

Article	16.3
Description	EU-CyCLONe shall have the following tasks: (a) to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;; (b) to develop a shared situational awareness for large-scale cybersecurity incidents and crises;; (c) to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;; (d) to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;; (e) to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Establish European Cyber Crisis Liaison Organization Network (EU-CyCLONe)

Article	16.1
Description	EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Regular Reporting by EU-CyCLONe to Cooperation Group

Article	16.5
Description	EU-CyCLONe shall report on a regular basis to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, focusing on their impact on essential and important entities.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Regular reporting by EU-CyCLONe to European Bodies

Article	16.7
Description	By 17 July 2024 and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

General aspects concerning supervision and enforcement.

Cooperation with Data Protection Supervisory Authorities

Article	31.3
Description	The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 Security Incident & Response (SIR) team maintains a list of incident response contacts for all partner organizations, including: organizations internal to Microsoft, incident response POCs within partner organizations covered via ISAs, and customer incident response contacts. These partner organizations are also provided direct contact information for the Office 365 SIR team.

Risk-based prioritization of supervisory tasks

Article	31.2
Description	Member States may allow their competent authorities to prioritize supervisory tasks. Such prioritization shall be based on a risk-based approach. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritization of such tasks following a risk-based approach.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Supervision for Compliance with the Directive

Article	31.1
Description	Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 compliance monitoring processes, methods and techniques are applied to customer content and access control data and are documented in ISAs and executed by Office 365 Trust.

Supervision of public administration entities

Article	31.4
Description	Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Governance

Manage accountability for cybersecurity risk-management.

Article	20.1
Description	cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article. The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Require regular cybersecurity training for management and employees.

Article	20.2
Description	Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Infringements entailing a personal data breach.

Cross-Member State Notification for Potential Data Breaches

Article	35.3
Description	Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in paragraph 1.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 SIR team reports incidents to designated authorities (including US-CERT) consistently with NIST SP 800-61 as documented in the Office 365 SIR Plan.

Notification of Personal Data Breaches to Supervisory Authorities

Article	35.1
Description	Where the competent authorities become aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Articles 21 and 23 of this Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 SIR team reports incidents to designated authorities (including US-CERT) consistently with NIST SP 800-61 as documented in the Office 365 SIR Plan.

International cooperation

International Agreements for Third-Party Participation

Article	17.1
Description	The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organizing their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with Union data protection law.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Jurisdiction and territoriality

Determining Main Establishment for Jurisdiction

Article	26.2
Description	For the purposes of this Directive, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Jurisdictional Scope for Entities

Article	26.1
Description	Entities falling within the scope of this Directive shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of: (a) providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;; (b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data Centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;; (c) public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Legal Actions Against Non-Represented Entities

Article	26.4
Description	The designation of a representative by an entity as referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Mutual Assistance for Supervisory and Enforcement Measures

Article	26.5
Description	Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on their territory.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Requirement for a representative in the Union for non-EU entities

Article	26.3
Description	If an entity as referred to in paragraph 1, point (b), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Inter-Member State Cooperation for Entities Operating in Multiple States

Article	37.1
Description	Where an entity provides services in more than one Member State or provides services in one or more Member States and its network and information systems are in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that: (a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken;; (b) a competent authority may request another competent authority to take supervisory or enforcement measures;; (c) a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner. The mutual assistance referred to in the first subparagraph, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Joint Supervisory Actions by Competent Authorities

Article	37.2
Description	Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Adopt national large-scale incident response plan.

Article	9.4
Description	Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: (a) the objectives of national preparedness measures and activities;; (b) the tasks and responsibilities of the cyber crisis management authorities;; (c) the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;; (d) national preparedness measures, including exercises and training activities;; (e) the relevant public and private stakeholders and infrastructure involved;; (f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Designate crisis management authorities

Article	9.1
Description	Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Identify crisis response capabilities.

Article	9.3
Description	The organization develops an incident response plan that provides a high-level approach for how the incident response capability fits into the overall organization.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Indicate coordinator for large-scale cybersecurity incidents.

Article	9.2
Description	Where a Member State designates or establishes more than one cyber crisis management authority pursuant to paragraph 1, it shall clearly indicate which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 tracks and documents security incidents using ticketing tools. Service teams notify the Office 365 Security Incident & Response (SIR) team of security incidents using ticketing tools. Likewise, if the Office 365 SIR team identifies a possible incident by themselves, they open a ticket. If the incident is categorized as a security incident, the Office 365 SIR team tracks and documents the security incident response process using a ticket. Various ticketing tools are used by the Office 365 SIR team and Service Team Engineering for reporting and tracking incidents are retained indefinitely. As part of the incident management process, the Office 365 SIR team and Service Team Engineering pull, review and attach system logs to tickets according to their troubleshooting guides. These logs can contain and be used as evidence of a security incident. If it is determined that additional evidence is required, the Office 365 SIR team will work with the service team and Corporate, External and Legal Affairs (CELA) to identify, collect and retain the evidence.

Notify commission of crisis management authority and changes

Article	9.5
Description	Within three months of the designation or establishment of the cyber crisis management authority referred to in paragraph 1, each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and to the European cyber crisis liaison organization network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 about their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information where and to the extent that such exclusion is necessary for their national security.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service team personnel are required to report suspected security incidents to the Office 365 Security Incident & Response (SIR) team in near real time upon discovering a suspected security incident. See the Office 365 Security Incident Response Plan for more information.

National cybersecurity strategy

Adopt National Cybersecurity Strategy

Article	7.1
Description	Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include: (a) objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II;; (b) a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2;; (c) a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts;; (d) a mechanism to identify relevant assets and an assessment of the risks in that Member State;; (e) an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors;; (f) a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;; (g) a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;; (h) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Implement cybersecurity policies in national strategy.

Article	7.2
Description	As part of the national cybersecurity strategy, Member States shall in particular adopt policies: (a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;; (b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;; (c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1);; (d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;; (e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;; (f) promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;; (g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;; (h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;; (i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs;; (j) promoting active cyber protection.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Notify Commission of National Strategies

Article	7.3
Description	Member States shall notify their national cybersecurity strategies to the Commission within three months of their adoption. Member States may exclude information which relates to their national security from such notifications.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Regular assessment and update of national strategies

Article	7.4
Description	Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years based on key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). CE equipment maintenance activities require peer reviews of the MOP checklist as a verification of completeness and quality assurance. During monthly review meetings with the CE team, DCM reviews/verifies all CE work that was completed in the previous month. The peer reviews verify that any required configurations or security settings are correctly in place before completion of the maintenance. The Site Services team follows detailed procedure documents that define step by step instructions for specific service requests. As part of the procedure documents, one of the final steps is to perform a Quality Control check to ensure that all steps were completed and that required security settings are in place.

Peer reviews

Conduct and confidentiality in peer reviews

Article	19.6
Description	Peer reviews shall entail physical or virtual on-site visits and off-site exchanges of information. In line with the principle of good cooperation, the Member State subject to the peer review shall provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts. Any information obtained through the peer review shall be used solely for that purpose. The cybersecurity experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft

Implementation Actions	Customer Responsibility: Government customers are responsible for having a process in place to check the validity of the Office 365 Web sites prior to signing on by reviewing the digital certificate on the site to ensure they are the Office 365 Web sites. If government customers are using USGCB baselines, supported web browsers will enforce this review automatically by default and prevent connections if the digital certificate is invalid. Government customers are responsible for ensuring that client software is configured to only establish sessions using FIPS 140-2 compliant protocols. This can be accomplished by restricting access to the government customer's ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 to VPN into the customer's network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections. For more information about configuring customer ADFS server(s) to only allow connections from customer internal networks, see: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh526961(v=ws.10) O365: Office 365 MT uses encryption to protect the integrity and confidentiality of transmitted information. Specifically, Office 365 provides FIPS 140-2 compliant cipher support for customer connections, interconnected system connections, and remote access connections to Office 365 MT . For connections to customers, Office 365 MT is configured to negotiate FIPS compliant TLS 1.2 protocols with supported client browsers, though non-FIPS compliant protocols are supported for legacy browser support.

Criteria for designating cybersecurity experts for peer reviews.

Article	19.2
Description	The methodology referred to in paragraph 1 shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews. The Commission and ENISA shall participate as observers in the peer reviews.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for establishing screening criteria that are consistent with their internal policies and procedures for personnel using Office 365 MT. Microsoft does not establish screening criteria for individuals hired by customers. Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to establish personnel screening criteria. Microsoft does not establish screening criteria for individuals hired by customers. O365: Office 365 MT, in coordination with Microsoft HR, has established screening criteria for Office 365 MT service team personnel by reviewing positions for risk as well as considering customer expectations. Screening criteria are documented at the following link and summarized below: http://hrweb/career/jobs/policies/Pages/BackgroundSpecializedScreensUS.aspx Roles with the “Cloud” risk designation are screened against the following: • Social Security Number Search • Criminal History Check • Office of Foreign Assets Control List • Bureau of Industry and Security List • Office of Defense Trade Controls Debarred Persons Personnel requesting additional access to an MT role type are required to undergo additional screening, outlined in the Office 365 MT personnel screening requirements. Enforcing screening requirements at the time of account creation and permission assignment ensures that personnel will not be inadvertently granted access prior to successful screening.

Disclose conflict of interest in peer review

Article	19.8
Description	Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of cybersecurity experts on duly substantiated grounds communicated to the designating Member State.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government customers are responsible for establishing screening criteria that are consistent with their internal policies and procedures for personnel using Office 365 MT. Microsoft does not establish screening criteria for individuals hired by customers. Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to establish personnel screening criteria. Microsoft does not establish screening criteria for individuals hired by customers. O365: Office 365 MT, in coordination with Microsoft HR, has established screening criteria for Office 365 MT service team personnel by reviewing positions for risk as well as considering customer expectations. Screening criteria are documented at the following link and summarized below: http://hrweb/career/jobs/policies/Pages/BackgroundSpecializedScreensUS.aspx Roles with the “Cloud” risk designation are screened against the following: • Social Security Number Search • Criminal History Check • Office of Foreign Assets Control List • Bureau of Industry and Security List • Office of Defense Trade Controls Debarred Persons Personnel requesting additional access to an MT role type are required to undergo additional screening, outlined in the Office 365 MT personnel screening requirements. Enforcing screening requirements at the time of account creation and permission assignment ensures that personnel will not be inadvertently granted access prior to successful screening.

Identify specific issues for peer reviews.

Article	19.3
Description	Member States may identify specific issues as referred to in paragraph 1, point (f), for the purposes of a peer review.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: See SI-6(a)

Limitations on repeated peer reviews

Article	19.7
Description	Once subject to a peer review, the same aspects reviewed in a Member State shall not be subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: See SI-6(a)

Notification of peer review scope

Article	19.4
Description	Before commencing a peer review as referred to in paragraph 1, Member States shall notify the participating Member States of its scope, including the specific issues identified pursuant to paragraph 3.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Part 1: O365: The Security Assessment Plan (SAP) is developed by a 3PAO-certified independent assessor for Office 365. Office 365 requires that the SAP include the security controls and enhancements under assessment, the assessment procedures, and an explanation of the assessment environment, team, and roles and responsibilities. The SAP is then reviewed and approved by Office 365, followed by a security assessment performed by the independent assessor. The SAP will be based on NIST SP 800-53A. Part 2: O365: See CA-02(a)(1) Part 3: O365: See CA-02(a)(1)

Peer review methodology and criteria

Article	19.1
Description	The Cooperation Group shall, on 17 January 2025, establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organizational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. Participation in peer reviews is voluntary. The peer reviews shall be carried out by cybersecurity experts. The cybersecurity experts shall be designated by at least two Member States, different from the Member State being reviewed. The peer reviews shall cover at least one of the following: (a) the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23;; (b) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities;; (c) the operational capabilities of the CSIRTs;; (d) the level of implementation of mutual assistance referred to in Article 37;; (e) the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29;; (f) specific issues of cross-border or cross-sector nature.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: See SI-6(a)

Self-assessment methodology for peer reviews

Article	19.5
Description	Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts. The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for the Member States' self-assessment.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Part 1: O365: The Security Assessment Plan (SAP) is developed by a 3PAO-certified independent assessor for Office 365. Office 365 requires that the SAP include the security controls and enhancements under assessment, the assessment procedures, and an explanation of the assessment environment, team, and roles and responsibilities. The SAP is then reviewed and approved by Office 365, followed by a security assessment performed by the independent assessor. The SAP will be based on NIST SP 800-53A. Part 2: O365: See CA-02(a)(1) Part 3: O365: See CA-02(a)(1) See SI-6(a)

Submission of peer review reports

Article	19.9
Description	Cybersecurity experts participating in peer reviews shall draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 business owners annually perform a business risk assessment using NIST SP 800-30 and 800-37 guidelines to ascertain the risk associated with operating Office 365 and to ensure financial and operational viability. The results of the risk assessment are documented in business and capital planning documentation. Office 365 Trust annually reviews existing assessments and performs security assessments to understand the risk posture of the service and to ensure security standards compliance. The results of the security assessment are captured in a SAR.

Registry of entities

European Network and Information Security Agency's (ENISA) role in creating a registry of various service providers.

Article	27.1
Description	ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data Centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Office 365 government customers are responsible for registering authenticators in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to register additional authenticators specific to Office 365 MT. Office 365 government customers are responsible for registering authenticators in compliance with their organizational policies and requirements for their organizational users. Office 365 government customers are responsible for registering authenticators in compliance with their organizational policies and requirements for their organizational users. Non-government customers managing user accounts in Azure Active Directory (AAD) via the SUE portal will need to register unique Office 365 authenticators. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349 O365: As part of the Office 365 registration process, Microsoft requires Microsoft administrators within Office 365 to obtain their YubiKey in person or via FedEx mail.

Forwarding Information to ENISA

Article	27.4
Description	Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Required information submission by entities to competent authorities.

Article	27.2
Description	main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3);; (d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3);; (e) the Member States where the entity provides services;; and (f) the entity's IP ranges.
Microsoft 365 Applicable?	Yes
Managed By	Customer
Implementation Actions	Need Implementation

Submission Through National Mechanisms

Article	27.5
Description	Where applicable, the information referred to in paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 SIR team reports incidents to designated authorities (including US-CERT) consistently with NIST SP 800-61 as documented in the Office 365 SIR Plan.

Timely updates on submitted information by entities.

Article	27.3
Description	Member States shall ensure that the entities referred to in paragraph 1 notify the competent authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Customer Responsibility: Government and non-government customers are responsible for implementing processes to notify customer account managers when accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need-to-know changes. Part 1,2,3: O365: Office 365 uses automated workflow account management tools that allow service teams to track the account management process through account request, approval, creation, modification, and deletion. As changes occur, the corresponding account manager is notified of the changes that require their approval. Information system usage and need-to-know are mapped to the roles defined by each service team. When an employee is transferred or their employment is terminated, the account management tools will automatically revoke the associated account's access to the privileges mapped to their previous role.

Report on the state of cybersecurity in the Union

ENISAs Biennial Cybersecurity Report

Article	18.1
Description	ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine-readable data and include the following: (a) a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape;; (b) an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union;; (c) an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises;; (d) an aggregated assessment of the outcome of the peer reviews referred to in Article 19;; (e) an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 requires 3PAO-certified independent assessors to produce a SAR that documents the results of the assessment, including security controls that are considered other than satisfied, security control weaknesses, recommended remediation steps, and the risks associated with the system.

Methodology for Aggregated Assessments by ENISA

Article	18.3
Description	ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e).
Microsoft 365 Applicable?	Yes
Managed By	Customer
Implementation Actions	Needs Implementation

Policy Recommendations in ENISAs Report

Article	18.2
Description	The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.
Microsoft 365 Applicable?	Yes
Managed By	Customer
Implementation Actions	Needs Implementation

Reporting obligations

Communication of Cyber Threats to Service Recipients

Article	23.2
Description	Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The IR plan is posted on the internal Office 365 SharePoint. The IR plan is also communicated as a part of the annual security training provided for Office 365 personnel. When updates are made, the personnel filling roles and responsibilities named in the plan are notified via email. In addition to Microsoft staff, FedRAMP personnel will also be notified.

Criteria for Significant Incidents

Article	23.3
Description	An incident shall be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams utilize alternate processing site agreements in accordance with the organization's availability requirements. Recovery Time Objectives (RTO) are established for services and are detailed as part of the Business Continuity Management (BCM) process. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Office 365 service.

Cross-Border Notification of Significant Incidents

Article	23.6
Description	Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 SIR team coordinates with peer teams inside MSIT and Azure as required for incidents internal to Microsoft. Coordination with third party entities is addressed in the ISAs with those groups for incidents that may cross organizational boundaries. The Office 365 SIR team coordinates with customers as required consistent with the reporting timeframes outlined. The Office 365 SIR team tracks all coordinated incidents.

Forwarding notifications to other affected Member States

Article	23.8
Description	At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 Security Incident & Response (SIR) team uses ticketing tools as an automated mechanism to assist in the reporting of security incidents. A ticketing tool tracks the time elapsed and phases of the incident response process, helping to assure that incidents are reported in the timeframes required by IR-06-part b.

Implementing acts for notification and reporting

Article	23.11
Description	The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article. By 17 October 2024, the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data Centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, adopt implementing acts further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities. The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in accordance with Article 14(4), point (e). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Implemented

Information Sharing Under EU Directive 2022/2557

Article	23.10
Description	The CSIRTs or, where applicable, the competent authorities shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive (EU) 2022/2557.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service team personnel are required to report suspected security incidents to the Office 365 Security Incident & Response (SIR) team in near real time upon discovering a suspected security incident. See the Office 365 Security Incident Response Plan for more information.

Notification and Reporting Timelines for Significant Incidents

Article	23.4
Description	Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: (a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;; (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;; (c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;; (d) a final report not later than one month after the submission of the incident notification under point (b), including the following: (i) a detailed description of the incident, including its severity and impact;; (ii) the type of threat or root cause that is likely to have triggered the incident;; (iii) applied and ongoing mitigation measures;; (iv) where applicable, the cross-border impact of the incident;; (e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident. By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Public Awareness and Disclosure of Significant Incidents

Article	23.7
Description	Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams utilize alternate processing site agreements in accordance with the organization's availability requirements. Recovery Time Objectives (RTO) are established for services and are detailed as part of the Business Continuity Management (BCM) process. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Office 365 service.

Quarterly summary reports to ENISA

Article	23.9
Description	The single point of contact shall submit to ENISA every three months a summary report, including anonymized and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received every six months.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams utilize alternate processing site agreements in accordance with the organization's availability requirements. Recovery Time Objectives (RTO) are established for services and are detailed as part of the Business Continuity Management (BCM) process. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Office 365 service.

Reporting Mechanism for Significant Incidents by Entities

Article	23.1
Description	Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability. Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt. In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 Security Incident & Response (SIR) team provides advice and assistance to Office 365 service team personnel via an internal SIR team wiki. The wiki includes such information as: • What are security incidents? • How to identify such incidents • How and Why to escalate the security incidents • List of sample security incidents • Who to contact in the event of a security incident The contact information includes 24/7 on-call information, so there is always a resource available should Office 365 service teams need advice or assistance.

Response and Guidance from CSIRT or Competent Authority

Article	23.5
Description	The CSIRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph 4, point (a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSIRT is not the initial recipient of the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in cooperation with the CSIRT. The CSIRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authorities.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service team personnel are required to report suspected security incidents to the Office 365 Security Incident & Response (SIR) team in near real time upon discovering a suspected security incident. See the Office 365 Security Incident Response Plan for more information.

Define Core Tasks of Computer Security Incident Response Teams (CSIRTs)

Article	11.3
Description	The CSIRTs shall have the following tasks: (a) monitoring and analyzing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;; (b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;; (c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;; (d) collecting and analyzing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;; (e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;; (f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;; (g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);; (h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3). When carrying out the tasks referred to in the first subparagraph, the CSIRTs may prioritize particular tasks on the basis of a risk-based approach.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams receive information system security alerts, advisories, and directives from the Office 365 Security and Azure Security teams. These teams are responsible for receiving alerts on an ongoing basis from designated external organizations (including US-CERT) and pushing them to the Office 365 service teams.

Ensure Technical Capabilities of Computer Security Incident Response Teams (CSIRTs)

Article	11.2
Description	Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3. Member States shall ensure that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 servers are configured to limit the use of processor and memory resources by process priority. This is a built-in feature of the Windows OS. Additionally, service teams monitor processor and memory utilization spikes and initiate the incident response process if spikes threaten the health of Office 365. Also, process and memory resources are capped per tenant, which prevents any single tenant from interfering with the availability of other tenant's services. Resource caps are "soft caps" meaning that under non-duress operation the processes can use whatever resources they need. Under duress (system is at >=97% CPU or <3% available mem) a service called PUMA applies a system enforced throttle per process. This is evaluated every hour and removed once the system is out of the duress state. The per process throttle is based on past usage and agreement with the component team owners. If a tenant has hit the process and / or memory cap usage is throttled back to acceptable level. The intent of the soft caps is to maintain critical customer facing operations at all costs. Processor and memory resources management are inherited from pre-existing FedRAMP Authorization for Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).

Establish computer security incident response teams (CSIRTs) cooperation with private sector.

Article	11.4
Description	The CSIRTs shall establish cooperation relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Directive.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Promote standard practices in CSIRT operations.

Article	11.5
Description	In order to facilitate cooperation referred to in paragraph 4, the CSIRTs shall promote the adoption and use of common or standardized practices, classification schemes and taxonomies in relation to: (a) incident-handling procedures;; (b) crisis management;; and (c) coordinated vulnerability disclosure under Article 12(1).
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	Out of Scope

Set Operational Requirements for Computer Security Incident Response Teams (CSIRTs)

Article	11.1
Description	The CSIRTs shall comply with the following requirements: (a) the CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times;; they shall clearly specify the communication channels and make them known to constituency and cooperative partners;; (b) the CSIRTs' premises and the supporting information systems shall be located at secure sites;; (c) the CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;; (d) the CSIRTs shall ensure the confidentiality and trustworthiness of their operations;; (e) the CSIRTs shall be adequately staffed to ensure availability of their services at all times and they shall ensure that their staff is trained appropriately;; (f) the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services. The CSIRTs may participate in international cooperation networks.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). In the event of a security incident, datacenter employees are able to communicate to each other using handheld radios and mobile phones. During an incident one practice is to create a conference bridge to allow for communication with alternate work sites and the Microsoft Azure C+AI Security Operations Center (SOC) team. Azure personnel are trained on incident response capabilities, and this training is conducted at least annually.

Review

Periodic Review and Reporting on the Directive

Article	40.1
Description	By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. To that end and with a view to further advancing the strategic and operational cooperation, the Commission shall consider the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The report shall be accompanied, where necessary, by a legislative proposal.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Service teams report and escalate findings to the Office 365 Security team when appropriate, who in turn follow the process defined in the Office 365 Security Incident Response Plan. The Office 365 Security Incident Response team acts as the designee of the ISSM or ISSO.

Standardization

Promotion of European and international standards

Article	25.1
Description	To promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favor of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams maintain, secure, manage, and store information system documentation, including documentation regarding: • Secure configuration, installation, and operation of the information system; • Effective use and maintenance of security features/functions; and • Known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions This documentation is stored in each service team's SharePoint site and Wiki and made available to service team administrators, developers, and testers. The documentation is secured via SharePoint's internal security mechanisms. Service team administrators act as the designee of the SCA / ISSO. Acquisition of hardware and associated documentation is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). Microsoft Azure service teams maintain, secure, manage, and store information system documentation. This documentation is stored in each service team's SharePoint site and made available to service team administrators. The documentation is secured via SharePoint's internal security mechanisms. Information system documentation is distributed to only the appropriate groups and individuals on a need-to-know basis and is based on job responsibilities. Documentation for externally provided software is available online at vendor websites.

Supervisory and enforcement measures in relation to essential entities

Competent authorities' supervisory powers over essential entities

Article	32.2
Description	Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to: (a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;; (b) regular and targeted security audits carried out by an independent body or a competent authority;; (c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;; (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;; (e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;; (f) requests to access data, documents and information necessary to carry out their supervisory tasks;; (g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence. The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information. The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 Security incorporates business requirements from Office 365 as a whole and coordinates security audit functions from individual service teams to enhance mutual support and to help guide the selection of auditable events.

Cooperation with Oversight Forum on Critical ICT Third-Party Service Providers

Article	32.10
Description	Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 does not have any outsourced dedicated information security services. If any services were to be outsourced after receiving a FedRAMP P-ATO, Office 365 Trust would complete an assessment of risk and follow FedRAMP change management processes.

Criteria for measures on essential entities

Article	32.1
Description	Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate, and dissuasive, taking into account the circumstances of each individual case.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 has established a continuous monitoring strategy, documented in the continuous monitoring strategy guide. This strategy is implemented by the continuous monitoring team and includes response actions to address results of the analysis of security-related information, including vulnerability mitigation, POA&M resolution, and control gap closure.

Detailed reasoning and preliminary notifications for enforcement measures

Article	32.8
Description	The competent authorities shall set out a detailed reasoning for their enforcement measures. Before adopting such measures, the competent authorities shall notify the entities concerned of their preliminary findings. They shall also allow a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: When security updates are identified from the above information sources, they are initially reviewed by Office 365 Service Team Engineering personnel. Qualified updates are pushed through monthly/emergency triage meetings to appropriate service groups who are responsible for patching servers appropriately and verify that servers are operational. Security remediation will be implemented as follows: • Remediation for High Risk vulnerabilities will be implemented within 30 days of the vulnerability mitigation being released by the vendor. • Remediation for Medium Risk vulnerabilities will be implemented within 90 days of vulnerability the vulnerability mitigation being released by the vendor. In the event where patching during the timeframe is infeasible, service groups may request exceptions, which are very limited and reviewed on a case-by-case basis. Exceptions and risks identified during the course of vulnerability remediation are tracked in Archer for stakeholder and Office 365 Security review. Office 365 Security also verifies degree of compliance using vulnerability scanners deployed in Office 365.

Enforcement powers over essential entities

Article	32.4
Description	Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to: (a) issue warnings about infringements of this Directive by the entities concerned;; (b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;; (c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;; (d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;; (e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;; (f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;; (g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;; (h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;; (i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Service teams report and escalate findings to the Office 365 Security team when appropriate, who in turn follow the process defined in the Office 365 Security Incident Response Plan. The Office 365 Security Incident Response team acts as the designee of the ISSM or ISSO.

Inter-Authority Communication for Critical Entities Under Different Directives

Article	32.4
Description	Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to: (a) issue warnings about infringements of this Directive by the entities concerned;; (b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;; (c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;; (d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;; (e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;; (f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;; (g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;; (h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;; (i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft

Implementation Actions	Customer Responsibility: Government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 access. For these events, these government customers are responsible for integrating audit record analysis with analysis of data/information collected from other sources to detect suspicious activity. Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365. O365: The Office 365 Security team correlates audit records with vulnerability scanning information and penetration test data to gain a more complete picture of potential exploits and to enhance the ability to detect inappropriate activity. Additionally, Office 365 Security uses vulnerability scanning reports in conjunction with performance and system monitoring data to identify unusual activity. Audit logs are uploaded to a repository service from all servers in the Office 365 environment, where they are correlated across service teams to support after-the-fact investigations of security incidents, including the use of audit logging data, incident monitoring reports, vulnerability scan data, and penetration testing results.

Liability of Legal Representatives of Essential Entities

Article	32.4
Description	Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to: (a) issue warnings about infringements of this Directive by the entities concerned;; (b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;; (c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;; (d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;; (e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;; (f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;; (g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;; (h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;; (i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 has established a continuous monitoring strategy, documented in the continuous monitoring strategy guide. This strategy is implemented by the continuous monitoring team and includes response actions to address results of the analysis of security-related information, including vulnerability mitigation, POA&M resolution, and control gap closure.

Remedial Actions for Ineffective Enforcement Measures

Article	32.4
Description	Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to: (a) issue warnings about infringements of this Directive by the entities concerned;; (b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;; (c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;; (d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;; (e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;; (f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;; (g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;; (h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;; (i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Security alerts, advisories, and directives are disseminated to Office 365 Service Team Operations and Security Manager personnel and any additional entities requested by the customer.

Specification of Information Requests by Competent Authorities

Article	32.3
Description	When exercising their powers under paragraph 2, point (e), (f) or (g), the competent authorities shall state the purpose of the request and specify the information requested.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Supervisory and enforcement measures in relation to important entities

Application of supervisory and enforcement measures for important entities

Article	33.5
Description	Article 32(6), (7) and (8) shall apply mutatis mutandis to the supervisory and enforcement measures provided for in this Article for important entities.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: When security updates are identified from the above information sources, they are initially reviewed by Office 365 Service Team Engineering personnel. Qualified updates are pushed through monthly/emergency triage meetings to appropriate service groups who are responsible for patching servers appropriately and verify that servers are operational. Security remediation will be implemented as follows: • Remediation for High Risk vulnerabilities will be implemented within 30 days of the vulnerability mitigation being released by the vendor. • Remediation for Medium Risk vulnerabilities will be implemented within 90 days of vulnerability the vulnerability mitigation being released by the vendor. In the event where patching during the timeframe is infeasible, service groups may request exceptions, which are very limited and reviewed on a case-by-case basis. Exceptions and risks identified during the course of vulnerability remediation are tracked in Archer for stakeholder and Office 365 Security review. Office 365 Security also verifies degree of compliance using vulnerability scanners deployed in Office 365.

Cooperation with oversight forum on important entities as critical ICT providers

Article	33.6
Description	Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 servers are configured to limit the use of processor and memory resources by process priority. This is a built-in feature of the Windows OS. Additionally, service teams monitor processor and memory utilization spikes and initiate the incident response process if spikes threaten the health of Office 365. Also, process and memory resources are capped per tenant, which prevents any single tenant from interfering with the availability of other tenant's services. Resource caps are "soft caps" meaning that under non-duress operation the processes can use whatever resources they need. Under duress (system is at >=97% CPU or <3% available mem) a service called PUMA applies a system enforced throttle per process. This is evaluated every hour and removed once the system is out of the duress state. The per process throttle is based on past usage and agreement with the component team owners. If a tenant has hit the process and / or memory cap usage is throttled back to acceptable level. The intent of the soft caps is to maintain critical customer facing operations at all costs. Processor and memory resources management are inherited from pre-existing FedRAMP Authorization for Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).

Enforcement powers over important entities

Article	33.4
Description	Member States shall ensure that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to: (a) issue warnings about infringements of this Directive by the entities concerned;; (b) adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive;; (c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;; (d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;; (e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;; (f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;; (g) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;; (h) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft

Implementation Actions	O365: The Office 365 servers are configured to limit the use of processor and memory resources by process priority. This is a built-in feature of the Windows OS. Additionally, service teams monitor processor and memory utilization spikes and initiate the incident response process if spikes threaten the health of Office 365. Also, process and memory resources are capped per tenant, which prevents any single tenant from interfering with the availability of other tenant's services. Resource caps are "soft caps" meaning that under non-duress operation the processes can use whatever resources they need. Under duress (system is at >=97% CPU or <3% available mem) a service called PUMA applies a system enforced throttle per process. This is evaluated every hour and removed once the system is out of the duress state. The per process throttle is based on past usage and agreement with the component team owners. If a tenant has hit the process and / or memory cap usage is throttled back to acceptable level. The intent of the soft caps is to maintain critical customer facing operations at all costs. Processor and memory resources management are inherited from pre-existing FedRAMP Authorization for Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).

Ex post supervisory measures for important entities

Article	33.1
Description	When provided with evidence, indication or information that an important entity allegedly does not comply with this Directive, in particular Articles 21 and 23 thereof, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures. Member States shall ensure that those measures are effective, proportionate, and dissuasive, taking into account the circumstances of each individual case.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: When security updates are identified from the above information sources, they are initially reviewed by Office 365 Service Team Engineering personnel. Qualified updates are pushed through monthly/emergency triage meetings to appropriate service groups who are responsible for patching servers appropriately and verify that servers are operational. Security remediation will be implemented as follows: • Remediation for High Risk vulnerabilities will be implemented within 30 days of the vulnerability mitigation being released by the vendor. • Remediation for Medium Risk vulnerabilities will be implemented within 90 days of vulnerability the vulnerability mitigation being released by the vendor. In the event where patching during the timeframe is infeasible, service groups may request exceptions, which are very limited and reviewed on a case-by-case basis. Exceptions and risks identified during the course of vulnerability remediation are tracked in Archer for stakeholder and Office 365 Security review. Office 365 Security also verifies degree of compliance using vulnerability scanners deployed in Office 365.

Specification of information requests for important entities

Article	33.3
Description	When exercising their powers under paragraph 2, point (d), (e) or (f), the competent authorities shall state the purpose of the request and specify the information requested.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 servers are configured to limit the use of processor and memory resources by process priority. This is a built-in feature of the Windows OS. Additionally, service teams monitor processor and memory utilization spikes and initiate the incident response process if spikes threaten the health of Office 365. Also, process and memory resources are capped per tenant, which prevents any single tenant from interfering with the availability of other tenant's services. Resource caps are "soft caps" meaning that under non-duress operation the processes can use whatever resources they need. Under duress (system is at >=97% CPU or <3% available mem) a service called PUMA applies a system enforced throttle per process. This is evaluated every hour and removed once the system is out of the duress state. The per process throttle is based on past usage and agreement with the component team owners. If a tenant has hit the process and / or memory cap usage is throttled back to acceptable level. The intent of the soft caps is to maintain critical customer facing operations at all costs. Processor and memory resources management are inherited from pre-existing FedRAMP Authorization for Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).

Supervisory powers over important entities

Article	33.2
Description	Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to: (a) on-site inspections and off-site ex post supervision conducted by trained professionals;; (b) targeted security audits carried out by an independent body or a competent authority;; (c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;; (d) requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;; (e) requests to access data, documents and information necessary to carry out their supervisory tasks;; (f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence. The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information. The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft

Implementation Actions	O365: The Office 365 servers are configured to limit the use of processor and memory resources by process priority. This is a built-in feature of the Windows OS. Additionally, service teams monitor processor and memory utilization spikes and initiate the incident response process if spikes threaten the health of Office 365. Also, process and memory resources are capped per tenant, which prevents any single tenant from interfering with the availability of other tenant's services. Resource caps are "soft caps" meaning that under non-duress operation the processes can use whatever resources they need. Under duress (system is at >=97% CPU or <3% available mem) a service called PUMA applies a system enforced throttle per process. This is evaluated every hour and removed once the system is out of the duress state. The per process throttle is based on past usage and agreement with the component team owners. If a tenant has hit the process and / or memory cap usage is throttled back to acceptable level. The intent of the soft caps is to maintain critical customer facing operations at all costs. Processor and memory resources management are inherited from pre-existing FedRAMP Authorization for Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).

Union level coordinated security risk assessments of critical supply chains.

Coordinated security risk assessments of critical ICT.

Article	22.1
Description	The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Identification of critical ICT for coordinated assessment.

Article	22.2
Description	The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.
Microsoft 365 Applicable?	No
Managed By	Customer
Implementation Actions	Out of Scope

Use of European cybersecurity certification schemes

Delegated Acts for Cybersecurity Certification

Article	24.2
Description	The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services, and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall include an implementation period. Before adopting such delegated acts, the Commission shall carry out an impact assessment and shall carry out consultations in accordance with Article 56 of Regulation (EU) 2019/881.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

ENISAs Role in Cybersecurity Certification Schemes

Article	24.3
Description	Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Requirement for Certified ICT Products and Services

Article	24.1
Description	essential and important entities to use ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, who are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.
Microsoft 365 Applicable?	No
Managed By	Microsoft
Implementation Actions	Out of Scope

Voluntary notification of relevant information

Processing and prioritization of notifications

Article	30.2
Description	Member States shall process the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23. Member States may prioritize the processing of mandatory notifications over voluntary notifications. Where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with the information about notifications received pursuant to this Article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: The Office 365 Security Incident & Response (SIR) team wiki provides information about incident response processes to Office 365 service teams. Additionally, battlecards and ticketing tools are used by the Office 365 SIR team for documenting and tracking the stages of the incident response process. Tickets are generated through automated processes, based on Office 365 Policy and criteria defined in Office 365 SIR's team wiki.

Voluntary notifications to CSIRTs or competent authorities

Article	30.1
Description	Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by: (a) essential and important entities with regard to incidents, cyber threats and near misses;; (b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.
Microsoft 365 Applicable?	Yes
Managed By	Microsoft
Implementation Actions	O365: Office 365 service teams utilize alternate processing site agreements in accordance with the organization's availability requirements. Recovery Time Objectives (RTO) are established for services and are detailed as part of the Business Continuity Management (BCM) process. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Office 365 service.

Thank you for reading our Technical Whitepaper NIS2 for Microsoft 365!

Please make sure you follow us on Github, Linkedin and our website www.itcowboys.nl for updates and more!

For more information

- Microsoft Purview NIS2 Directive (EU) 2022/2555 Assessment
- ITCowboys GitHub
- Microsoft Documentation
- NIS 2.0 Technology Mapping by Tony Krijnen @Microsoft
- NIS2directive.eu

We hope you enjoyed the ride!

Your ITCowboys, Jordy Herber & Paul Erlings