New ISO 27001:2022 controls & How Microsoft Saves the Day.

NOTE: These controls are **not mandatory**, if you have taken a risk-based approach to exclude the controls from your scope as a business. The controls will however be excluded from your certification.

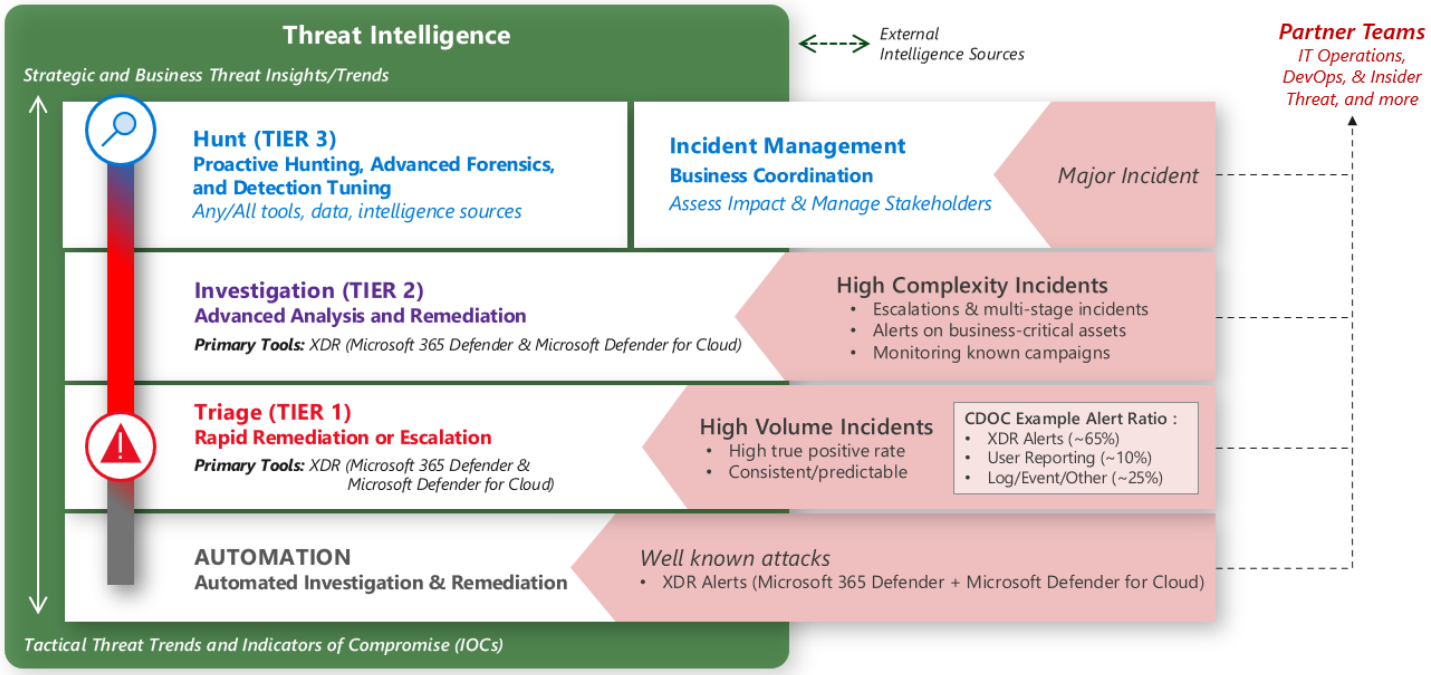
Relevant controls:

A.5.7 Threat intelligence

*Description. This control requires you to gather information about threats and **analyse them**, in order to **take appropriate mitigation actions**. This information could be about particular attacks, about methods and technologies the attackers are using, and/or about attack trends. You should gather this information internally, as well as from external **sources like vendor reports**, government agency announcements, etc.*

Microsoft Solutions

Security Operations Model – Functions and Tools



- **Azure Sentinel**
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps

Further Opportunity

Assessments and recommendations (Assessments should include an indication of the risk factor of choosing to exclude the control) conducted on behalf of clients, are now auditable requirements of the standard and will always create the opportunity for an extended engagement as this is a control we can manage on their behalf.

On the Microsoft front, the implementation of the stated technologies in an already existing tenant is now validated by the new control and creates further the opportunity to improve their security posture as an organisation.

A.5.23 Information security for use of cloud services

Description. This control requires you to set security requirements for cloud services in order to have better protection of your information in the cloud. This includes purchasing, using, managing, and terminating the use of cloud services.

Microsoft Solutions

Full Scope of Security, compliance & identity management, related to cloud computing services. The methodology associated with this implementation is directly related to the full process of security posture adoption on behalf of the client.

A.5.30 ICT readiness for business continuity

Description. This control requires your information and communication technology to be ready for potential disruptions so that required information and assets are available when needed. This includes readiness planning, implementation, maintenance, and testing.

Microsoft Solutions

An internal assessment needs to be conducted with regards to the scope of implementation related to disaster recovery and backups for clients. ***(ReadStore/MP360/ NBQ/ Azure site recovery/ Enable)***

A.8.9 Configuration management

Description. This control requires you to manage the whole cycle of security configuration for your technology to ensure a proper level of security and to avoid any unauthorized changes. This includes configuration definition, implementation, monitoring, and review.

Microsoft Solutions

This control requires configuration and management that is mostly governed within the various admin centres across the Microsoft environment, related to security. These include:

- Policy enforcements
- Restrictions
- Additional M365 SCI tooling (refer to licensing offering)

A.8.10 Information deletion

Description. This control requires you to delete data when no longer required, in order to avoid leakage of sensitive information and to enable compliance with privacy and other requirements. This could include deletion in your IT systems, removable media, or cloud services.

Microsoft Solutions

Retention policies within *Information governance* could be applied within M365 to permanently delete content from the client's organisation. Retention settings can be configured for the following settings:

- Delete-only: Permanently delete content after a specified period of time.
- Retain and then delete: Retain content for a specified period of time and then permanently delete it.

A.8.11 Data masking

Description. This control requires you to use data masking together with access control in order to limit the exposure of sensitive information. This primarily means ***personal data****, because they are heavily regulated through privacy regulations, but it could also include other categories of sensitive data.*

Microsoft Solutions

Information Protection. ***Protect your data***

To apply flexible protection actions that include encryption, access restrictions, and visual markings, use the following capabilities:

Capability	**What problems does it solve?**	**Get started**
Sensitivity labels	A single solution across apps, services, and devices to label and protect your data as it travels inside and outside your organization. Example scenarios: - Manage sensitivity labels for Office apps - Encrypt documents and emails - Apply and view labels in Power BI For a comprehensive list of scenarios for sensitivity labels, see the Get started documentation.	Get started with sensitivity labels
Azure Information Protection unified labelling client	For Windows computers, extends labelling to File Explorer and PowerShell, with additional features for Office apps if needed	Azure Information Protection unified labelling client administrator guide
Double Key Encryption	Under all circumstances, only your organization can ever decrypt protected content or for regulatory	Deploy Double Key Encryption

Capability	What problems does it solve?	Get started
	requirements, you must hold encryption keys within a geographical boundary.	
Office 365 Message Encryption (OME)	Encrypts email messages and attached documents that are sent to any user on any device, so only authorized recipients can read emailed information. Example scenario: Revoke email encrypted by Advanced Message Encryption	Set up new Message Encryption capabilities
Service encryption with Customer Key	Protects against viewing of data by unauthorized systems or personnel and complements BitLocker disk encryption in Microsoft datacentres.	Set up Customer Key for Office 365
SharePoint Information Rights Management (IRM)	Protects SharePoint lists and libraries so that when a user checks out a document, the downloaded file is protected so that only authorized people can view and use the file according to policies that you specify.	Set up Information Rights Management (IRM) in SharePoint admin centre
Rights Management connector	Protection-only for existing on-premises deployments that use Exchange or SharePoint Server, or file servers that run Windows Server and File Classification Infrastructure (FCI).	Steps to deploy the RMS connector
Azure Information Protection unified labelling scanner	Discovers, labels, and protects sensitive information that resides in data stores that are on premises.	Configuring and installing the Azure Information Protection unified labelling scanner
Microsoft Defender for Cloud Apps	Discovers, labels, and protects sensitive information that resides in data stores that are in the cloud.	Discover, classify, label, and protect regulated and sensitive data stored in the cloud
Azure Purview	Identifies sensitive data and applies automatic labelling to content in Azure Purview assets. These include files in storage such as Azure Data Lake and Azure Files, and schematized data such as columns in Azure SQL DB, and Cosmos DB.	Labelling in Azure Purview
Microsoft Information Protection SDK	Extends sensitivity labels to third-party apps and services. Example scenario: Set and get a sensitivity label (C++)	Microsoft Information Protection (MIP) SDK setup and configuration

Further Opportunity

Review customer licensing and possibly increase the scope of implementation due to new requirement.

A.8.12 Data leakage prevention

Description. This control requires you to apply various data leakage measures in order to avoid unauthorized disclosure of sensitive information, and if such incidents happen, to detect them in a timely manner. This includes information in IT systems, networks, or any devices.

Microsoft solution

Information Protection. ***Prevent data loss***

To help prevent accidental oversharing of sensitive information, use the following capabilities:

Capability	**What problems does it solve?**	**Get started**
Data loss prevention	Helps prevent unintentional sharing of sensitive items.	Get started with the default DLP policy
Endpoint data loss prevention	Extends DLP capabilities to items that are used and shared on Windows 10 computers.	Get started with Endpoint data loss prevention
Microsoft Compliance Extension	Extends DLP capabilities to the Chrome browser	Get started with the Microsoft Compliance Extension
Microsoft 365 data loss prevention on-premises scanner (preview)	Extends DLP monitoring of file activities and protective actions for those files to on-premises file shares and SharePoint folders and document libraries.	Get started with Microsoft 365 data loss prevention on-premises scanner (preview)
Protect sensitive information in Microsoft Teams chat and channel messages	Extends some DLP functionality to Teams chat and channel messages	Learn about the default data loss prevention policy in Microsoft Teams (preview)

Further Opportunity

Review customer licensing and possibly increase the scope of implementation due to new requirement.

A.8.23 Web filtering

Description. This control requires you to manage which websites your users are accessing, in order to protect your IT systems. This way, you can prevent your systems from being compromised by malicious code, and also prevent users from using illegal materials from the Internet.

Microsoft Solutions

Microsoft Defender for Endpoint (Web Content Filtering)

Web content filtering includes:

- Users are prevented from accessing websites in blocked categories, whether they are browsing on-premises or away.
- You can conveniently deploy varied policies to various sets of users using the device groups defined in the Microsoft Defender for Endpoint role-based access control settings.
- You can access web reports in the same central location, with visibility over actual blocks and web usage.