



Mapping Microsoft Cyber Offerings to: NIST Cybersecurity (CSF),
CIS Controls and ISO27001:2013 Frameworks



The NIST Cybersecurity Framework (CSF) is a voluntary Framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk. The Framework complements an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one. Just as the Framework is not industry-specific, the common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

For this document, we referenced the NIST CSF for Improving Critical Infrastructure Cybersecurity version 1.0 from February 2014, Center for Internet Security Controls¹ and ISO 27001:2013. Note: the two latter standards had already been mapped by NIST². What we provide in this document is information and guidance on:

- Microsoft Cyber Offerings that can help an organization meet the security functions
- Certain functions that should be fulfilled by the implementing organization utilizing either internal resources or third parties

In the table below, we have included four out of the five NIST CSF Core Functions (Identify, Protect, Detect, Respond and Recover) from the NIST CSF for which Microsoft Cyber Offerings can help. These offerings can help organizations with 70 of the 98 subcategories. Under the column "Microsoft Cyber Offerings that Help", the resources (hyperlinks) listed reflect product information and how-to documentation. Where no offering is shown, the activity should be covered by the implementing organization utilizing internal resources or third parties. For Microsoft partners, that white space is the opportunity to step in and provide much needed services.

¹ Formerly known as Council on CyberSecurity Critical Security Controls (CCS CSC)

² Alternative View: Appendix A - Framework Core Informative References: <https://www.nist.gov/sites/default/files/documents/itl/alternative-view-framework-core-021214.pdf>



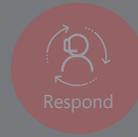
ID.AM: Asset Management

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
ID.AM-1 Physical devices and systems within the organization are inventoried	1	A.8.1.1, A.8.1.2	System Center Configuration Manager Inventory – for fully managed devices Active Directory (AD) – Domain Joined Devices Azure AD Registered Devices IoT Hub – Device Identity Registry Microsoft Intune Device Inventory – for lightly managed devices Windows Analytics	Inventory devices and systems (both Microsoft and non-Microsoft such as iOS, Mac OS X, Android).
ID.AM-2 Software platforms and applications within the organization are inventoried	2	A.8.1.1, A.8.1.2	Software Inventory with System Center Configuration Manager Microsoft Intune Device Inventory – for lightly managed devices Azure Subscription Inventory and Analysis – MSIT Showcase Windows Server 2016 – Software Inventory Logging Windows Server 2016 – Software Restriction Policies Shadow IT/SaaS App Discovery with Cloud App Security (CAS)	Inventory software platforms and apps (both Microsoft and non-Microsoft).
ID.AM-3 Organizational communication and data flows are mapped	1	A.13.2.1	Shadow IT/SaaS App Discovery with Cloud App Security Service Map solution in Azure Azure Network Watcher Azure Network Security Groups – ACLs Azure IoT Hub IP Filtering Enhanced Security Administrative Environment (ESAE)	Automatically discover, map and monitor various data flows (cloud apps usage, Network Security Groups, IP filtering, and application components on systems, administrative activity) and map communication between services.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>ID.AM-4</p> <p>External information systems are catalogued</p>		A.11.2.6	<p>Azure AD Integrated Apps</p> <p>Shadow IT/SaaS App Discovery with Cloud App Security</p>	<p>Maintain accountability of users' access and usage of SaaS apps.</p>
<p>ID.AM-5</p> <p>Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value</p>		A.8.2.1	<p>Azure Information Protection (AIP) – Data Classification</p> <p>Privileged Access Reference Material</p> <p>Azure AD Privileged Identity Management</p>	<p>Enable data classification, secure privileged access, and the ability to manage, control, and monitor access to Azure and Azure AD resources and other online services (e.g. Office 365 or Intune).</p>
<p>ID.AM-6</p> <p>Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</p>		A.6.1.1	<p>Privileged Access Reference Material</p> <p>Azure AD Privileged Identity Management</p> <p>Just Enough Administration</p> <p>Just in Time Administration – Privileged Access Management</p>	<p>Define roles and responsibilities (e.g. related to privileged access) across Azure and Windows environments, to prevent credential theft and to safeguard sensitive resources and data.</p>



ID.BE: Business Environment

The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>ID.BE-1</p> <p>The organization’s role in the supply chain is identified and communicated</p>		<p>A.15.1.3, A.15.2.1, A.15.2.2</p>	<p>Privileged Access Workstation Design and Implementation for Active Directory (DIAD)</p>	<p>Define, communicate as needed, and centrally store and manage information about organization’s users’ roles (including their privileges).</p>
<p>ID.BE-2</p> <p>The organization’s place in critical infrastructure and its industry sector is identified and communicated</p>				
<p>ID.BE-3</p> <p>Priorities for organizational mission, objectives, and activities are established and communicated</p>				



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
ID.BE-4		A.11.2.2, A.11.2.3, A.12.1.3		
ID.BE-5		A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1	Designing Resilient Applications for Microsoft Azure	Define resilience requirements to support building and delivery of applications/services in Azure.

ID.GV: Governance

The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
ID.GV-1		A.5.1.1		
ID.GV-2		A.6.1.1, A.7.2.1	Azure – Shared Responsibility Microsoft Incident Response and Shared Responsibility	Microsoft and its customers have certain information security roles and responsibilities that must be coordinated and aligned for successful outcomes for the organization.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>ID.GV-3</p> <p>Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p>		A.18.1	<p>Microsoft Compliance Offerings</p> <p>CAS – third-party risk evaluation and known certifications</p> <p>Microsoft and General Data Protection Regulation (GDPR)</p> <p>Microsoft Compliance Manager</p> <p>Privacy with Microsoft</p>	Microsoft itself as a technology solutions provider adheres to legal, data privacy and regulatory/compliance requirements regarding cybersecurity and enables customers to do the same.
<p>ID.GV-4</p> <p>Governance and risk management processes address cybersecurity risks</p>			<p>Microsoft Cloud Services Risk Assessment</p>	Microsoft cloud services have implemented security and privacy controls. If desired, customers can perform risk assessment of the services to assess compliance.

ID.RA: Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>ID.RA-1</p> <p>Asset vulnerabilities are identified and documented</p>	4	A.12.6.1, A.18.2.3	<p>Vulnerability Assessment in Azure Security Center</p> <p>Office 365 Secure Score</p> <p>AD Risk Assessment</p> <p>Microsoft Cloud Services Risk Assessment</p> <p>PAW</p> <p>DIAD</p>	Microsoft offers tools and services to help identify and report /document vulnerabilities across assets on premise and in the cloud.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>ID.RA-2 Threat and vulnerability information is received from information sharing forums and sources</p>		A.6.1.4	<p>Microsoft Security Intelligence Azure Log Analytics</p>	<p>Microsoft analyzes many billions of data points monthly, building intelligence on threats and vulnerabilities which is then used to actively protect the information of enterprises and customers.</p>
<p>ID.RA-3 Threats, both internal and external, are identified and documented</p>			<p>Microsoft Threat Modeling Tool Microsoft Threat Management Azure Log Analytics</p>	<p>Microsoft provides various tools, products and services to help organizations identify (detect) and document (report on), protect and respond to threats.</p>
<p>ID.RA-4 Potential business impacts and likelihoods are identified</p>				
<p>ID.RA-5 Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>		A.12.6.1	<p>Cybersecurity Operations Service</p>	<p>Microsoft provides proactive analysis (including detection of threats and vulnerabilities) by incident response experts to determine likelihoods to determine risk.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

ID.RA-6
Risk responses are identified and prioritized

[Cybersecurity Operations Service](#)

Microsoft provides proactive analysis (including detection of threats and vulnerabilities) by incident response experts to determine likelihoods to determine risk.

ID.RM: Risk Management Strategy

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

ID.RM-1
Risk management processes are established, managed, and agreed to by organizational stakeholders

[Cybersecurity Risk Review service - contact the Microsoft Services team to learn more](#)

Whether your organization has suffered a data loss incident or is planning a major security improvement program, the Cybersecurity Risk Review (CRR) service can help. It is an assessment that helps your organization understand the current security environment across technical, organizational, and operational controls.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

<p>ID.RM-2</p> <p>Organizational risk tolerance is determined and clearly expressed</p>			<p>Cybersecurity Risk Review Service - contact the Microsoft Services team to learn more</p>	
<p>ID.RM-3</p> <p>The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis</p>				<p>The Cybersecurity Risk Review (CRR) service is an assessment that helps your organization understand the current security environment across technical, organizational, and operational controls.</p>



PR.AC: Protect (PR) Access Control

Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
PR.AC-1 Identities and credentials are managed for authorized devices and users	16	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	Best Practices for Securing AD Microsoft Identity Manager: Connect your Directories Connect AD with Azure AD Azure AD – Group Management Automated User Provisioning and Deprovisioning to SaaS Apps Azure AD Join (Devices) Enroll devices for management in Microsoft Intune Control Access to Azure IoT Hub Azure IoT Hub – Device Identity Registry Azure AD Privileged Identity Management Privileged Access Management for AD Domain Services PAW DIAD Azure AD B2C Fast Start – Azure for Identity Dynamic Identity Framework (DIF) ESAE Microsoft Identity Manager Implementation Services	Microsoft offers tools, products and services for managing identities and credentials for authorized devices and users (e.g. privileged accounts).



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.AC-1 continued Identities and credentials are managed for authorized devices and users</p>	16	<p>A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3</p>	<p>Privileged Access Management Azure AD Implementation Services (AADIS) Enterprise Modernization for AD</p>	<p>Microsoft offers tools, products and services for managing identities and credentials for authorized devices and users (e.g. privileged accounts).</p>
<p>PR.AC-2 Physical access to assets is managed and protected</p>		<p>A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3</p>	<p>Protecting Data in Azure (Page 23, Physical Security) PAW DIAD</p>	<p>Microsoft provides protections for Azure (e.g. employs rigorous operations and processes to prevent unauthorized access, Azure nodes physically protected, and so forth), hardens dedicated physical workstations used by administrators and for Active Directory, offers a service engagement for deployment of read-only domain controllers (RODCs) for locations where physical security cannot be guaranteed.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.AC-3</p> <p>Remote access is managed</p>		<p>A.6.2.2</p> <p>A.13.1.1,</p> <p>A.13.2.1</p>	<p>Conditional Access in Azure AD</p> <p>Remote Desktop Services in Server 2016</p> <p>Server 2016: Web Application Proxy</p> <p>Secure Remote Access to on-premises applications:</p> <p>Azure AD App Proxy</p> <p>Azure Security – Remote Management</p> <p>CAS – Cloud App Governance and Control</p> <p>Device Compliance Policies for Conditional Access</p> <p>PAW</p> <p>DIAD</p>	<p>Microsoft security services enable control over and management of remote access (to applications and data) in support of security and compliance requirements.</p>
<p>PR.AC-4</p> <p>Access permissions are managed, incorporating the principles of least privilege and separation of duties</p>	<p>12, 15</p>	<p>A.6.1.2,</p> <p>A.9.1.2,</p> <p>A.9.2.3,</p> <p>A.9.4.1,</p> <p>A.9.4.4</p>	<p>Just Enough Administration (PowerShell - White Paper and Resources)</p> <p>Just Enough Administration: Step by Step</p> <p>Windows Server: Dynamic Access Control</p> <p>Microsoft Azure: Role Based Access Control</p> <p>Azure AD Privileged Identity Management</p> <p>Privileged Access Management for AD Domain Services</p> <p>PAW</p> <p>DIAD</p> <p>ESAE</p>	<p>Microsoft offers the ability to define access control policies based on a just enough administration approach, role based access control and privileged access management for managing access permissions, incorporating the principles of least privilege and separation of duties.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.AC-5</p> <p>Network integrity is protected, incorporating network segregation where appropriate</p>		<p>A.13.1.1, A.13.1.3, A.13.2.1</p>	<p>Microsoft Azure: Secure network with virtual appliances</p> <p>Microsoft Cloud Services and Network Security</p> <p>Azure Network Security Best Practices</p> <p>Azure Network Security Whitepaper</p> <p>PAW</p> <p>DIAD</p> <p>ESAE</p>	<p>Microsoft has spent more than two years establishing secure, isolated environments, credential management services and policies, and secure admin workstations to help protect mission-critical systems and services—including those used to manage cloud services, like Azure. And, Microsoft has a comprehensive approach to protect cloud infrastructure needed to run hyper-scale global services. Microsoft cloud infrastructure includes hardware, software, networks, and administrative and operations staff, in addition to the physical data centers.</p>



PR.AT: Awareness and Training

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
PR.AT-1 All users are informed and trained	9	A.7.2.2	ESAE	Cyber-attackers have been successful at rapidly gaining administrative access to corporate and government computing environments. At minimum, organizations must inform and train all users on cybersecurity. To help secure without impeding administrators, the Microsoft Enhanced Security Administrative Environment (ESAE) service utilizes advanced technologies and recommended practices to provide an administrative environment and workstations with enhanced security protection.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.AT-2</p> <p>Privileged users understand roles & responsibilities</p>	<p>9</p>	<p>A.6.1.1, A.7.2.2</p>	<p><u>ESAE</u></p>	<p>Credential hygiene is the recommended practice of verifying that privileged accounts only log on to workstations and servers that are sufficiently trusted and do not perform high-risk activities. The Microsoft Enhanced Security Administrative Environment (ESAE) service enforces credential hygiene by separating administrative accounts from normal user accounts (for email and web browsing) and compartmentalizing logon access for each type of administrative account.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.AT-3</p> <p>Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities</p>	<p>9</p>	<p>A.6.1.1, A.7.2.2</p>	<p><u>ESAE</u></p>	<p>Third-party stakeholders must understand their roles and responsibilities regarding access to corporate resources and data. To help thwart a critical element of credential theft attacks—the inadvertent exposure of administrative credentials—the Microsoft Enhanced Security Administrative Environment (ESAE) service utilizes advanced technologies and recommended practices to provide an administrative environment and workstations with enhanced security protection.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.AT-4</p> <p>Senior executives understand roles & responsibilities</p>	<p>9</p>	<p>A.6.1.1, A.7.2.2</p>	<p><u>ESAE</u></p>	<p>Senior executives, due to the overly sensitive nature of intellectual property and insider knowledge on corporate strategy and financial data they have at their disposal, are a highly valuable target for cyberattacks, and, particularly, credential theft attacks. This makes it imperative for them to understand their roles and responsibilities regarding access to corporate resources and data. To help thwart a critical element of credential theft attacks—the inadvertent exposure of administrative credentials—the Microsoft Enhanced Security Administrative Environment (ESAE) service utilizes advanced technologies and recommended practices to provide an administrative environment and workstations with enhanced security protection.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.AT-5</p> <p>Physical and information security personnel understand roles & responsibilities</p>	<p>9</p>	<p>A.6.1.1, A.7.2.2</p>	<p>ESAE</p>	<p>Physical and information security personnel, based on their very roles, must understand and take very seriously their responsibilities related to protecting systems, applications and data. Credential theft attacks can be particularly concerning. To help thwart a critical element of credential theft attacks—the inadvertent exposure of administrative credentials—the Microsoft Enhanced Security Administrative Environment (ESAE) service utilizes advanced technologies and recommended practices to provide an administrative environment and workstations with enhanced security protection.</p>



PR.DS: Data Security

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
PR.DS-1 Data-at-rest is protected	17	A.8.2.3	Windows Server 2016: Full disk Encryption with BitLocker – How to install Windows 10 Full disk encryption – BitLocker Shielded VMs in Windows Server 2016 Azure disk encryption for IaaS VMs Azure Storage Service Encryption for data at rest Azure Storage Security Guide SQL Server Encryption AIP – File Classification and Protection Windows Information Protection Encryption in Office 365 Azure Backup Data Encryption Microsoft Trust Center – Encryption Secure Mobile Devices with Microsoft Intune CAS – Govern Connected SaaS apps Azure SQL Transparent Data Encryption PAW ESAE DIAD AIP Full Volume Encryption – Windows BitLocker Drive Encryption	Microsoft offers encryption and data backup solutions within its on premise (e.g. Windows server, Windows 10 device) and cloud (e.g. Azure, Office 365) offerings and services to protect data-at-rest.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.DS-2</p> <p>Data-at-rest is protected</p>	<p>17</p>	<p>A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3</p>	<p>Azure VPN Gateway</p> <p>Azure ExpressRoute</p> <p>Office 365 Message Encryption</p> <p>Data Encryption in OneDrive for Business and Sharepoint Online</p> <p>SMB Encryption</p> <p>Remote Desktop Protocol Encryption</p> <p>Encrypting Connections to SQL Server</p> <p>Microsoft Trust Center – Encryption</p> <p>Internet Protocol Security (IPSec)</p> <p>ESAE</p>	<p>Microsoft offers encryption solutions and services (for Azure cloud and cloud services such as Office 365, OneDrive for Business) to protect data-in-transit.</p>
<p>PR.DS-3</p> <p>Assets are formally managed throughout removal, transfers, and disposition</p>		<p>A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7</p>	<p>Protecting Data in Azure (Page 18, Media Destruction)</p> <p>ESAE</p>	<p>Microsoft enables data management in Azure, and Microsoft Enhanced Security Administrative Environment (ESAE) service enables improved security and management of administrative accounts across the lifecycle (removal, transfers and disposition).</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.DS-4 Adequate capacity to ensure availability is maintained</p>		A.12.3.1	<p>Azure Subscription Service Limits Server 2016 Locks and Limits Exchange Online Limits SQL Server 2016 Limits</p>	<p>Microsoft offers options to adjust the capacity of resources within Azure/SQL Server 2016 or higher to ensure availability.</p>
<p>PR.DS-5 Protections against data leaks are implemented</p>	17	<p>A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3</p>	<p>Office 365 Data Loss Prevention (DLP) Windows Information Protection Microsoft CAS and DLP Microsoft Intune Mobile Application Management and DLP ESAE</p>	<p>Microsoft data loss prevention, information protection and credential theft attack prevention capabilities built into various products and services help protect against data leaks.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.DS-6</p> <p>Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>		<p>A.12.2.1, A.12.5.1</p>	<p>Windows Device Guard</p> <p>Introduction to Code Signing</p> <p>Signing PowerShell scripts, Part 1</p> <p>Signing PowerShell scripts, Part 2</p> <p>Deploying code integrity policies with Windows Defender Application Control (WDAC)</p> <p>ESAE</p>	<p>Microsoft performs integrity checking to verify software and firmware and information integrity for products. It also offers built-in security features to maintain integrity. For instance, Device Guard helps keep a Windows 10 device from running malware or other untrusted apps. Furthermore, Microsoft offers input on code signing for determining integrity of software, provides instructions on signing PowerShell Scripts, WDAC provides control over a computer running Windows 10 by specifying whether a driver or application is trusted and can be run, and ESAE service helps with credential theft-based attacks.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

PR.DS-7

The development and testing environment(s) are separate from the production environment

A.12.1.4

[Azure DevTest Labs](#)
[Use DevOps environments effectively for your web apps](#)
[MSDN/Visual Studio subscription \(Dev/Test tools, licenses, and cloud services\)](#)
[ESAE](#)

Microsoft provides Azure-based tools for testing only, input on setting up staging environments in Azure App Service, and setting up staging environments in Azure App Service, development tools for MSDN/Visual Studio, and the Enhanced Security Administrative Environment (ESAE) service that enforces credential hygiene by separating administrative accounts from normal user accounts (for email and web browsing) and compartmentalizing logon access for each type of administrative account.



PR.IP: Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.IP-1</p> <p>A baseline configuration of information technology/ industrial control systems is created and maintained</p>	3, 10	A.12.1.2, A.12.5.1	<p>Windows Security Baseline</p> <p>Azure Automation Desired State Configuration</p> <p>PowerShell Desired State Configuration</p> <p>Compliance Settings in SCCM</p> <p>Change Tracking with Log Analytics</p> <p>Azure Security Center – Common Configuration Identifiers and Baseline Rules</p> <p>Continuous Assurance with Secure DevOps Kit for Azure (AzSDK)</p> <p>PAW</p> <p>ESAE</p> <p>DIAD</p>	<p>Microsoft offers security baselines for various information technology products. A security baseline is a group of Microsoft-recommended configuration settings that explains their security impact. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.IP-2 A System Development Life Cycle to manage systems is implemented</p>		<p>A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5</p>	<p>Microsoft Security Development Lifecycle Security Development Lifecycle Tools Secure Development with AzSDK</p>	<p>The Microsoft Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. Microsoft offers several SDL tools to developers.</p>
<p>PR.IP-3 Configuration change control processes are in place</p>		<p>A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4</p>	<p>Change Management for Enterprise: Office 365 Configuring Change and Activity Management with System Center Service Manager How Microsoft IT approaches Organization Change Management Managing Changes and Activities with System Center</p>	<p>Microsoft offers advice on organizational change management for an enterprise, which focuses on the people side of change: how people’s behaviors influence operational changes, and how changes impact the intended audience. Microsoft also offers some controls within product (System Center) for operational change management, which focuses on the physical aspect of a change, for example, infrastructure, software, hardware, or environmental changes.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.IP-4</p> <p>Backups of information are conducted, maintained, and tested periodically</p>		<p>A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3</p>	<p>System Center Data Protection Manager Azure Backup ESAE</p>	<p>Microsoft offers the ability to perform backups of information. Furthermore, the Microsoft Enhanced Security Administrative Environment (ESAE) solution may be deployed to protect all administrative accounts or only higher privilege domain administrator accounts. These accounts typically have access to information that should be periodically backed up to prevent compromise and/or loss.</p>
<p>PR.IP-5</p> <p>Policy and regulations regarding the physical operating environment for organizational assets are met</p>		<p>A.11.1.4, A.11.2.1 A.11.2.2 A.11.2.3</p>	<p>Azure Security, Privacy, and Compliance Whitepaper</p>	<p>Microsoft Azure and Office 365 have been built with security, privacy and compliance with regulations in mind.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.IP-5 continued</p> <p>Policy and regulations regarding the physical operating environment for organizational assets are met</p>		<p>A.11.1.4, A.11.2.1 A.11.2.2 A.11.2.3</p>	<p><u>Security and Compliance in Office 365</u></p> <p><u>ESAE</u></p>	<p>Azure code development adheres to Microsoft’s Security Development Lifecycle (SDL). Managing security and compliance is a partnership. The organization using Microsoft services such as Office 365 is responsible for protecting data, identities, and devices, while Microsoft vigorously protects Office 365 services. Microsoft offers several tips and recommendations on how to achieve the appropriate level of protection for your organization. Furthermore, the Microsoft Enhanced Security Administrative Environment (ESAE) solution may be deployed to protect all administrative accounts or only higher privilege domain administrator accounts. These accounts typically access sensitive organizational assets to which access should be regulated.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.IP-6</p> <p>Data is destroyed according to policy</p>		<p>A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7</p>	<p>Retention Policies in Office 365 Compliance Center</p> <p>Protecting Data in Microsoft Azure (See Media Destruction and Data Deletion)</p>	<p>Microsoft offers options in Office 365 and Azure to destroy (delete) data (virtually/physically stored) based on security policy.</p>
<p>PR.IP-7</p> <p>Protection processes are continuously improved</p>			<p>Office 365 Secure Score</p> <p>Microsoft Enterprise Cloud Red Teaming (PDF download)</p> <p>Penetration testing of your Azure hosted Applications</p>	<p>Microsoft enables tools and tips for assessing the security posture of an organization against best practice security controls and measures. Microsoft also offers rules of engagement to perform penetration testing of the Microsoft cloud should an organization so desire to do so. This information can help an organization continuously assess and improve its protection processes.</p>
<p>PR.IP-8</p> <p>Effectiveness of protection technologies is shared with appropriate parties</p>		<p>A.16.1.6</p>		



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.IP-9 Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</p>		<p>A.16.1.1, A.17.1.1, A.17.1.2</p>	<p>Microsoft Azure Security Response in the Cloud Office 365 Security Incident Management Windows Defender ATP – response actions Responding to IT Security Incidents Azure Site Recovery Cybersecurity Operations Service</p>	<p>Microsoft offers incident response controls in Azure, Office 365 and Windows Defender Advanced Threat Protection. Microsoft also offers advice on responding to security incidents and a pre-incident response service called Cybersecurity Operations Service in which the Microsoft Detection and Response team will provide the strategic guidance needed to properly harden environments against advanced and persistent attacks.</p>
<p>PR.IP-10 Response and recovery plans are tested</p>		<p>A.17.1.3</p>	<p>Test Failover to Azure in Site Recovery</p>	<p>Microsoft offers the option to run a disaster recovery drill to Azure.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.IP-11</p> <p>Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)</p>		<p>A.7.1.1, A.7.3.1, A.8.1.4</p>		
<p>PR.IP-12</p> <p>A vulnerability management plan is developed and implemented</p>		<p>A.12.6.1, A.18.2.2</p>	<p>Vulnerability Assessment in Azure Security Center Vulnerabilities detected by Azure AD Identity Protection SCCM Vulnerability Assessment</p>	<p>Microsoft checks if VMs in Azure are running a vulnerability assessment solution, Azure Active Directory Identity Protection detects and reports on vulnerabilities (e.g. MFA registration not configured, unmanaged cloud apps) and SCCM Vulnerability Assessment allows you to scan managed systems for common missing security updates and misconfigurations which might make client computers more vulnerable to attack.</p>



PR.MA: Maintenance

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.MA-1</p> <p>Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools</p>		<p>A.11.1.2, A.11.2.4, A.11.2.5</p>	<p>Windows Automatic Maintenance</p> <p>Azure Security and Audit Log Management</p>	<p>Microsoft offers automatic maintenance for Windows that helps maintain the health and performance of a Windows PC. The security logs in Microsoft Azure Cloud Services (which provides Platform as a Service or PaaS) and Virtual Machines (which provides Infrastructure as a Service or IaaS) contain vital information that can provide intelligence and powerful insights into the following security issues: policy violations, internal and external threats, regulatory compliance and network, host, and user activity anomalies.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.MA-2</p> <p>Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access</p>		<p>A.11.2.4, A.15.1.1, A.15.2.1</p>	<p>Azure AD B2B</p> <p>Azure Security and Audit Log Management</p> <p>PAW</p> <p>ESAE</p> <p>DIAD</p>	<p>Microsoft has tools and services for ensuring only authorized access to organizational assets (e.g. apps and data, including credentials).</p>



PR.PT: Protective Technology

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
PR.PT-1 Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	14	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	Azure Security and Audit Log Management Microsoft Azure log integration and Security Information and Event Management (SIEM) systems Office 365 Audit logs Azure log analytics AD Auditing Windows Server 2016 Security Auditing AIP Logging CAS – Governance and Audit for Microsoft and 3rd party SaaS apps CAS SIEM integration SQL Server Audit Microsoft Dynamics Auditing Overview PAW DIAD	Microsoft builds audit/log records for Azure, Azure AD, Office 365, Cloud App Security, SQL Server, and Dynamics.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>PR.PT-2</p> <p>Removable media is protected and its use restricted according to policy</p>		<p>A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9</p>	<p>BitLocker Policy reference – Windows 10 (Removable Drive section)</p> <p>Control Access to Removable Media (Group Policy)</p> <p>Full Volume Encryption – Windows BitLocker Drive Encryption</p>	<p>Microsoft enables controls for securing against removable media based cyber threats, preventing data compromise from decommissioned computers and other purposes.</p>
<p>PR.PT-3</p> <p>Access to systems and assets is controlled, incorporating the principle of least functionality</p>		<p>A.9.1.2</p>	<p>Application Whitelisting with Configuration Manager and Windows 10</p> <p>AppLocker: Application Whitelisting</p> <p>Server 2016 Hardening Guideline</p> <p>PAW</p> <p>ESAE</p> <p>DIAD</p>	<p>Microsoft offers capabilities in Windows 10, Server 2016 and through services (PAW, ESAE, DIAD) to enable controlled access to systems and assets (e.g. devices and apps).</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
PR.PT-4 Communications and control networks are protected	7	A.13.1.1, A.13.2.1	Creating and using network isolated environments (System Center Virtual Machine Manager or SCVMM, Hyper-V) Introduction to Server and Domain Isolation (reference) Azure Network Security Whitepaper PAW ESAE DIAD	<p>When you create a SCVMM environment, you can enable network isolation, which allows you to run multiple identical copies (or "clones") of the environment. With the Microsoft Windows operating systems (Windows Server 2008 and Vista), you can isolate your domain and server resources to limit access to authenticated and authorized computers. For Azure, each deployment can be isolated from the other deployments at the network level. Each virtual network is isolated from the other virtual networks. Additionally, some Microsoft services (PAW, ESAE, DIAD) enable controlled access.</p>



DE.AE: Anomalies and Events

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>DE.AE-1</p> <p>A baseline of network operations and expected data flows for users and systems is established and managed</p>			<p>Advanced Threat Analytics (See question regarding baseline)</p> <p>Advanced Threat Analytics Implementation Services (ATAIS)</p> <p>Microsoft CAS – Anomaly Detection – SaaS Apps</p> <p>Office 365 CAS – Anomaly Detection</p> <p>Azure Security Center – see Anomaly Detection</p> <p>PAW</p> <p>DIAD</p>	<p>When relevant, Microsoft products and services help with establishing a baseline for cyber security operations and expected data flows for users and systems. With Microsoft Advanced Threat Analytics, there is no need to create rules, thresholds, or baselines and then fine-tune. ATA analyzes the behaviors among users, devices, and resources—as well as their relationship to one another—and can detect suspicious activity and known attacks fast. With Microsoft Cloud App Security and Office 365 Cloud App Security, the anomaly detection policies are automatically enabled,</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

DE.AE-1 continued

A baseline of network operations and expected data flows for users and systems is established and managed

- [Advanced Threat Analytics \(See question regarding baseline\)](#)
- [Advanced Threat Analytics Implementation Services \(ATAIS\)](#)
- [Microsoft CAS – Anomaly Detection – SaaS Apps](#)
- [Office 365 CAS – Anomaly Detection](#)
- [Azure Security Center – see Anomaly Detection](#)
- [PAW](#)
- [DIAD](#)

but Cloud App Security has an initial learning period of seven days during which not all anomaly detection alerts are raised. After that, each session is compared to the activity, when users were active, IP addresses, devices, etc. detected over the past month and the risk score of these activities. These detections are part of the heuristic anomaly detection engine that profiles your environment and triggers alerts with respect to a baseline that was learned on your organization’s activity. With Microsoft Azure Security Center, anomaly detection uses statistical profiling to build a historical baseline. It alerts on deviations from established baselines that conform to a potential attack vector. Additionally, some Microsoft services (PAW and DIAD) enable controlled access based on users and roles (privileges).



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>DE.AE-2</p> <p>Detected events are analyzed to understand attack targets and methods</p>		<p>A.16.1.1, A.16.1.4</p>	<p>Azure Log Analytics - Log Searches Advanced Threat Analytics – working with suspicious activities Advanced Threat Analytics Implementation Services (ATAIS)</p>	<p>Microsoft has various tools and services for searching logs, as well as analyzing suspicious activities. Microsoft Services help organizations get the most out of their investment in threat detection services through preparation, design, and the implementation of Microsoft Advanced Threat Analytics (ATA), including assistance with reviewing events that are identified by ATA after installation to help address false positive events.</p>
<p>DE.AE-3</p> <p>Event data are aggregated and correlated from multiple sources and sensors</p>			<p>Azure Log Analytics - Log Searches Advanced Threat Analytics – SIEM integration Advanced Threat Analytics Implementation Services (ATAIS) Azure logs – SIEM integration SIEM integration – CAS PAW DIAD ESAE</p>	



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

<p>DE.AE-4</p> <p>Impact of events is determined</p>			<p>Azure AD Risk Events</p> <p>Cybersecurity Operations Service</p>	<p>Discovering compromised identities is no easy task. Azure Active Directory uses adaptive machine learning algorithms and heuristics to detect suspicious actions related to user accounts and each action is stored in a record called risk event. The Microsoft Cybersecurity Operations Service is a pre-incident response service in which the Microsoft Detection and Response team will provide the strategic guidance needed to properly harden environments against advanced and persistent attacks.</p>
---	--	--	---	--



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>DE.AE-5</p> <p>Incident alert thresholds are established</p>			<p>Creating alert rules in Log Analytics</p> <p>Office 365 – creating security and audit alerts</p> <p>Azure AD Privileged Identity Management – Creating Alerts</p> <p>Azure AD Risk Events</p> <p>Azure Security Center – managing alerts</p> <p>CAS – Control cloud apps with policies (fine tuning thresholds)</p> <p>Advanced Threat Analytics – working with suspicious activities</p> <p>Advanced Threat Analytics Implementation Services (ATAIS)</p> <p>PAW</p> <p>DIAD</p> <p>Cybersecurity Operations Service</p>	<p>Microsoft offers capabilities and services for establishing alert thresholds based on user activity (suspicious, unsafe), breaches, devices (infected), risky cloud apps, an IP address, and/or other criteria.</p>



DE.CM: Security Continuous Monitoring

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>DE.CM-1</p> <p>The network is monitored to detect potential cybersecurity events</p>	<p>14, 16</p>		<p>Azure Log Analytics</p> <p>Index of Security related information from SCOM</p> <p>Advanced Threat Analytics – Events Detected</p> <p>Advanced Threat Analytics Implementation Services (ATAIS)</p> <p>Azure Network Security</p>	<p>Microsoft provided capabilities for detection of potential cybersecurity events in products such as Azure Log Analytics (manage and protect on-premises and cloud infrastructure), SCOM, Advanced Threat Analytics (detect the following various phases of an advanced attack: reconnaissance, credential compromise, lateral movement, privilege escalation, domain dominance, and others), Azure network security functions like DDoS defense system that is part of Azure’s continuous monitoring process, and is continually improved through penetration-testing. Azure’s DDoS defense system is designed to not only withstand attacks from the outside, but also from other Azure tenants.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

DE.CM-2

The physical environment monitored to detect potential cybersecurity events

[Azure Security and Compliance \(See Infrastructure Protection section\)](#)

Azure runs in geographically distributed Microsoft facilities, each designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability and are managed, monitored, and administered by Microsoft operations personnel.

DE.CM-3

Personnel activity is monitored to detect potential cybersecurity events

A.12.4.1 [Microsoft CAS – Anomaly Detection – SaaS Apps](#)
[Azure Events – Audit Logs](#)
[O365 – Audit Logging](#)
[Windows Security Audit Events](#)

Microsoft Cloud App Security monitors anomalous personnel user activity related to cloud apps to detect potential cybersecurity events. For Azure, the Audit Logs provides a view of many of the events that occurred against the subscription (who has access, what kind of access, and who gained/lost access). For Office 365, the Audit logs can be used to search for event



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>DE.CM-3 continued</p> <p>Personnel activity is monitored to detect potential cybersecurity events</p>		A.12.4.1	<p>Microsoft CAS – Anomaly Detection – SaaS Apps</p> <p>Azure Events – Audit Logs</p> <p>O365 – Audit Logging</p> <p>Windows Security Audit Events</p>	<p>information (date and time when event occurred, device IP address, user who performed action that triggered the vent, user activity, item created or modified (if applicable) and detail) for investigation purposes. For Windows, the security and system logs can be used to record and store collected security events so that an administrator can track key system and network activities to monitor potentially harmful behaviors and to mitigate those risks.</p>
<p>DE.CM-4</p> <p>Malicious code is detected</p>	5	A.12.2.1	<p>Office 365 Advanced Threat Protection (ATP)</p> <p>Windows Defender Advanced Threat Protection (ATP)</p> <p>Antimalware for Azure Services and VMs</p> <p>System Center – Endpoint Protection</p> <p>Microsoft Intune: Protecting Windows PCs against malware threats</p>	<p>Microsoft offers products and services for detection of unsafe attachments, malicious links, malware or unwanted software attempting to install or run on Azure systems. When System Center 2012 Endpoint Protection is used with Microsoft System Center 2012 Configuration Manager.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>DE.CM-4 continued</p> <p>Malicious code is detected</p>	5	A.12.2.1	<p>Office 365 Advanced Threat Protection (ATP)</p> <p>Windows Defender Advanced Threat Protection (ATP)</p> <p>Antimalware for Azure Services and VMs</p> <p>System Center – Endpoint Protection</p> <p>Microsoft Intune: Protecting Windows PCs against malware threats</p>	<p>it provides a comprehensive enterprise management solution that lets an organization do several things, including configuring default and custom antimalware policies that apply to groups of computers. Microsoft Intune can help an organization quickly protect and monitor managed Windows PCs against malware threats.</p>
<p>DE.CM-5</p> <p>Unauthorized mobile code is detected</p>		A.12.5.1	<p>Blacklisting/whitelisting apps for KNOX</p> <p>Blacklisting/whitelisting apps on iOS with Intune</p> <p>Compliant/noncompliant apps on Android with Intune</p>	<p>Microsoft offers blacklisting of mobile apps (blocking them on the device).</p>
<p>DE.CM-6</p> <p>External service provider activity is monitored to detect potential cybersecurity events</p>		A.14.2.7, A.15.2.1	<p>Microsoft Incident Response in the Cloud (see Customer Security Incident Notification section)</p>	<p>For Azure services, if during the investigation of a security event, Microsoft becomes aware that customer data has been accessed by an unlawful or unauthorized party, the security incident manager will immediately begin execution of the Customer Security Incident Notification Process.</p>



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>DE.CM-7</p> <p>Monitoring for unauthorized personnel, connections, devices, and software is performed</p>			<p>Microsoft Azure AD: Conditional Access</p> <p>Advanced Threat Analytics: Threats Detected</p> <p>Advanced Threat Analytics Implementation Services (ATAIS)</p> <p>AppLocker Overview – Application Auditing/Restrictions</p> <p>Windows Security Audit Events</p>	<p>Microsoft offers built-in capabilities for Azure AD, Advanced Threat Analytics and Windows to monitor for unauthorized personnel, connections, devices, and software (e.g. applications).</p>
<p>DE.CM-8</p> <p>Vulnerability scans are performed</p>		<p>A.12.6.1</p>	<p>Vulnerability Assessment in Azure Security Center</p> <p>SCCM Vulnerability Assessment</p> <p>Scan cloud application (Azure resources) for continuous assurance with AzSDK</p>	<p>The vulnerability assessment in Azure Security Center is part of the Security Center virtual machine (VM) recommendations. If Security Center doesn't find a vulnerability assessment solution installed on your VM, it recommends that you install one. SCCM Vulnerability Assessment allows scanning managed systems for common missing security updates and misconfigurations which might make client computers more vulnerable to attack. It is also possible to perform scanning of Azure workloads using Secure DevOps Kit for Azure.</p>



DE.DP: Detection Processes

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
DE.DP-1 Roles and responsibilities for detection are well defined to ensure accountability	5	A.6.1.1		
DE.DP-2 Detection activities comply with all applicable requirements		A.18.1.4		
DE.DP-3 Detection processes are tested		A.14.2.8	Microsoft Cloud – Red Teaming (Blog and link to whitepaper)	To help combat emerging threats, Microsoft employs an innovative Assume Breach strategy and leverages highly specialized groups of security experts, known as the Red Team, to strengthen threat detection, response and defense for its enterprise cloud services.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
----------	-----	--------------------	-------------------------------------	------------------------------------

DE.DP-4
 Event detection information is communicated to appropriate parties

A.16.1.2

DE.DP-5
 Detection processes are continuously improved

A.16.1.6

[Azure AD Identity Protection \(See section on using machine learning for continuous improvement\)](#)
[Windows Defender ATP – using threat intel to improve detection](#)

Microsoft Azure AD and Windows Defender ATP use machine learning to continuously learn of anomalies and suspicious incidents—thereby continuously improving detection.



RS.RP: Response Planning

Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
<p>RS.RP-1</p> <p>Response plan is executed during or after an event</p>	18	A.16.1.5	<p>Microsoft Azure Security Response in the Cloud</p> <p>Microsoft Incident Response and Shared Responsibility Incident Response Guide</p> <p>Responding to IT Security Incidents</p> <p>Azure AD role in Incident Response</p> <p>Leverage Azure Security Center and Azure Log Analytics (formerly Operations Management Suite) for Incident Response (video)</p> <p>Security Incident Management in Office 365</p>	<p>Microsoft provides: built-in capabilities in Azure for security response, written guidance on shared responsibility between Microsoft and customer for incident response (IR), advice on responding to incidents, and shares Azure AD's role in IR, how to use Azure Security Center and Azure Log Analytics for IR, and how Microsoft handles security incidents in Office 365. An organization may benefit from using some of the Azure capabilities for its response plan.</p>



RS.CO: Communications

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
RS.CO-1 Personnel know their roles and order of operations when a response is needed		A.6.1.1, A.16.1.1		
RS.CO-2 Events are reported consistent with established criteria		A.6.1.3, A.16.1.2		
RS.CO-3 Information is shared consistent with response plans		A.16.1.2		
RS.CO-4 Coordination with stakeholders occurs consistent with response plans				



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
RS.CO-5			Microsoft Active Protections Program	The Microsoft Active Protections Program (MAPP) is a program for security software providers that gives them early access to vulnerability information so that they can provide updated protections to customers faster.
<p>Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</p>				

RS.AN: Analysis

Analysis is conducted to ensure adequate response and support recovery activities.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
RS.AN-1		A.12.4.1, A.12.4.3, A.16.1.5		
<p>Notifications from detection systems are investigated</p>				
RS.AN-2		A.16.1.6	Microsoft Incident Response and Recovery Process Services	Microsoft provides human-based assistance with incident response, to determine the impact of an incident, among other things.
<p>The impact of the incident is understood</p>				



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
RS.AN-3 Forensics are performed		A.16.1.7	A guide to Windows Forensics Windows Security and Forensics course	Microsoft provides guidance and help through an online (free) tutorial on Windows Forensics.
RS.AN-4 Incidents are categorized consistent with response plans		A.16.1.4		

RS.MI: Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
RS.MI-1 Incidents are contained		A.16.1.5	Responding to IT Security Incidents Microsoft Incident Response and Recovery Process Services Windows Defender ATP – response actions	Microsoft provides advice on and human-based assistance with incident response. In addition, Windows Defender ATP offers controls to help quickly respond to detected attacks so that an organization can contain or reduce and prevent further damage caused by malicious attackers.



NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
RS.MI-2 Incidents are mitigated		A.12.2.1, A.16.1.5	Responding to IT Security Incidents Microsoft Incident Response and Recovery Process Services	Microsoft provides advice on and human-based assistance with incident response.
RS.MI-3 Newly identified vulnerabilities are mitigated or documented as accepted risks		A.12.6.1		

RS.IM: Improvements

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

NIST CSF	CCS	ISO/IEC 27001:2013	Microsoft Cyber Offerings that Help	Explanation of Microsoft Offerings
RS.IM-1 Response plans incorporate lessons learned		A.16.1.6		
RS.IM-2 Response strategies are updated				

This document is a commentary on the NIST Cybersecurity Framework, as Microsoft interprets it, as of the date of publication. Microsoft has spent a lot of time implementing the framework and considering opportunities for Microsoft technology to help organizations with their cybersecurity capabilities, but cybersecurity is highly fact-specific and this paper addresses only generally applicable concepts and may not perfectly align with all of your organization's needs.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. This document is provided for informational purposes only and should not be relied upon as legal advice or to determine how to precisely implement any specific aspect of the framework in a compliant manner. We encourage you to work with a legally qualified professional to discuss how best to ensure compliance and cybersecurity with applicable standards and regulations.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes only.



Published 6/8/2018

Version 2.0

© 2018 Microsoft Corporation. All rights reserved.