Microsoft

Mapping Microsoft Cyber Offerings to NIST Cybersecurity Framework (CSF) Subcategories

The NIST CSF is designed with the intent that individual businesses and other organizations use an assessment of the business risks they face to guide their use of the framework in a cost-effective way.

The Framework is typically customized based on organizations' unique risk posture (e.g., variance in threats, vulnerabilities, and risk tolerances, and how they implement the practices in the Framework). Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity 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.

In the table below, we have included four of the five Core Functions from the NIST CSF: Identify, Protect, Detect and Respond, because Microsoft Cyber Offerings can help with 61 of the 98 subcategories under those four high level functions. The resources (hyperlinks) listed reflect product information and how-to documentation. Where we have left subcategories blank, 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.

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.

ID.AM-1

Physical devices and systems within the organization are inventoried

- System Center Configuration Manager Inventory – for fully managed devices
- Active Directory – Domain Joined Devices
- Azure AD Registered Devices
- IoT Hub – Device Identity Registry
- Microsoft Intune Device Inventory – for lightly managed devices
- Windows Analytics

ID.AM-2

Software platforms and applications within the organization are inventoried

- 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

ID.AM-3

Organizational communication and data flows are mapped

- Shadow IT/SaaS App Discovery with Cloud App Security
- Operations Management Suite (OMS) Service Maps (Systems Interconnections)
- Azure Network Watcher
- Azure Network Security Groups – ACLs
- Azure IoT Hub IP Filtering
- Enhanced Security Administrative Environment (ESAE)

ID.AM-4

External information systems are catalogued

- Azure AD Integrated Apps
- Shadow IT/SaaS App Discovery with Cloud App Security

ID.AM-5

Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

Azure Information Protection – Data Classification
Privileged Access Reference Material
Azure AD Privileged Identity Management

ID.AM-6

Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Privileged Access Reference Material
Azure AD Privileged Identity Management
Just Enough Administration
Just in Time Administration – Privileged Access Management

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.

ID.BE-1

The organization's role in the supply chain is identified and communicated

Privileged Access Workstation
Design and Implementation for Active Directory (DIAD)

ID.BE-2

The organization's place in critical infrastructure and its industry sector is identified and communicated*

ID.BE-3

Priorities for organizational mission, objectives, and activities are established and communicated*

ID.BE-4

Dependencies and critical functions for delivery of critical services are established*

ID.BE-5

Resilience requirements to support delivery of critical services are established

Designing Resilient Applications for Microsoft Azure

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

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.

ID.GV-1

Organizational information security policy is established*

ID.GV-2

Information security roles & responsibilities are coordinated and aligned with internal roles and external partners

- Azure – Shared Responsibility
- Microsoft Incident Response and Shared Responsibility

ID.GV-3

Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

- Microsoft Compliance Offerings
- Cloud App Security – third-party risk evaluation and known certifications
- Microsoft and General Data Protection Regulation (GDPR)
- Privacy with Microsoft

ID.GV-4

Governance and risk management processes address cybersecurity risks

- Microsoft Cloud Services Risk Assessment

ID.RA: Risk Assessment

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

ID.RA-1

Asset vulnerabilities are identified and documented

- Qualys Virtual Scanner Appliance in Azure Marketplace
- Vulnerability Assessment in Azure Security Center
- Office 365 Secure Score
- Active Directory Risk Assessment
- Microsoft Cloud Services Risk Assessment
- Privileged Access Workstation
- Design and Implementation for Active Directory (DIAD)

ID.RA-2

Threat and vulnerability information is received from information sharing forums and sources

- Microsoft Security Intelligence
- Microsoft Operations Management Suite (OMS) Security and Compliance

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

ID.RA-3 Threats, both internal and external, are identified and documented	Microsoft Threat Modeling Tool Microsoft Threat Management Microsoft Operations Management Suite (OMS) Security and Compliance
ID.RA-4 Potential business impacts and likelihoods are identified*	
ID.RA-5 Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Cybersecurity Operations Service
ID.RA-6 Risk responses are identified and prioritized	Cybersecurity Operations Service

ID.RM: Risk Management Strategy

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

ID.RM-1 Risk management processes are established, managed, and agreed to by organizational stakeholders*	
ID.RM-2 Organizational risk tolerance is determined and clearly expressed*	
ID.RM-3 The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis*	

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

PR.AC: Access Control

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

PR.AC-1

Identities and credentials are managed for authorized devices and users

- Best Practices for Securing Active Directory
- Microsoft Identity Manager: Connect your Directories
- Connect Active Directory with Azure Active Directory
- Azure Active Directory – 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 Active Directory Domain Services
- Privileged Access Workstation
- Design and Implementation for Active Directory (DIAD)
- Azure Active Directory B2C
- Fast Start – Azure for Identity
- Dynamic Identity Framework (DIF)
- Enhanced Security Administrative Environment (ESAE)
- Microsoft Identity Manager Implementation Services
- Privileged Access Management
- Azure Active Directory Implementation Services (AADIS)
- Enterprise Modernization for Active Directory

PR.AC-2

Physical access to assets is managed and protected

- Protecting Data in Azure (Page 23, Physical Security)
- Privileged Access Workstation
- Design and Implementation for Active Directory (DIAD)

PR.AC-3

Remote access is managed

Conditional Access in Azure AD
Remote Desktop Services in Server 2016
Server 2016: Web Application Proxy
Secure Remote Access to on-premises applications: Azure AD App Proxy
Azure Security – Remote Management
Cloud App Security – Cloud App Governance and Control
Device Compliance Policies for Conditional Access
Privileged Access Workstation
Design and Implementation for Active Directory (DIAD)

PR.AC-4

Access permissions are managed, incorporating the principles of least privilege and separation of duties

Just Enough Administration (PowerShell - White Paper and Resources)
Just Enough Administration: Step by Step
Windows Server: Dynamic Access Control
Microsoft Azure: Role Based Access Control
Azure AD Privileged Identity Management
Privileged Access Management for Active Directory Domain Services
Privileged Access Workstation
Design and Implementation for Active Directory (DIAD)

PR.AC-5

Network integrity is protected, incorporating network segregation where appropriate

Microsoft Azure: Secure network with virtual appliances
Microsoft Cloud Services and Network Security
Azure Network Security Best Practices
Azure Network Security Whitepaper
Privileged Access Workstation
Design and Implementation for Active Directory (DIAD)

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.

PR.AT-1

All users are informed and trained

Enhanced Security Administrative Environment (ESAE)

PR.AT-2

Privileged users understand roles & responsibilities

Enhanced Security Administrative Environment (ESAE)

PR.AT-3

Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

Enhanced Security Administrative Environment (ESAE)

PR.AT-4

Senior executives understand roles & responsibilities	Enhanced Security Administrative Environment (ESAE)

PR.AT-5

Physical and information security personnel understand roles & responsibilities	Enhanced Security Administrative Environment (ESAE)

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.

PR.DS-1

Data-at-rest is protected	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 Azure Information Protection - 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 Cloud App Security – Govern Connected SaaS apps Azure SQL Transparent Data Encryption Privileged Access Workstation Enhanced Security Administrative Environment (ESAE) Design and Implementation for Active Directory (DIAD) Azure Information Protection Full Volume Encryption - Windows BitLocker Drive Encryption

PR.DS-2

Data-in-transit is protected	Azure VPN Gateway Azure ExpressRoute Office 365 Message Encryption Data Encryption SharePoint Online and OneDrive for Business SMB Encryption Remote Desktop Protocol Encryption Encrypting Connections to SQL Server Microsoft Trust Center – Encryption Internet Protocol Security (IPSec) Enhanced Security Administrative Environment (ESAE)

PR.DS-3

Assets are formally managed throughout removal, transfers, and disposition

Protecting Data in Azure (Page 18, Media Destruction)
Enhanced Security Administrative Environment (ESAE)

PR.DS-4

Adequate capacity to ensure availability is maintained

Azure Subscription Service Limits
Server 2016 Locks and Limits
Exchange Online Limits
SQL Server 2016 Limits
Operations Management Suite (OMS): Hyper-V Capacity Management Solution
Systems Center Operations Manager: Monitoring
Enhanced Security Administrative Environment (ESAE)

PR.DS-5

Protections against data leaks are implemented

Office 365 Data Loss Prevention
Windows Information Protection
Microsoft Cloud App Security and Data Loss Prevention
Microsoft Intune Mobile Application Management and Data Loss Prevention
Enhanced Security Administrative Environment (ESAE)

PR.DS-6

Integrity checking mechanisms are used to verify software, firmware, and information integrity

Windows Device Guard
Introduction to Code Signing
Signing PowerShell Scripts, Part 1
Signing PowerShell Scripts, Part 2
Deploying code integrity policies
Enhanced Security Administrative Environment (ESAE)

PR.DS-7

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

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

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.

PR.IP-1

A baseline configuration of information technology/ industrial control systems is created and maintained

Windows Security Baseline
Azure Automation Desired State Configuration
PowerShell Desired State Configuration
Compliance Settings in System Center Configuration Manager
Change Tracking with OMS - Log Analytics
Azure Security Center - Common Configuration Identifiers and Baseline Rules

	Privileged Access Workstation Enhanced Security Administrative Environment (ESAE) Design and Implementation for Active Directory (DIAD)
PR.IP-2 A System Development Life Cycle to manage systems is implemented	Microsoft Security Development Lifecycle Security Development Lifecycle Tools
PR.IP-3 Configuration change control processes are in place	Change Management for Enterprise: Office 365 Incident and Change Management with System Center Service Manager How Microsoft IT approaches Organization Change Management Skype for Business Change Management and Adoption Managing Changes and Activities with System Center
PR.IP-4 Backups of information are conducted, maintained, and tested periodically	System Center Data Protection Manager Azure Backup Enhanced Security Administrative Environment (ESAE)
PR.IP-5 Policy and regulations regarding the physical operating environment for organizational assets are met	Azure Security, Privacy, and Compliance Whitepaper Security and Compliance in Office 365 Enhanced Security Administrative Environment (ESAE)
PR.IP-6 Data is destroyed according to policy	Retention Policies in Office 365 Compliance Center Protecting Data in Microsoft Azure (See Media Destruction and Data Deletion)
PR.IP-7 Protection processes are continuously improved	Office 365 Secure Score Microsoft Enterprise Cloud Red Teaming (PDF download) Penetration testing of your Azure hosted Applications
PR.IP-8 Effectiveness of protection technologies is shared with appropriate parties*	
PR.IP-9 Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Microsoft Azure Security Response in the Cloud Office 365 Security Incident Management Responding to Security IT Incidents Azure Site Recovery Cybersecurity Operations Service

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

PR.IP-10

Response and recovery plans are tested

Test Failover to Azure in Site Recovery

PR.IP-11

Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)*

PR.IP-12

A vulnerability management plan is developed and implemented

Vulnerability Assessment in Azure Security Center
Vulnerabilities detected by Azure AD Identity Protection
System Center Configuration Manager Vulnerability Assessment Pack
Enhanced Security Administrative Environment (ESAE)

PR.MA: Maintenance

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

PR.MA-1

Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

Windows Automatic Maintenance
Azure Security and Audit Log Management

PR.MA-2

Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

Azure AD B2B
Azure Security and Audit Log Management
Privileged Access Workstation
Enhanced Security Administrative Environment (ESAE)
Design and Implementation for Active Directory (DIAD)

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.

PR.PT-1

Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Azure Security and Audit Log Management
Microsoft Azure log integration/Security Information/SIEM systems
Office 365 Audit logs
Azure log analytics
Active Directory Auditing
Windows Server 2016 Security Auditing
Azure Information Protection Logging
Cloud App Security - Governance & Audit for Microsoft & 3rd party SaaS apps

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

	Cloud App Security SIEM integration SQL Server Audit Microsoft Dynamics Auditing Overview Privileged Access Workstation Design and Implementation for Active Directory (DIAD)
PR.PT-2 Removable media is protected and its use restricted according to policy	BitLocker Policy reference – Windows 10 (See the Removable Drive section) Control Access to Removable Media (Group Policy) Privileged Access Workstation Enhanced Security Administrative Environment (ESAE) Design and Implementation for Active Directory (DIAD) Full Volume Encryption - Windows BitLocker Drive Encryption
PR.PT-3 Access to systems and assets is controlled, incorporating the principle of least functionality	Application Whitelisting w/ Win10 Device Guard, AppLocker, & Configuration Mgr AppLocker: Application Whitelisting Server 2016 Hardening Guideline Privileged Access Workstation Enhanced Security Administrative Environment (ESAE) Design and Implementation for Active Directory (DIAD)
PR.PT-4 Communications and control networks are protected	Creating and using network isolated environments (SCVMM, Hyper-V) Introduction to Server and Domain Isolation (reference) Azure Network Security Whitepaper Privileged Access Workstation Enhanced Security Administrative Environment (ESAE) Design and Implementation for Active Directory (DIAD)

DE.AE: Anomalies and Events

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

DE.AE-1

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 Cloud App Security - Anomaly Detection - SaaS Apps
- Azure Security Center - see Anomaly Detection
- Office 365 - Anomaly Detection with ASM
- Monitoring networks with System Center Operations Manager
- Privileged Access Workstation
- Design and Implementation for Active Directory (DIAD)

DE.AE-2

Detected events are analyzed to understand attack targets and methods

- OMS - Log Analytics
- Advanced Threat Analytics - working with suspicious activities
- Advanced Threat Analytics Implementation Services (ATAIS)
- Privileged Access Workstation
- Enhanced Security Administrative Environment (ESAE)
- Design and Implementation for Active Directory (DIAD)

DE.AE-3

Event data are aggregated and correlated from multiple sources and sensors

- OMS - Log Analytics
- Advanced Threat Analytics - SIEM integration
- Advanced Threat Analytics Implementation Services (ATAIS)
- Azure logs - SIEM integration
- SIEM integration - Cloud App Security
- Privileged Access Workstation
- Design and Implementation for Active Directory (DIAD)

DE.AE-4

Impact of events is determined

- Azure AD Risk Events
- Privileged Access Workstation
- Design and Implementation for Active Directory (DIAD)
- Cybersecurity Operations Service

DE.AE-5

Incident alert thresholds are established

- Creating alert rules in Log Analytics
- Office 365 - creating security and audit alerts
- Azure AD Privileged Identity Management - Creating Alerts
- Azure AD Risk Events
- Azure Security Center - managing alerts
- Managing alerts in System Center Operations Manager
- Cloud App Security - Control cloud apps with policies (fine tuning thresholds)
- Advanced Threat Analytics - working with suspicious activities
- Advanced Threat Analytics Implementation Services (ATAIS)
- Privileged Access Workstation
- Design and Implementation for Active Directory (DIAD)
- Cybersecurity Operations Service

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.

DE.CM-1

The network is monitored to detect potential cybersecurity events

- OMS - Security and Audit Solution
- Index of Security related information from SCOM
- Advanced Threat Analytics - Events Detected
- Advanced Threat Analytics Implementation Services (ATAIS)
- Azure Network Security

DE.CM-2

The physical environment monitored to detect potential cybersecurity events

- Azure Security and Compliance (See Infrastructure Protection section)

DE.CM-3

Personnel activity is monitored to detect potential cybersecurity events

- Microsoft Cloud App Security - Anomaly Detection - SaaS Apps
- Azure Events - Audit Logs
- O365 - Audit Logging
- Windows Security Audit Events

DE.CM-4

Malicious code is detected

- Office 365 Advanced Email Protection
- Windows Defender Advanced Threat Protection

	Antimalware for Azure Services and VMs System Center - Endpoint Protection Microsoft Intune: Protecting Windows PCs against malware threats Enhanced Security Administrative Environment (ESAE)
DE.CM-5 Unauthorized mobile code is detected	Whitelisting/blacklisting apps for KNOX Blacklisting/whitelisting apps on iOS with Intune Compliant/noncompliant apps on Android with Intune
DE.CM-6 External service provider activity is monitored to detect potential cybersecurity events	Microsoft Incident Response in the Cloud (see Customer Notification section)
DE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed	Microsoft Azure AD: Conditional Access Advanced Threat Analytics: Threats Detected Advanced Threat Analytics Implementation Services (ATAIS) AppLocker Overview - Application Auditing/Restrictions Windows Security Audit Events
DE.CM-8 Vulnerability scans are performed	Qualys Virtual Scanner Appliance in Azure Marketplace Vulnerability Assessment in Azure Security Center System Center Configuration Manager Vulnerability Assessment Pack Enhanced Security Administrative Environment (ESAE)

DE.DP: Detection Processes

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

DE.DP-1 Roles and responsibilities for detection are well defined to ensure accountability*	
DE.DP-2 Detection activities comply with all applicable requirements*	
DE.DP-3 Detection processes are tested	Microsoft Cloud - Red Teaming (Blog and link to whitepaper)

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

DE.DP-4 Event detection information is communicated to appropriate parties*	
DE.DP-5 Detection processes are continuously improved	Azure AD Identity Protection (See machine learning for continuous improvement) Windows Defender Advanced Threat Protection - threat intel to improve detection

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

RS.RP: Response Planning

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

RS.RP-1

Response plan is executed during or after an event

- Microsoft Azure Security Response in the Cloud
- Microsoft Incident Response & Shared Responsibility Incident Response Guide
- Responding to Security IT Incidents
- Azure AD role in Incident Response
- Leverage Azure Security Center & Operations Mgmt Suite for Incident Response (vid)
- Security Incident Management in Office 365

RS.CO: Communications

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

RS.CO-1

Personnel know their roles and order of operations when a response is needed*

RS.CO-2

Events are reported consistent with established criteria*

RS.CO-3

Information is shared consistent with response plans*

RS.CO-4

Coordination with stake-holders occurs consistent with response plans*

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

RS.CO-5

Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

Microsoft Active Protections Program

RS.AN: Analysis

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

RS.AN-1

Notifications from detection systems are investigated*

RS.AN-2

The impact of the incident is understood*

RS.AN-3

Forensics are performed

A guide to Windows Forensics

Windows Security and Forensics course

RS.AN-4

Incidents are categorized consistent with response plans*

RS.MI: Mitigation

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

RS.MI-1

Incidents are contained

Responding to Security IT Incidents

Windows Defender Advanced Threat Protection – response actions

RS.MI-2

Incidents are mitigated

Responding to Security IT Incidents

RS.MI-3

Newly identified vulnerabilities are mitigated or documented as accepted risks*

RS.IM: Improvements

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

RS.IM-1

Response plans incorporate lessons learned*

RS.IM-2

Response strategies updated*

*The activity should be covered by the implementing organization utilizing internal resources or third parties.

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 12/5/2017
Version 1.0