



NIST 800-171 Rev. 2 Compliance as a Service

Partner Enablement

Vandy Rodrigues
Clayton Barlow
Matthew Perry
Simona Kovatcheva



Agenda



OVERVIEW NIST CSF
(NEW TO FRAMEWORK)



NIST CYBER SECURITY
FRAMEWORK VER. 1.1
(DEEP DIVE)



THE FIVE FUNCTIONS
(PPT VERSION)



NIST 800-171
OVERVIEW



AZURE CAPABILITIES



BUILDING A SCALABLE
NIST 800-171
ENVIRONMENT



BUSINESS VALUE –
DEMONSTRATING AND
STAYING COMPLIANT

NIST CyberSecurity Framework (CSF)

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:



Describe their current cybersecurity posture



Define their target state for cybersecurity



Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process



Assess progress toward the target state



Communicate amongst internal and external stakeholders about cybersecurity risk

CyberSecurity Framework: Three Primary Components

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources **using** the desired outcomes of the Framework Core

Tiers

A qualitative measure of organizational cybersecurity risk management practices



NIST Cyber Security Framework

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state;
- Communicate among internal and external stakeholders about cybersecurity risk



CSF Core - Function, Category, Subcategory, Reference

| Function | Category | ID |
|----------|---|-------|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| | Supply Chain Risk Management | ID.SC |
| Protect | Identity Management and Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

| Subcategory | Informative References |
|---|--|
| ID.BE-1: The organization's role in the supply chain is identified and communicated | COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12 |
| ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated | COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8 |
| ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14 |
| ID.BE-4: Dependencies and critical functions for delivery of critical services are established | COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 |
| ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 |

NIST 800-171 Overview

NIST 800-171 Rev. 2



Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations



The requirements recommended for use in this publication are derived from [FIPS 200] and the moderate security control baseline in [SP 800-53] and are based on the CUI regulation [32 CFR 2002].



The recommended security requirements contained in this publication are only applicable to a nonfederal system or organization when mandated by a federal agency in a contract, grant, or other agreement.



The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

NIST 800-171 Control Families

Access Control

Awareness and Training

Audit and Accountability

Configuration Management

Identification and Authentication

Incident Response

Systems and Communications Protection

Maintenance

Media Protection

Personnel Security


Physical Protection

Risk Assessment

Security Assessment

System and Information Integrity

CRM – Customer Responsibility Matrix

| 1  | | Azure Security and Compliance Blueprint | | Reference architecture control coverage | | | Version last update | How To: (Prescriptive Guidance how to enable the control) | How to Automate (Options how to automation with ARM) |
|---|------------|--|-----------------------------------|---|---|--|---------------------|---|--|
| 2 | Control ID | Control description | NIST SP 800-53 Controls Reference | Reference architecture coverage | Key Azure service | Service configuration detail | | | |
| 3 | 3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | AC-02 AC-03 AC-17 | Yes | Azure Active Directory | This reference architecture enforces logical access authorizations using role-based access control enforced by Azure Active Directory by assigning users to roles. Azure Active Directory roles assigned to users or groups control logical access to resources within Azure at the resource, group, or subscription level. | | Assign RBAC roles to users, security groups, service principals, or managed identities | Create PowerShell scripts or runbooks to automate RBAC role assignment Use ARM templates to assign RBAC roles |
| 5 | 3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | AC-02 AC-03 AC-17 | Yes | Azure Active Directory | This reference architecture enforces logical access authorizations using role-based access controls enforced by Azure Active Directory by assigning users to roles. Azure Active Directory roles assigned to users or groups control logical access to resources within Azure at the resource, group, or subscription level. | | Assign RBAC roles to users, groups, service principals, or managed identities Create custom RBAC roles to assign to users, groups, service principals, or managed identities | Create PowerShell scripts or runbooks to automate RBAC role creation and assignment Create ARM templates to create RBAC roles and assign them |
| 6 | 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | AC-4 | Yes - Partial | Azure Networking | This reference architecture enforces information flow restrictions through the use of network security groups applied to the subnets in which resources are deployed. Network security groups ensure that information flow is controlled between resources based on approved rules. The customer is responsible for developing network security group and rules that control the flow of CUI for customer bulk data imports. | | Create Network Security Groups and associate them with subnets or NICs or both Create appropriate rules in those NSGs for your traffic needs Consider using Application Security Groups to minimize number of NSGs Follow least privilege principle when assigning RBAC roles (i.e. assign role at resource group level instead of subscription level) | Create PowerShell scripts or runbooks to automate NSG creation and association Create ARM templates to create NSGs and rules |
| 7 | 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | AC-5 | No | | | | | Create PowerShell scripts or runbooks to automate RBAC role assignment Create ARM templates to assign RBAC roles |
| 8 | 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | AC-06 AC-06 (01) AC-06 (05) | Yes - Partial | Azure Active Directory | This reference architecture implements role-based access control which can be configured to separate duties according to organization requirements. Azure Active Directory account privileges are implemented using role-based access controls by assigning users to roles. The customer is responsible for appropriately assigning users to roles and/or security groups. Furthermore, the customer is responsible for implementing a process or service, such as Azure Active Directory Privileged Identity Management, to lower the exposure time of privileges and increase visibility into the use of security functions and privileged accounts through reports and alerts. | | Assigns roles at the appropriate levels (i.e. resource, resource group, subscription scopes) Create custom roles to define specific functions required Manage privileged identities with Privileged Identity Management tool in Azure AD (need P2 licensing). Monitor security alerts in Azure AD or through Security Center Identity & Access | Create PowerShell scripts or runbooks to automate RBAC role creation and assignment Create ARM templates to create RBAC roles and assign them |
| 9 | 3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions. | AC-06 (02) | No | | | | | |
| 10 | 3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | AC-06 (09) AC-06 (10) | Yes - Partial | Azure Active Directory | This reference architecture implements role-based access control to restrict users to only privileges explicitly assigned in Azure Active Directory. Activity logs capture operations performed on Azure resources. The customer is responsible for appropriately assigning users to roles and/or security groups. | | Assign RBAC roles to users, groups, service principals, or managed identities Assign Azure AD administrator roles to appropriate users Managed privileged identities (i.e. administrators) with Privileged Identity Management tool in Azure AD | Automate with Powershell runbooks and ARM templates Once Azure automation account created, can use runbook gallery with examples |
| 11 | 3.1.8 | Limit unsuccessful logon attempts. | AC-07 | Yes - Partial | Azure Active Directory Azure portal | The Azure portal limits consecutive invalid logon attempts by users and locks the account after the limit is reached. Azure Active Directory can be used to limit consecutive invalid logon attempts (e.g. no more than three within a 15 minute period) by locking the user account when the login attempt limit is reached. | | Smart Lookup is enabled automatically on users, but you can change lockout threshold and lockout duration in seconds | Through portal only |
| 12 | 3.1.9 | Provide privacy and security notices consistent with applicable CUI rules. | AC-08 | No | | | | | |
| 13 | 3.1.10 | Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity. | AC-11 AC-11 (01) | No | | | | | |
| 14 | 3.1.11 | Terminate (automatically) a user session after a defined condition. | AC-12 | Yes | Azure portal | The settings to automatically terminate a user session can be configured in the Azure portal to meet organization session termination requirements for the resource group. | | Create conditional access policies in Azure Active Directory | Coming soon to Powershell and Graph API |
| 15 | 3.1.12 | Monitor and control remote access sessions. | AC-17 (01) | Yes - Partial | Azure Active Directory Azure Security Center | This reference architecture provides remote access to the information system through the Azure portal or a customer-implemented ExpressRoute or VPN gateway. Access through the Azure portal is audited. | | Create Express Route or VPN connection (or both in conjunction) as hybrid | Create and configure Express Route and VPN with Powershell scripts and |

<https://github.com/microsoft/azuredevopsgenerator/blob/master/nist800171Rev2/Customer%20Reponsibility%20Matrix%20-%20NIST%20800-171.xlsx>

Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171

NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

Patricia Toth

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.HB.162>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

This publication is available free of charge from: <https://doi.org/10.6028/NIST.HB.162>

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

Does the company use passwords?

Yes No Partially Does Not Apply Alternative Approach

Does the company have an authentication mechanism?

Yes No Partially Does Not Apply Alternative Approach

Does the company require users to login to gain access?

Yes No Partially Does Not Apply Alternative Approach

Are account requests authorized before system access is granted?

Yes No Partially Does Not Apply Alternative Approach

Does the company maintain a list of authorized users, defining their identity and role and sync with system, application, and data layers?

Yes No Partially Does Not Apply Alternative Approach

Additional information:

User access security refers to the set of procedures by which authorized users access the system and unauthorized users are prevented accessing the system.

Where to Look:

- access control policy
- account management procedures
- access enforcement procedures
- security plan
- configuration management plan
- information system design documentation
- information system configuration settings and associated documentation
- list of active system accounts along with the name of the individual associated with each account
- list of conditions for group and role membership
- notifications or records of recently transferred, separated, or terminated employees

- list of recently disabled information system accounts along with the name of the individual associated with each account
- list of approved authorizations (user privileges)
- access authorization records
- account management compliance reviews
- information system monitoring records
- information system audit records
- remote access implementation and usage (including restrictions) procedures
- remote access authorizations

Who to Talk to:

- employees with account management responsibilities
- system/network administrators
- employees with responsibilities for managing remote access connections
- employees with information security responsibilities
- employees with access enforcement responsibilities
- system developers

Perform Test On:

- processes account management on the information system
- automated mechanisms for implementing account management
- automated mechanisms implementing access control policy
- remote access management capability

Scope: Azure NIST 800-171



| NIST 800-171 CONTROL FAMILIES | |
|---------------------------------------|----------------------------------|
| Access Control | Awareness and Training |
| Audit and Accountability | Configuration Management |
| Identification and Authentication | Incident Response |
| Systems and Communications Protection | Maintenance |
| Media Protection | Personnel Security |
| Physical Protection | Risk Assessment |
| Security Assessment | System and Information Integrity |

Azure Capabilities

Securing the Platform

Security Development Lifecycle (SDL)

- ✓ Security Embedded in Planning, Design, Development, & Deployment

Infrastructure security controls

- ✓ Datacenter Security
- ✓ Secure Multi-tenancy
- ✓ Network Protection
- ✓ DDoS Defense
- ✓ Data Segregation
- ✓ Data Protection

Operational security controls

- ✓ Prevent & Assume Breach Strategy
- ✓ Incident Response
- ✓ Access Policy & Controls
- ✓ Threat Detection
- ✓ Forensics

Compliance

- ✓ Strategy
- ✓ Certifications

Azure compliance

Global



- ✓ CSA STAR Attestation
- ✓ CSA STAR Certification
- ✓ CSA STAR Self-Assessment

- ✓ ISO 22301
- ✓ ISO 27001
- ✓ ISO 27017

- ✓ ISO 27018
- ✓ SOC 1 Type 2
- ✓ SOC 2 Type 2

U.S. Government



- ✓ CJIS
- ✓ DoD DISA SRG Level 2
- ✓ DoD DISA SRG Level 4
- ✓ DoD DISA SRG Level 5

- ✓ FedRAMP
- ✓ FIPS 140-2
- ✓ High JAB P-ATO
- ✓ IRS 1075

- ✓ ITAR
- ✓ Moderate JAB P-ATO
- ✓ Section 508 VPAT
- ✓ SP 800-171

Industry



- ✓ CDSA
- ✓ FACT UK
- ✓ FERPA
- ✓ FFIEC

- ✓ FISC Japan
- ✓ GLBA
- ✓ GxP 21 CFR Part 11
- ✓ HIPAA / HITECH
- ✓ HITRUST

- ✓ IG Toolkit UK
- ✓ MARS-E
- ✓ MPAA
- ✓ PCI DSS Level 1
- ✓ Shared Assessments

Regional

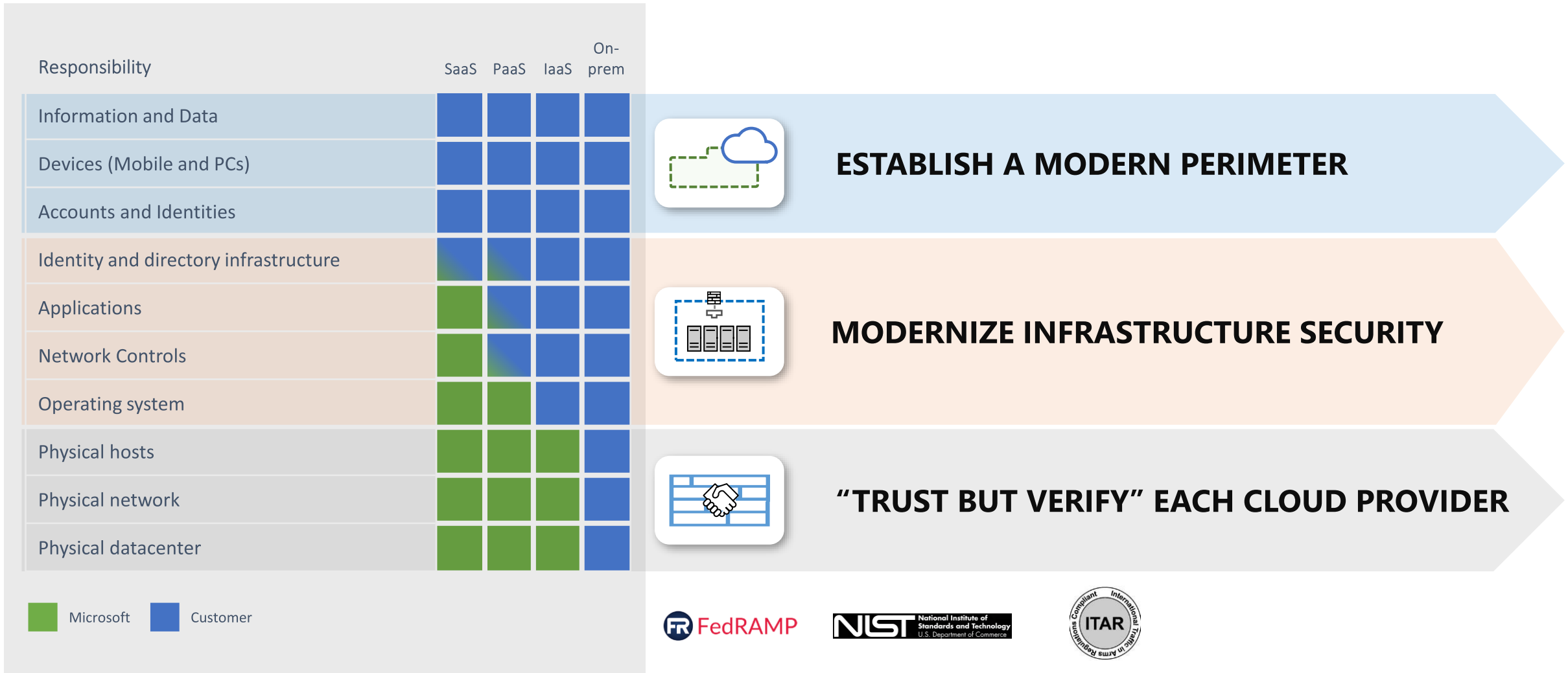


- ✓ Argentina PDPA
- ✓ Australia IRAP/CCSL
- ✓ Canada Privacy Laws
- ✓ China DJCP
- ✓ China GB 18030
- ✓ China TRUCS

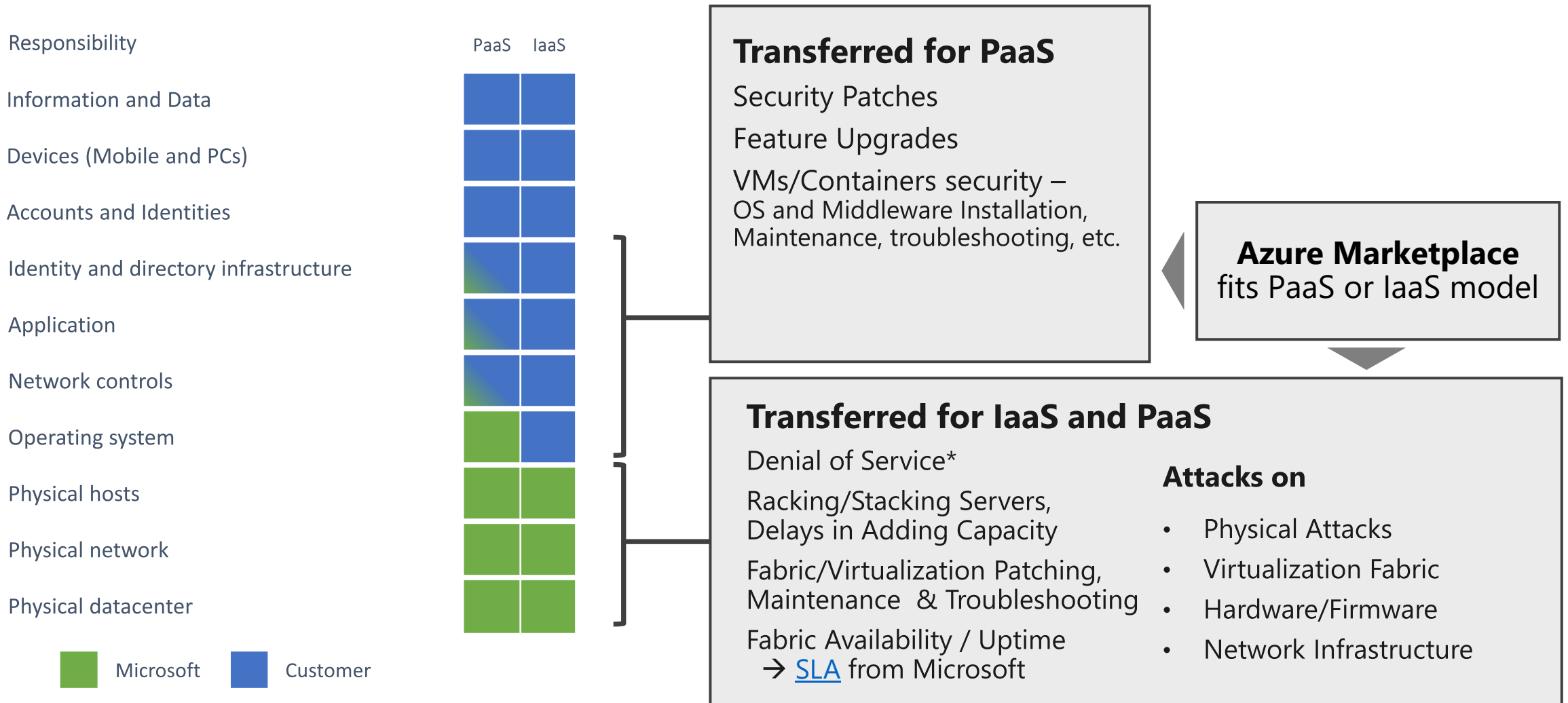
- ✓ ENISA IAF
- ✓ EU Model Clauses
- ✓ EU-US Privacy Shield
- ✓ Germany IT Grundschutz
- ✓ India MeitY
- ✓ Japan CS Mark Gold

- ✓ Japan My Number Act
- ✓ New Zealand GCIO
- ✓ Singapore MTCS
- ✓ Spain DPA
- ✓ Spain ENS
- ✓ UK G-Cloud

Shared Responsibility and Key Strategies



Security Responsibilities Transfer to Cloud Provider



Azure Governance & Compliance Orchestration



Compose



Orchestrate



Control



Enable

Compose and
construct cloud
environment in a
repeatable
manner

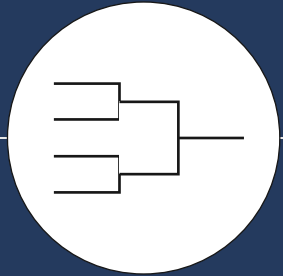
Orchestrate
resource template
deployment

Lock down
foundational
infrastructure that
are shared across
subscriptions

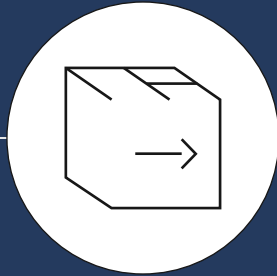
Let app teams
operate within a
governed &
standardized
subscription in a
self-service
manner

Azure Blueprint

Fast track to certification and compliance of applications built on Azure



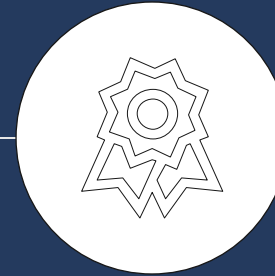
Architecture



Deployment



Certification



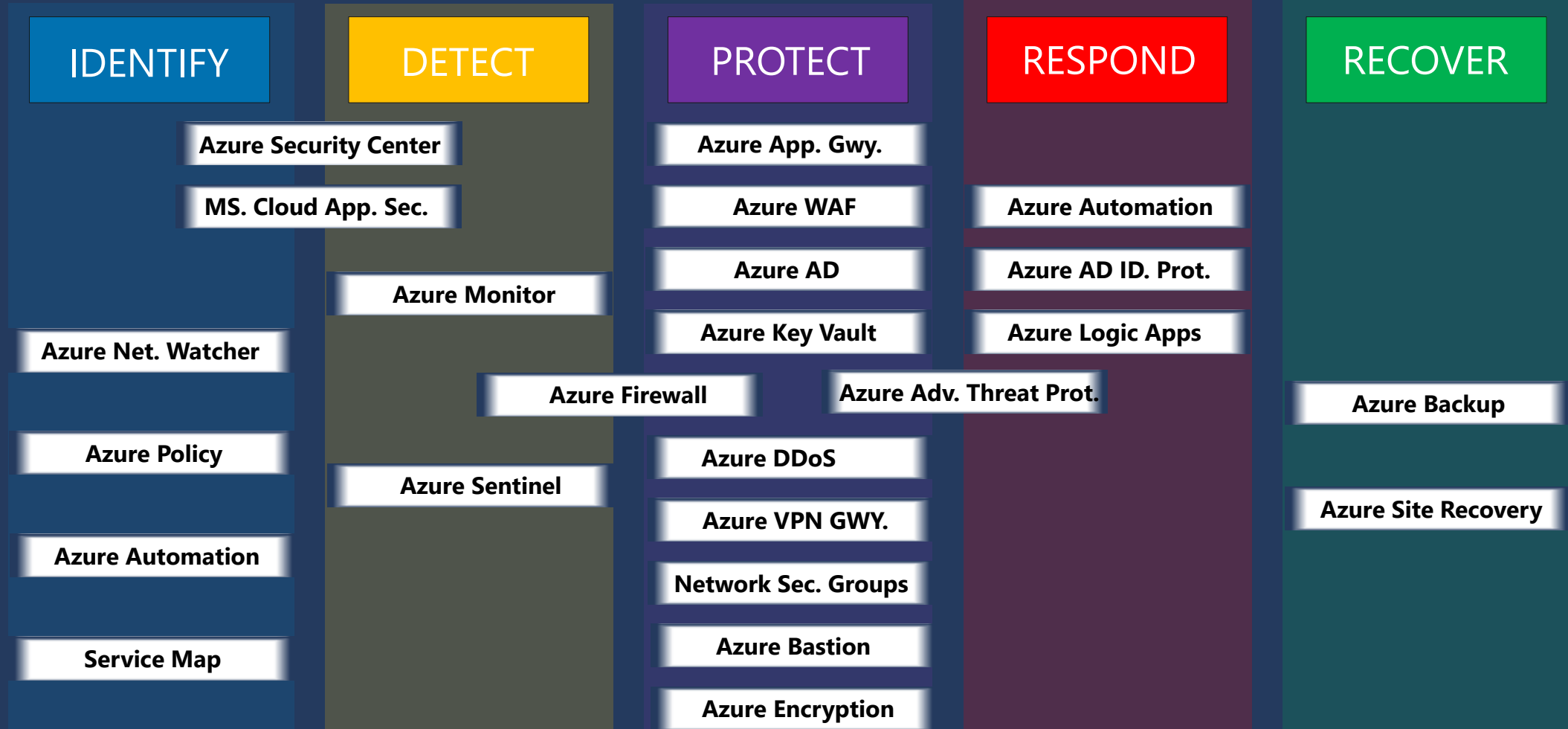
Expertise



Partnership

5-step process that streamlines paperwork through templates and tools, and allows your security professionals to focus on security – not paperwork

Azure Security Stack vs. NIST Cybersecurity Framework



Execution Process

Execution – NIST 800 171

Requirements



Create or use an existing Azure DevOps organization



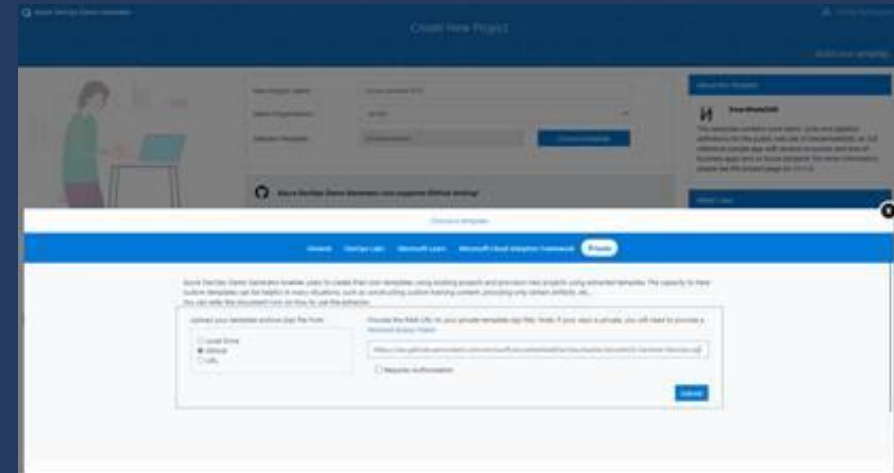
Access to Azure NIST 800-171 DevOpsTemplate (Github)



Access to Azure DevOps Generator

Azure DevOps NIST 800-171 Template

Azure DevOps Generator



Access to [Azure DevOps Generator](#)

Azure DevOps Project – Template: Agile

NT

NIST 800-171 Template

+

Overview

Boards

Work items

Boards

Backlogs

Sprints

Queries

Repos

Pipelines

Test Plans

Artifacts

Compliance

NIST 800-171 Template Team

▼

★

🔍

Backlog

Analytics

+ New Work Item

👁 View as Board

🔗 Column Options

...

Stories ▼

🔧

🔍

⚙

🔗

| + | Order | Work Item Type | Title | State | Story ... | Value Area |
|---|-------|----------------|---|-------|-----------|------------|
| + | 1 | User Story | > Prerequisites | ● New | | Business |
| | 2 | User Story | > Assess the workload | ● New | | Business |
| | 3 | User Story | > VM - UX Server | ● New | | Business |
| | 4 | User Story | > VM - Middle Tier | ● New | | Business |
| | 5 | User Story | > VM 3 - SQL Server | ● New | | Business |
| | 6 | User Story | > Test Workload | ● New | | Business |
| | 7 | User Story | > Optimize Workload Assets | ● New | | Business |
| | 8 | User Story | > Promote Workload | ● New | | Business |
| | 9 | User Story | > Decomission Retired Assets | ● New | | Business |
| | 10 | User Story | > Extend the landing zone for VMWare | ● New | | Business |
| | 11 | User Story | > Migrate VMs | ● New | | Business |
| | 12 | User Story | > Update migration assessment, decision tree, and tooling | ● New | | Business |
| | 13 | User Story | Azure Architecture Framework | ● New | | Business |
| | 14 | User Story | Azure Readiness Guide | ● New | | Business |
| | 15 | User Story | Landing zone considerations | ● New | | Business |
| | 16 | User Story | > Azure Subscription Architecture | ● New | | Business |
| | 17 | User Story | > Identity and Access Management | ● New | | Business |
| | 18 | User Story | > Azure Network Architecture | ● New | | Business |
| | 19 | User Story | > Governance, Security and Compliance | ● New | | Business |
| | 20 | User Story | > Monitoring and Reporting | ● New | | Business |
| | 21 | User Story | > Cloud Automation | ● New | | Business |

Planning

✕

Drag and drop work items to include them in a sprint.

NIST 800-171 Template Team Backlog

Iteration 2

Current

4/1/2020 - 4/22/2020

Planned Effort: -

16 working days

18

Iteration 3

4/23/2020 - 5/14/2020

16 working days

No work scheduled yet

+ New Sprint

Building a Scalable Environment

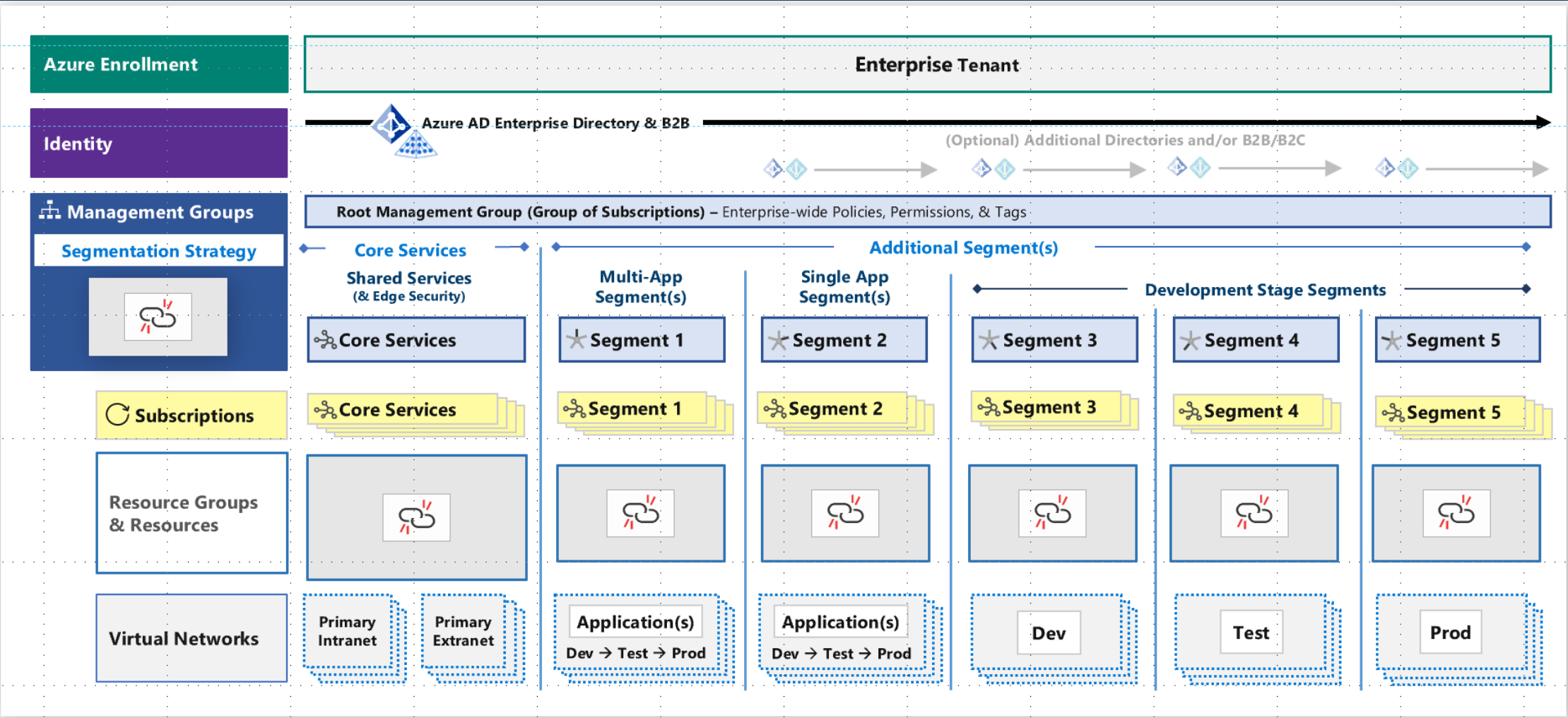
Business Value

Time to Research

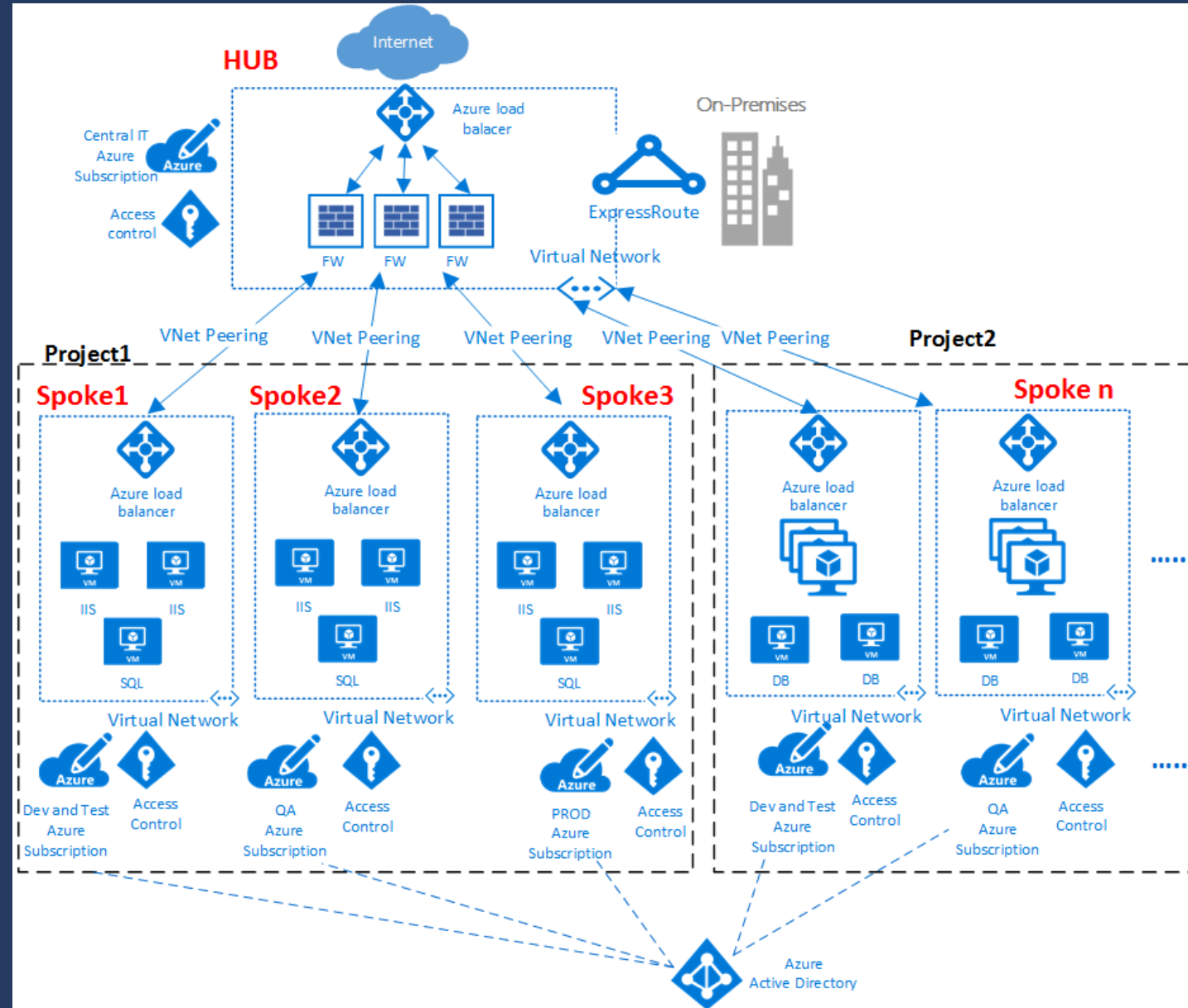
Ensuring Compliance Through Consistency

Drive Practice Maturity

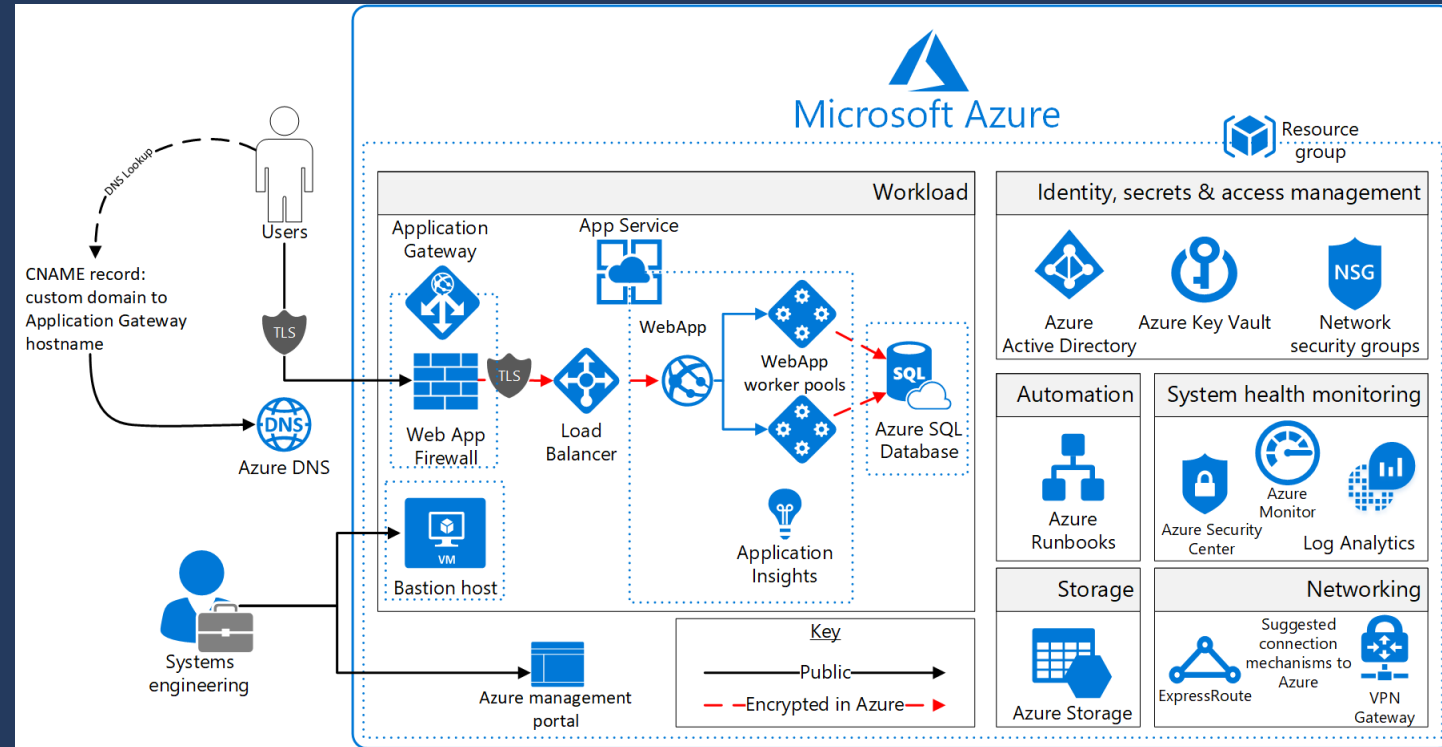
Reference Design - Azure Administration Model



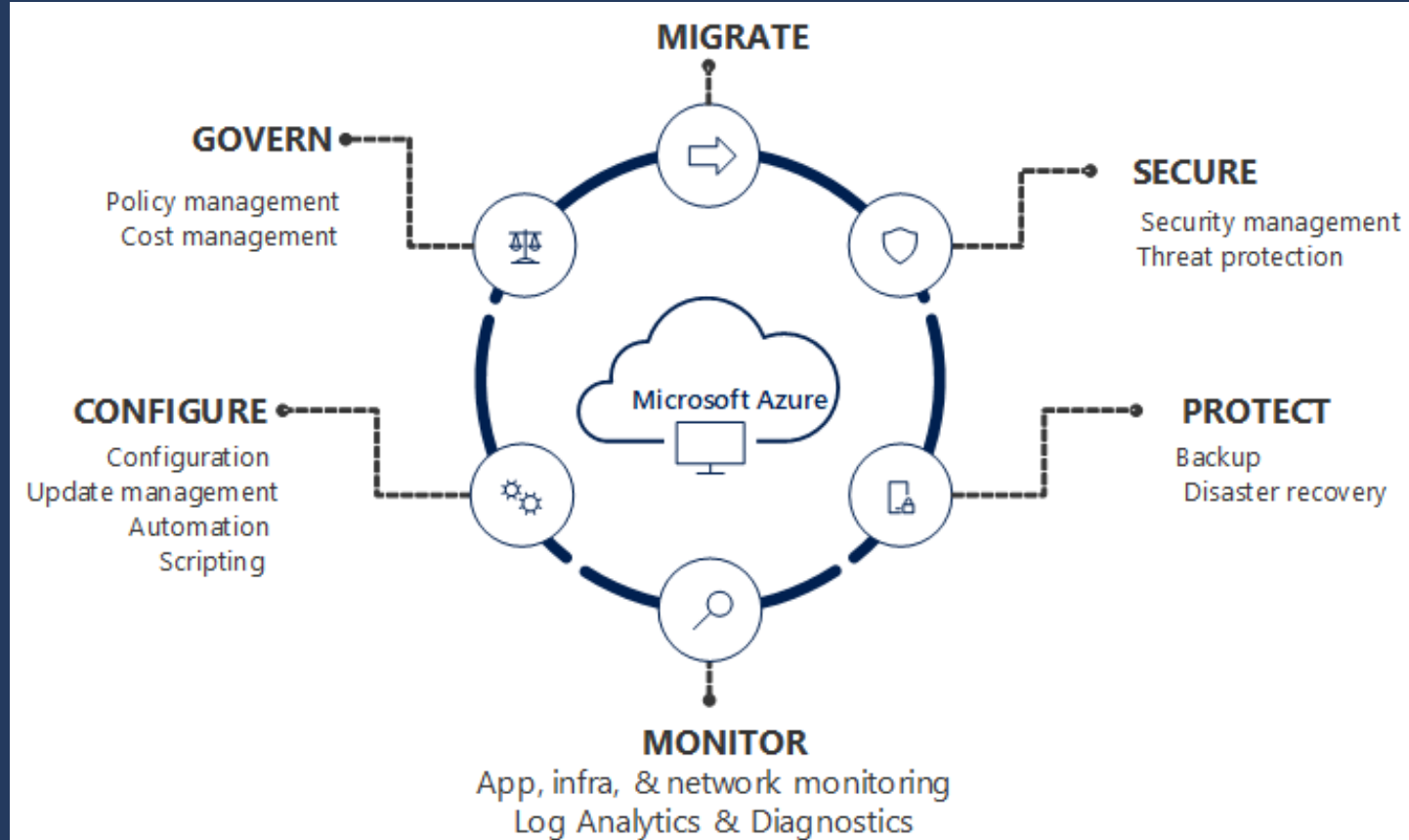
Azure Virtual Data Center: Hub & Spoke Architecture



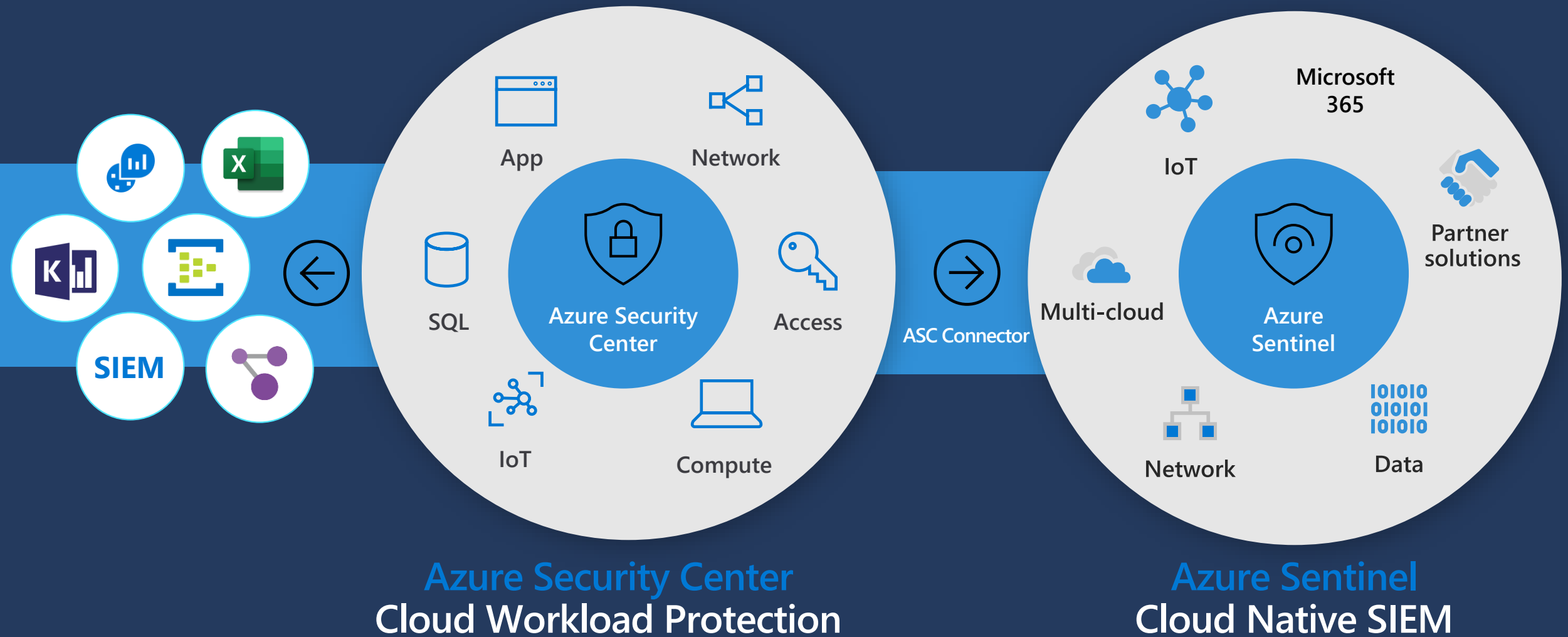
Deploying Compliance and Staying compliant with Azure Blueprint



Management Services in Azure



Threat protection for cloud at scale: Export assessments and alerts for security roles



Appendix

Cloud Adoption Framework Journey



Cloud Adoption Framework Tools (Optional)

Tools to help you get started

Discover relevant tools and personalized recommendations to help you explore cloud adoption, define your strategy, and remove your blockers.



Navigate quickly to relevant content in the Cloud Adoption Framework

Identify your cloud adoption needs with an assessment in this cloud journey tracker tool—and find recommendations for your unique cloud journey.

[Discover where you are in your cloud journey >](#)



Define your governance baseline

Use this assessment to help you identify gaps in your organization's current state of governance. Get a personalized benchmark report and curated guidance on how to get started.

[Set up the governance benchmark >](#)



Evaluate workloads against resiliency best practices

Mitigate concerns by evaluating workloads across the five pillars of resiliency, scalability, DevOps, security, and cost.

[Take the Azure Architecture Review >](#)

Source: <https://azure.microsoft.com/en-us/cloud-adoption-framework/#cloud-adoption-journey>