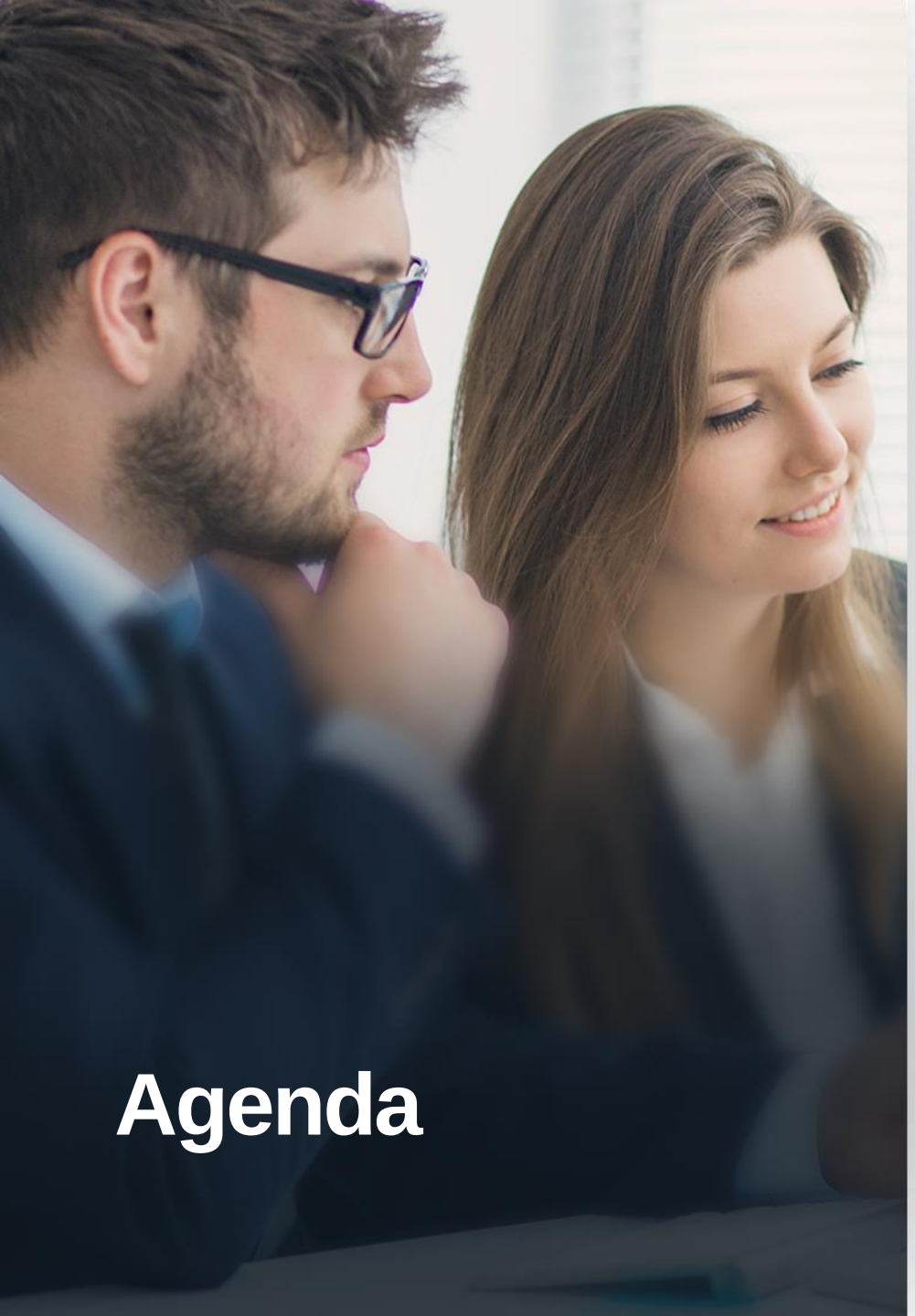
Microsoft | MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

CLOUD SUCCESS PLAN FOR AZURE

INTRODUCTION TO SECURITY

Mike McKanna, PMP, ITIL
CSA-E
February 7, 2023



Agenda

- Introduction to:
  - Zero Trust Architecture
  - Defense in Depth
  - Microsoft Cloud Adoption Framework (CAF) Secure
- Fulfill Your Security Responsibility
- Azure Security Benchmark
- SACA [Optional]
- Resources, Recommendations, & Learning availability

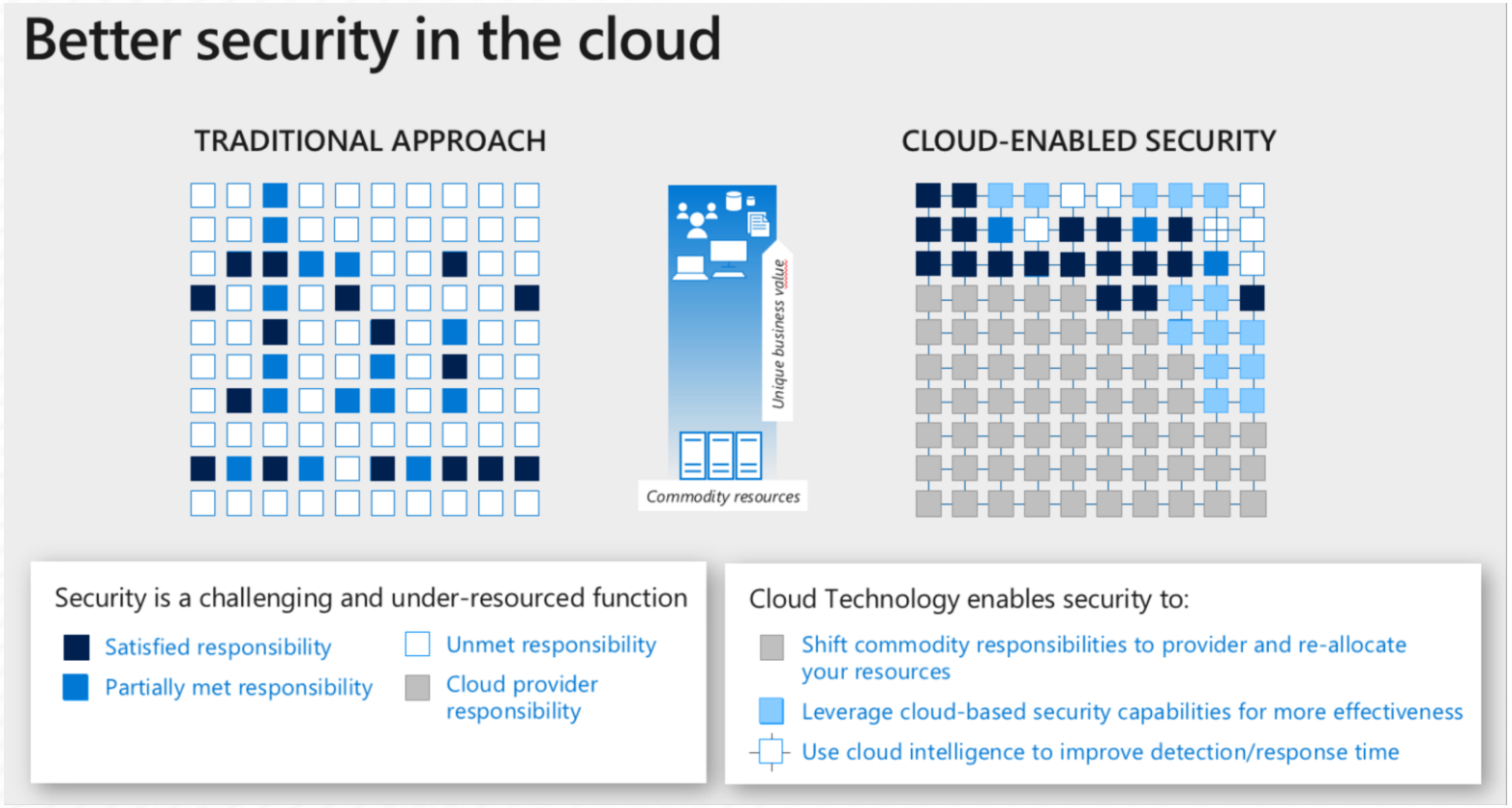
MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Introduction to Security

Foundations for operating in the cloud

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Cloud Security Advantages

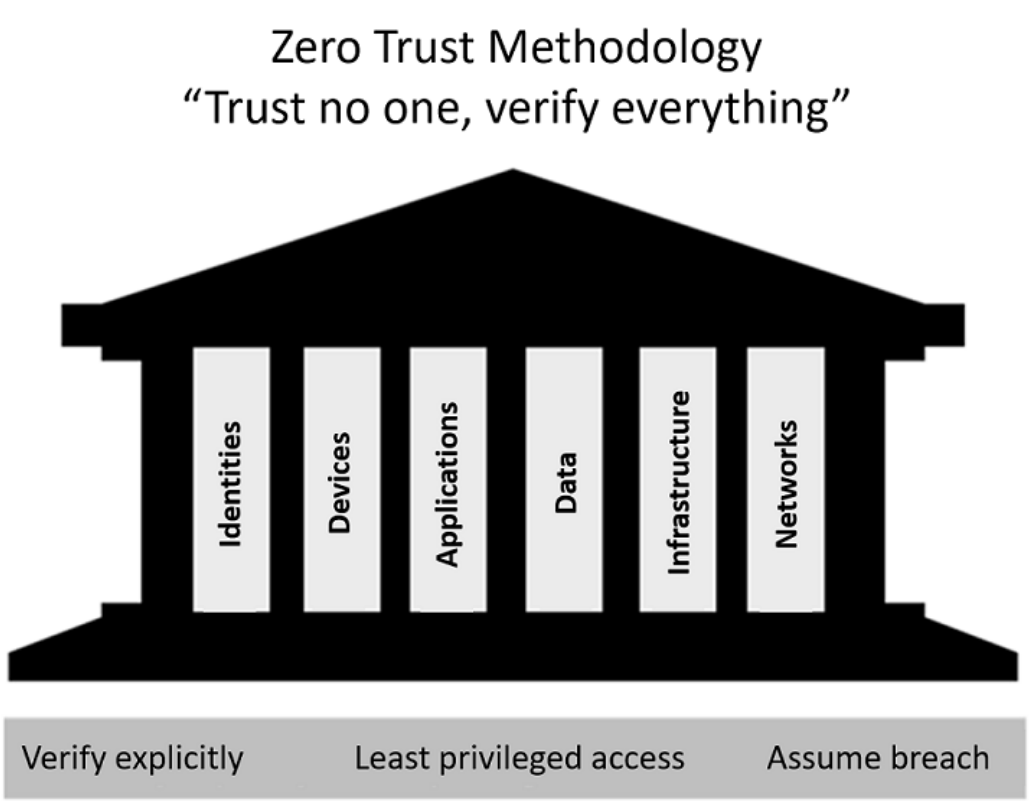


The cloud offers significant advantages for solving long standing information security challenges. In an on-premises environment, organizations likely have unmet responsibilities and limited resources available to invest in security, which creates an environment where attackers can exploit vulnerabilities at all layers.

https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Zero Trust Architecture



Microsoft's Zero Trust Architecture (ZTA) Guiding Principles:

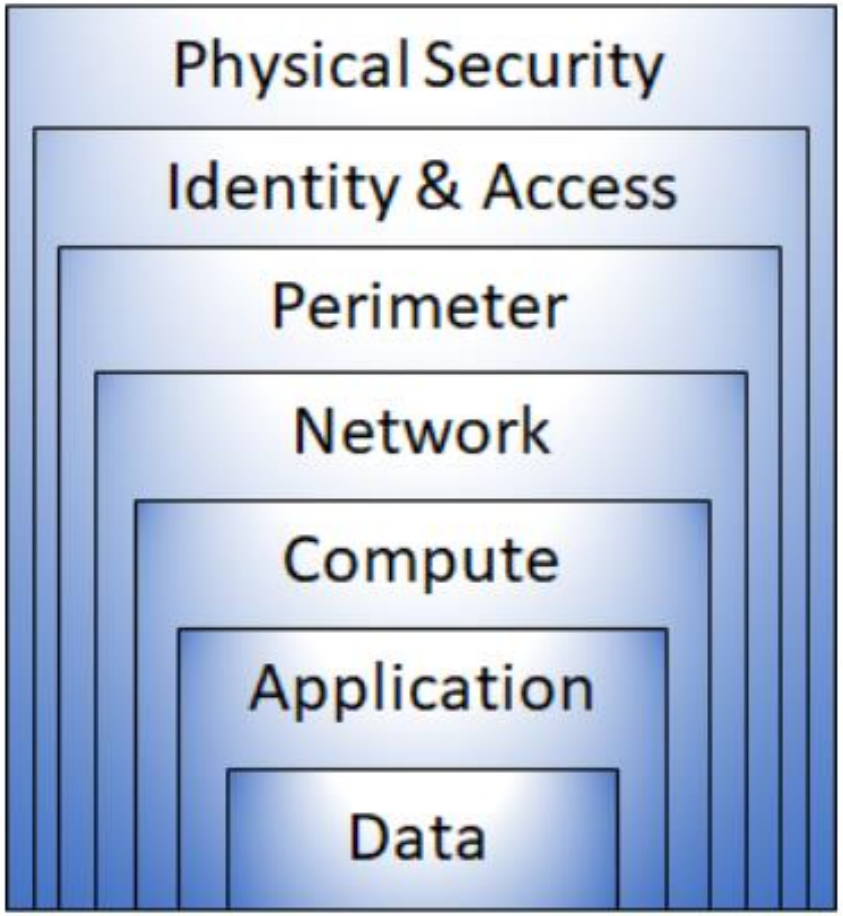
1. **Verify explicitly -** Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.
2. **Least privileged access -** Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
3. **Assume breach** - Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

https://docs.microsoft.com/en-us/learn/modules/describe-security-concepts-methodologies/2-describe-zero-trust-methodology

Defense in Depth

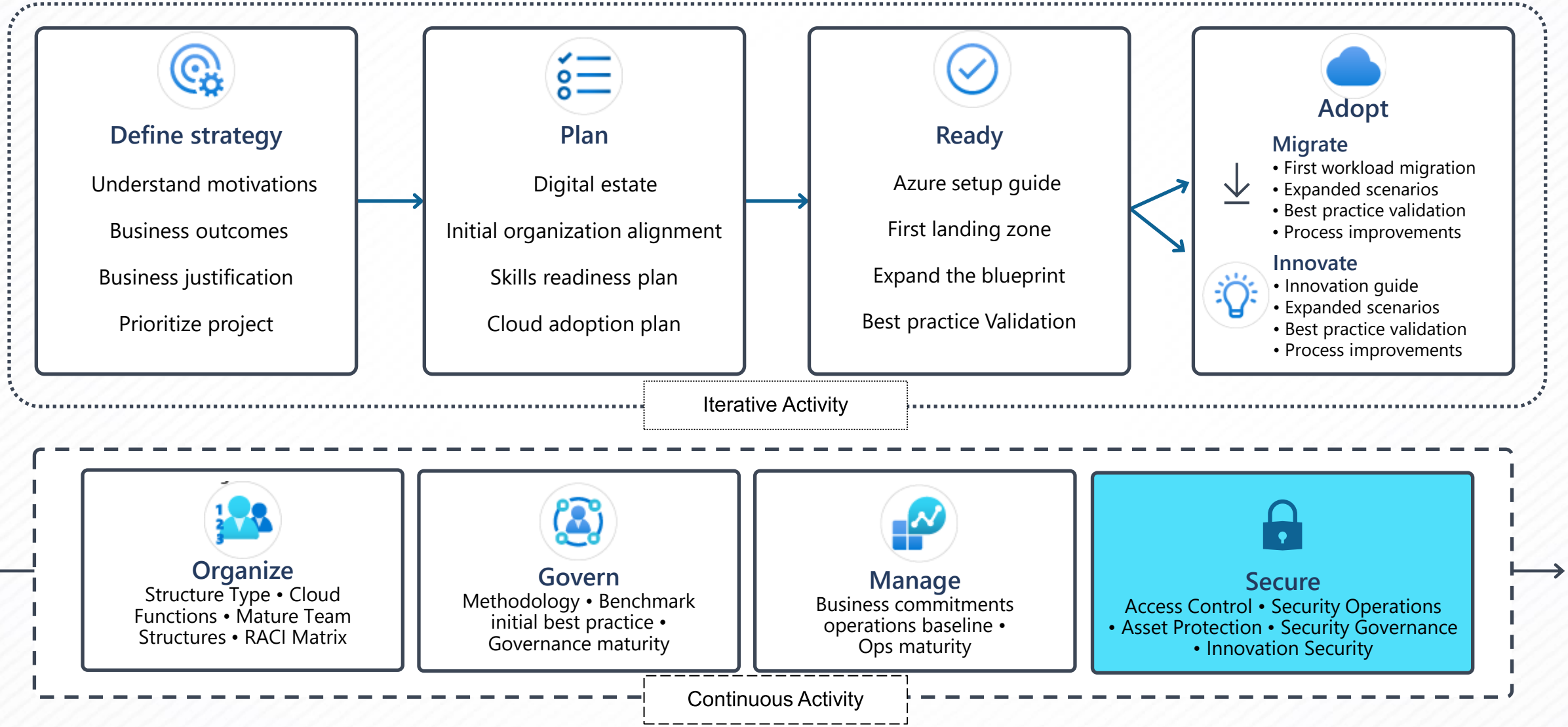
Defense in Depth examples might include:

- **Physical security** such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controls, such as multi-factor authentication or condition-based access, to control access to infrastructure and change control.
- **Perimeter security** including distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network security**, such as network segmentation and network access controls, to limit communication between resources.
- **Compute layer security** such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application layer security** to ensure applications are secure and free of security vulnerabilities.
- **Data layer** security including controls to manage access to business and customer data and encryption to protect data.



https://docs.microsoft.com/en-us/learn/modules/describe-security-concepts-methodologies/4-describe-defense-depth

Microsoft Cloud Adoption Framework for Azure



https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/

CAF Secure Alignment

Business	Platform	Workload

Define strategy
Understand motivations
Business outcomes
Business justification
Prioritize project

Plan
Digital estate
Initial organization alignment
Skills readiness plan
Cloud adoption plan

Organize
Structure Type • Cloud Functions • Mature Team Structures • RACI Matrix

Ready
Azure setup guide
First landing zone
Expand the blueprint
Best practice Validation

Govern
Methodology • Benchmark initial best practice • Governance maturity

Adopt

Migrate
- First workload migration
- Expanded scenarios
- Best practice validation
- Process improvements

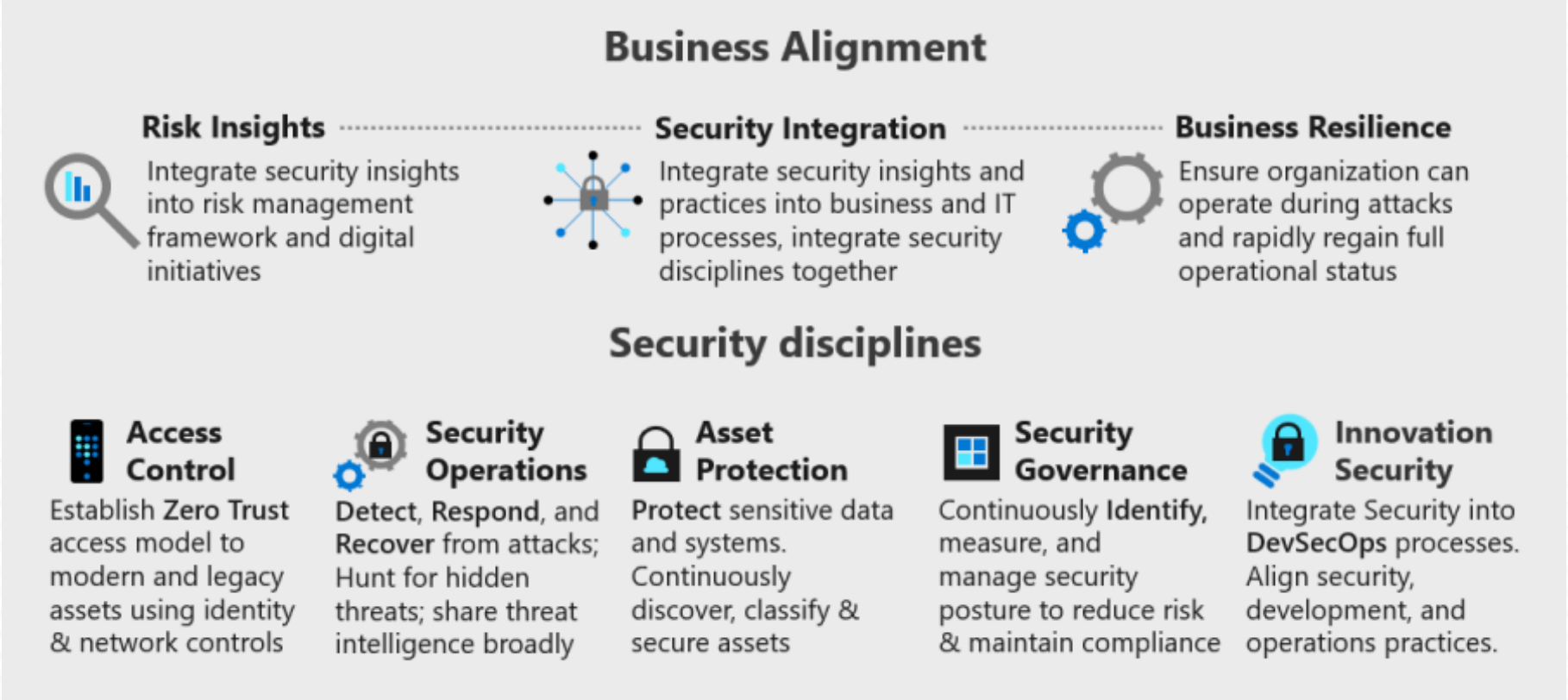
Innovate
- Innovation guide
- Expanded scenarios
- Best practice validation
- Process improvements

Manage
Business commitments operations baseline • Ops maturity

Secure
Access Control • Security Operations • Asset Protection • Security Governance • Innovation Security

Envision a Security End State

The Secure methodology provides a vision of the complete end state to guide the improvement of your security program over time. The following infographic provides a visual mapping of the key ways that security integrates with the larger organization and the disciplines within security.



https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/

Feature Availability for US Government Clouds

Azure Government uses the same underlying technologies as Azure (sometimes referred to as Azure Commercial or Azure Public), which includes the core components of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Both Azure and Azure Government have comprehensive security controls in place, and the Microsoft commitment on the safeguarding of customer data.

Azure Government is a physically isolated cloud environment dedicated to US federal, state, local, and tribal governments, and their partners. Whereas both cloud environments are assessed and authorized at the FedRAMP High impact level, Azure Government provides an extra layer of protection to customers through contractual commitments regarding storage of customer data in the United States and limiting potential access to systems processing customer data to screened US persons. These commitments may be of interest to customers using the cloud to store or process data subject to US export control regulations such as the EAR, ITAR, and DoE 10 CFR Part 810.

https://docs.microsoft.com/en-us/azure/security/fundamentals/feature-availability

Cloud Services by Audit Scope

Microsoft Azure cloud environments meet demanding US government compliance requirements that produce formal authorizations, including:

- Federal Risk and Authorization Management Program (FedRAMP)
- Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Impact Level (IL) 2, 4, 5, and 6
- Intelligence Community Directive (ICD) 503
- Joint Special Access Program (SAP) Implementation Guide (JSIG)

Azure (also known as Azure Commercial, Azure Public, or Azure Global) maintains the following authorizations:

- FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB)
- DoD IL2 Provisional Authorization (PA) issued by the Defense Information Systems Agency (DISA)

Azure Government maintains the following authorizations that pertain to Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia:

- FedRAMP High P-ATO issued by the JAB
- DoD IL2 PA issued by DISA
- DoD IL4 PA issued by DISA
- DoD IL5 PA issued by DISA

Azure Government Secret maintains:

- DoD IL6 PA issued by DISA
- ICD 503 ATO with facilities at ICD 705 (for authorization details, contact your Microsoft account representative)
- JSIG PL3 ATO (for authorization details, contact your Microsoft account representative)

Azure Government Top Secret maintains:

- ICD 503 ATO with facilities at ICD 705 (for authorization details, contact your Microsoft account representative)
- JSIG PL3 ATO (for authorization details, contact your Microsoft account representative)

For current Azure Government regions and available services, see Products available by region

https://docs.microsoft.com/en-us/azure/azure-government/compliance/azure-services-in-fedramp-auditscope

Fulfill Your Security Responsibilities

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Division of Responsibility

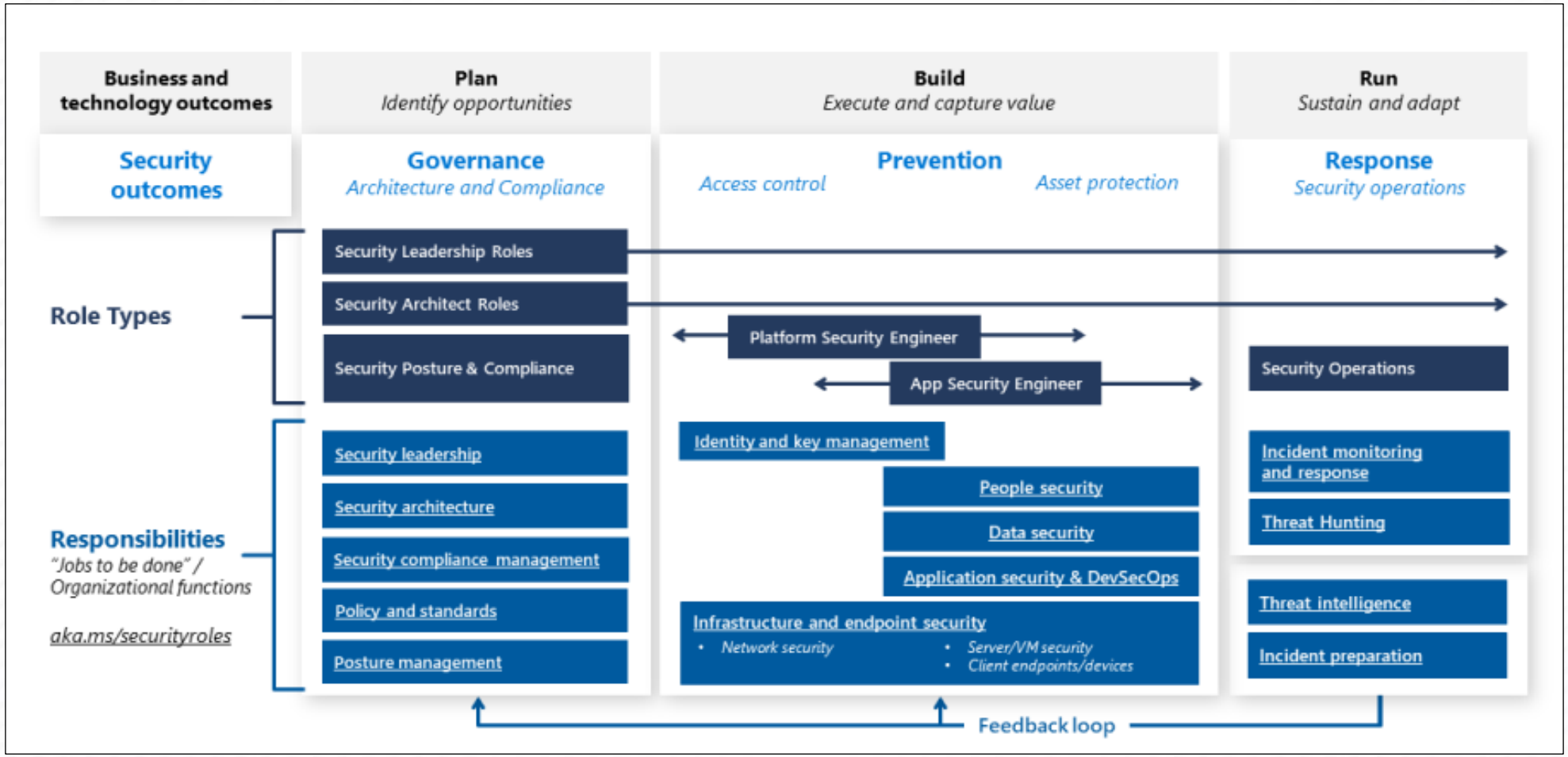
Regardless of the type of deployment, the following responsibilities are always retained by you:

- Data
- Endpoints
- Account
- Access management

https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Mapping Roles and Responsibilities

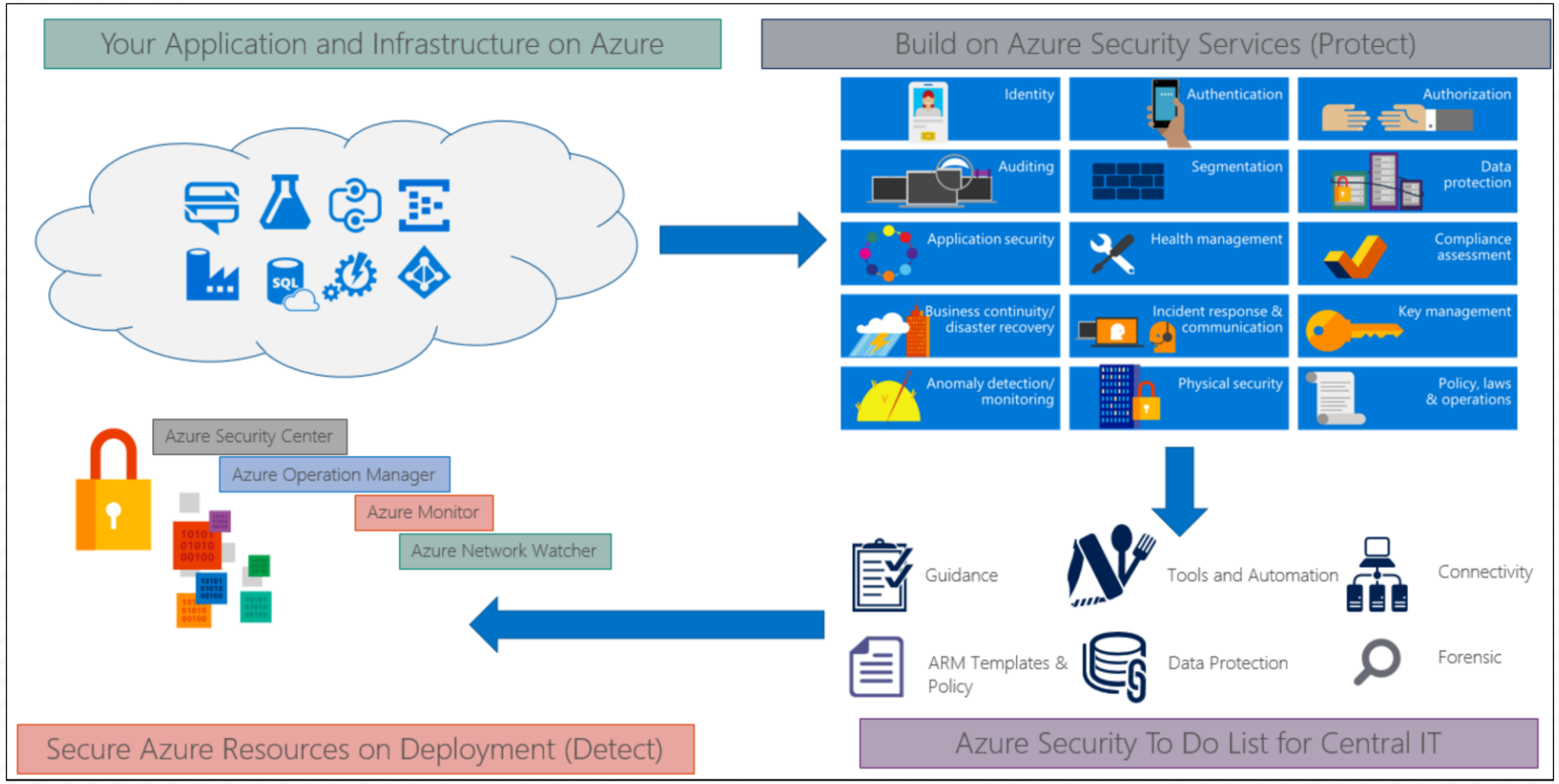
While security is a highly technical discipline, it's first and foremost a human discipline reflective of the long history of human conflict (but updated for computers and the internet).



https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/organize/cloud-security

Security Technical Capabilities

Microsoft Azure provides services that help you meet your security, privacy, and compliance needs.



https://docs.microsoft.com/en-us/azure/security/fundamentals/technical-capabilities

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

IaaS Security

In most infrastructure as a service (IaaS) scenarios, Azure virtual machines (VMs) are the main workload for organizations that use cloud computing. This fact is evident in hybrid scenarios where organizations want to slowly migrate workloads to the cloud.

In such scenarios, follow the general security considerations for IaaS, and apply security best practices to all your VMs.

1. Protect VMs by using authentication and access control
2. Use multiple VMs for better availability
3. Protect against malware
4. Manage your VM updates
5. Manage your VM security posture
6. Monitor VM performance
7. Encrypt your virtual hard disk files
8. Restrict direct internet connectivity

https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

Deploy STIG-compliant Windows VMs

Microsoft Azure Security Technical Implementation Guides (STIGs) solution templates are currently IN PREVIEW and help you accelerate your DoD STIG compliance by delivering an automated solution to deploy virtual machines and apply STIGs through the Azure portal.

This quickstart shows how to deploy a STIG-compliant Windows virtual machine (Preview) on Azure or Azure Government using the corresponding portal.

1. Prerequisites
2. Sign in to Azure
3. Create a STIG-compliant virtual machine
4. High availability and resiliency
5. Business continuity and disaster recovery (BCDR)
6. Clean up resources
7. Support

https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-stig-windows-vm

Identity Management

Security principals (identities) may include services, applications, users, groups, etc. Microsoft identity and access management solutions help IT protect access to applications and resources across the corporate datacenter and into the cloud. Such protection enables additional levels of validation, such as Multi-Factor Authentication and Conditional Access policies. Monitoring suspicious activity through advanced security reporting, auditing, and alerting helps mitigate potential security issues.

Azure Active Directory Premium provides single sign-on (SSO) to thousands of cloud software as a service (SaaS) apps and access to web apps that you run on-premises.

Azure identity management and access control security best practices include:

1. Treat identity as the primary security perimeter
2. Enable single sign-on
3. Turn on Conditional Access
4. Plan for routine security improvements
5. Enable password management
6. Enforce multi-factor verification for users
7. Use role-based access control
8. Lower exposure of privileged accounts
9. Actively monitor for suspicious activities
10. Use Azure AD for storage authentication

https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview

Network Security

Azure includes a robust networking infrastructure to support your application and service connectivity requirements. Network connectivity is possible between resources located in Azure, between on-premises and Azure hosted resources, and to and from the internet and Azure.

These best practices are based on a consensus opinion, and Azure platform capabilities and feature sets, as they exist at the time this article was written. Opinions and technologies change over time and this article will be updated on a regular basis to reflect those changes.

1. Use strong network controls
2. Logically segment subnets
3. Adopt a Zero Trust approach
4. Control routing behavior
5. Use virtual network appliances
6. Deploy perimeter networks for security zones
7. Avoid exposure to the internet with dedicated WAN links
8. Optimize uptime and performance
9. Disable RDP/SSH Access to virtual machines
10. Secure your critical Azure service resources to only your virtual networks

https://docs.microsoft.com/en-us/azure/security/fundamentals/network-overview

Azure Service Fabric Security

Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices. Service Fabric also addresses the significant challenges in developing and managing cloud applications. Developers and administrators can avoid complex infrastructure problems and focus on implementing mission-critical, demanding workloads that are scalable, reliable, and manageable.

Recommend the following Azure Service Fabric security best practices:

- Use Azure Resource Manager templates and the Service Fabric PowerShell module to create secure clusters.
- Use X.509 certificates
- Configure security policies
- Implement the Reliable Actors security configuration
- Configure TLS for Azure Service Fabric
- Use network isolation and security with Azure Service Fabric
- Set up Azure Key Vault for security
- Assign users to roles

https://docs.microsoft.com/en-us/azure/security/fundamentals/service-fabric-best-practices

Azure Security Best Practices and Patterns

The best practices are intended to be a resource for IT pros. This might include designers, architects, developers, and testers who build and deploy secure Azure solutions:

- Azure boundary security best practices (Adopt a Zero Trust Approach)
- Azure database security best practices
- Azure data security and encryption best practices
- Azure identity management and access control security best practices
- Azure network security best practices
- Azure operational security best practices
- Azure PaaS Best Practices
- Azure Service Fabric security best practices
- Best practices for Azure VM security
- Implementing a secure hybrid network architecture in Azure
- Internet of Things security best practices
- Securing PaaS databases in Azure
- Securing PaaS web and mobile applications using Azure App Service
- Securing PaaS web and mobile applications using Azure Storage
- Security best practices for IaaS workloads in Azure

https://docs.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

End-to-End Security

Azure Security Benchmark

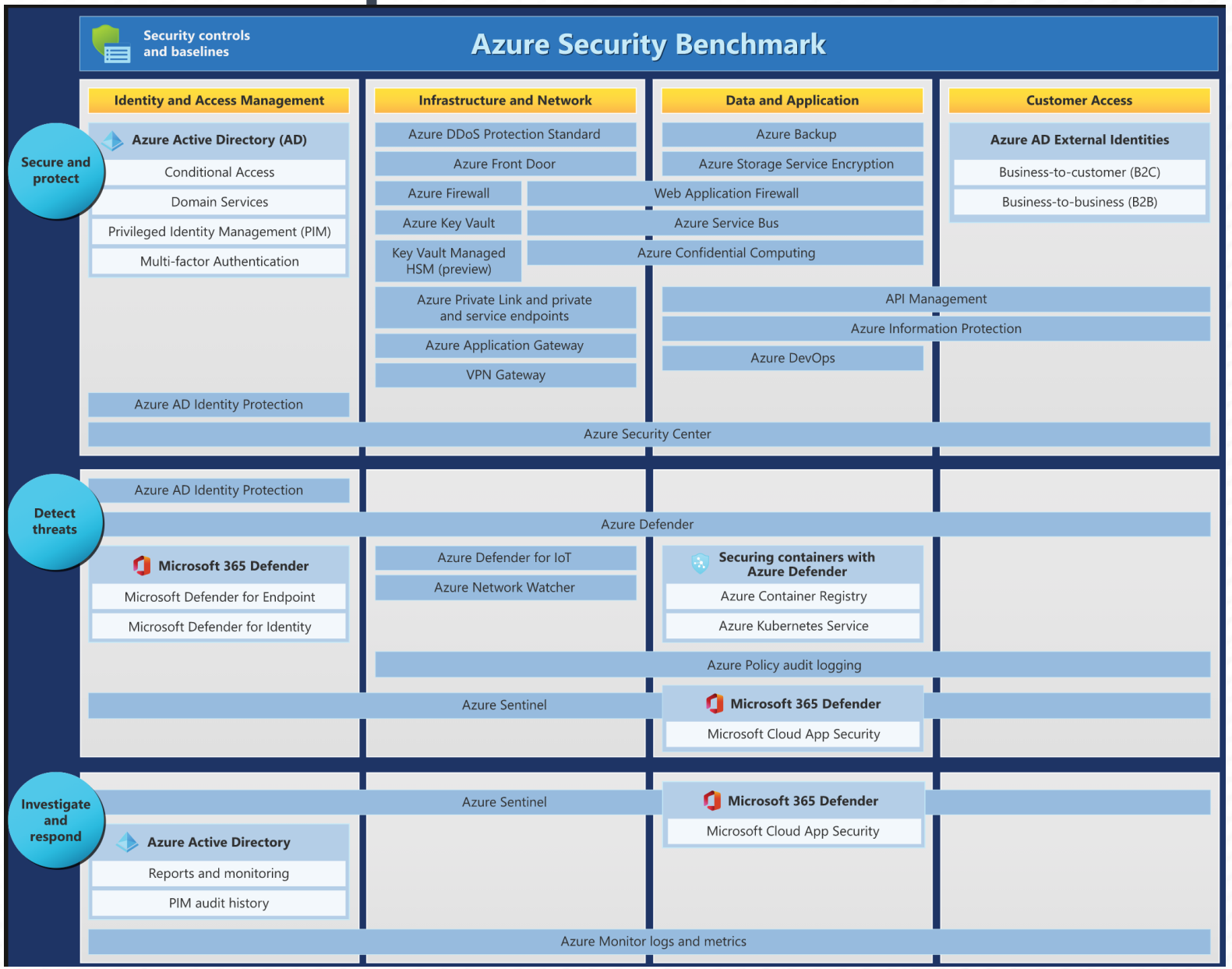
MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Microsoft Security Services Map

The security services map organizes services by the resources they protect (column). The diagram also groups services into the following categories (row):

- **Secure and protect** - Services that let you implement a layered, defense in-depth strategy across identity, hosts, networks, and data. This collection of security services and capabilities provides a way to understand and improve your security posture across your Azure environment.
- **Detect threats** – Services that identify suspicious activities and facilitate mitigating the threat.
- **Investigate and respond** – Services that pull logging data so you can assess a suspicious activity and respond.

https://docs.microsoft.com/en-us/azure/security/fundamentals/end-to-end



The Right Level of Security Friction

Security naturally creates friction that slows down processes, it's critical to identifying which elements are healthy in your DevOps and IT processes and which are not:

- **Healthy friction**: Much like the resistance in exercise makes a muscle stronger, integrating the right level of security friction strengthens the system or application by forcing critical thinking at the right time. This typically takes the form of considering how and why an attacker may try to compromise an application or system during design (known as threat modeling), and reviewing, identifying, and ideally fixing potential vulnerabilities an attacker can exploit in software code, configurations, or operational practices.
- **Unhealthy friction**: Impedes more value than it protects. This often happens when security bugs generated by tools have a high false positive rate (such as false alarms) or when the effort to discover or fix security issues far exceeds the potential impact of an attack.

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/define-security-strategy

Secure Azure Computing Architecture

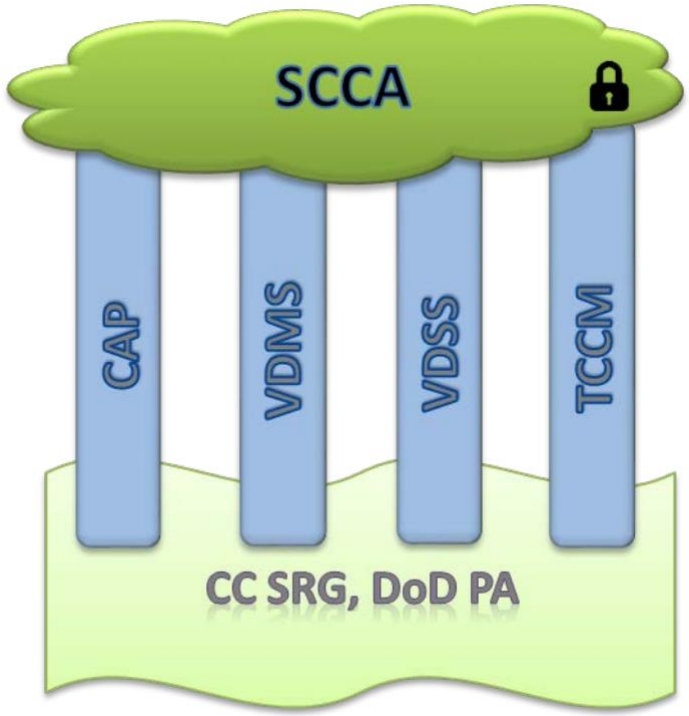
Provided in response to DISA SCCA FRD

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Secure Azure Computing Architecture

US Department of Defense (DoD) customers who deploy workloads to Azure have asked for guidance to set up secure virtual networks and configure the security tools and services that are stipulated by DoD standards and practice.

In 2017, the Defense Information System Agency (DISA) published the Secure Cloud Computing Architecture (SCCA) Functional Requirements Document (FRD). SCCA describes the functional objectives for securing the Defense Information System Network's (DISN) and commercial cloud provider connection points. SCCA also describes how mission owners secure cloud applications at the connection boundary. Every DoD entity that connects to the commercial cloud must follow the guidelines set forth in the SCCA FRD.



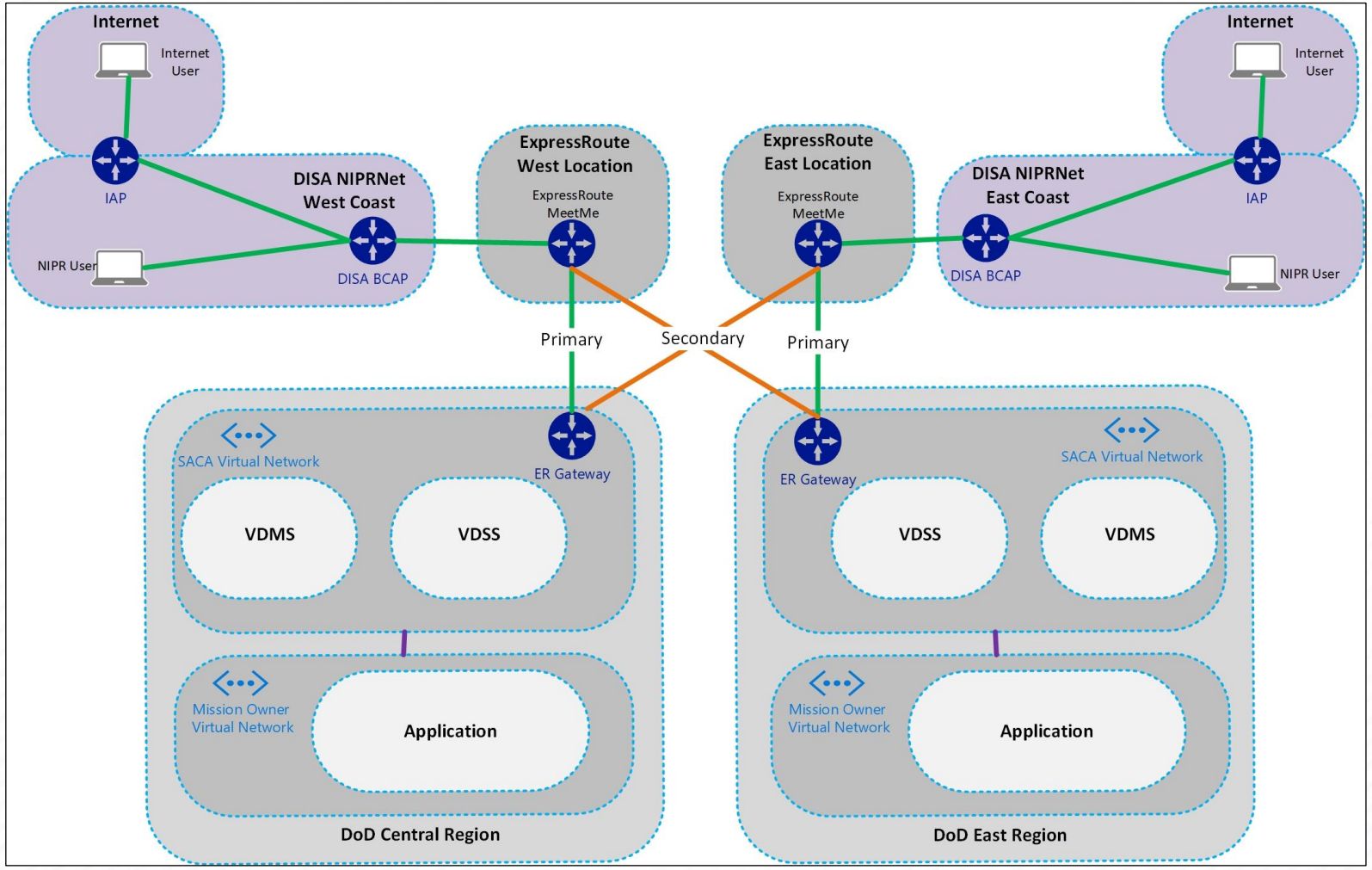
The SCCA has four components:

- Boundary Cloud Access Point (BCAP)
- Virtual Datacenter Security Stack (VDSS)
- Virtual Datacenter Managed Services (VDMS)
- Trusted Cloud Credential Manager (TCCM)

https://docs.microsoft.com/en-us/azure/azure-government/compliance/secure-azure-computing-architecture

Most Common Deployment Scenario

Several Microsoft customers have gone through the full deployment or at least the planning stages of their SACA environments. Their experiences revealed insight into the most common deployment scenario.



Automated SACA Deployment Options

Microsoft has partnered with vendors to create automated SACA infrastructure templates. These templates deploy the following Azure components:

- SACA virtual network
  - VDMS subnet - where VMs and services used for VDMS are deployed, including the jump box VMs.
  - Untrusted, trusted, management, or Azure Firewall Subnet subnets - where virtual appliances or Azure Firewall are deployed.
- Management jump box virtual machines - used for out-of-band management of the environment.
- Network virtual appliances
- Azure Bastion - used to securely connect to VMs over SSL
- Public Ips - for the front end until ExpressRoute is brought online. These IPs translate to the back-end Azure private address space.
- Route tables - applied during automation, these route tables force tunnel all traffic through the virtual appliance via the internal load balancer.
- Azure load balancers - Standard SKU - used to load-balance traffic across the third-party appliances.
- Network security groups - used to control which types of traffic can traverse to certain endpoint

Deployment options:

1. Azure SACA Deployment - For documentation and deployment scripts, see this GitHub link
2. Palo Alto Networks SACA deployment - For documentation and deployment script, see this GitHub link.
3. F5 Networks SACA deployment - For documentation and deployment script, see this GitHub link.
4. Citrix SACA deployment - For documentation and deployment script, see this GitHub link

Conclusion

Resources, Recommendations, and Available Learning

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Additional Resources

- Introduction to Azure security - https://docs.microsoft.com/en-us/azure/security/fundamentals/overview
- Microsoft Security documentation hub - https://docs.microsoft.com/en-us/security/
- Azure Security Benchmark documentation - https://docs.microsoft.com/en-us/security/benchmark/azure/
- What is Azure Security Center? https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction
- Learn about Microsoft's commitment to security in the Azure Data Centers: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure
- Learn about Microsoft's platform security and integrity: https://docs.microsoft.com/en-us/azure/security/fundamentals/platform
- Learn how U.S. government agencies can use security features in Azure cloud services to help achieve compliance with the Trusted Internet Connections (TIC) initiative - https://docs.microsoft.com/en-us/azure/azure-government/compliance/compliance-tic
- The white paper Security best practices for Azure solutions is a (April 2019) collection of the security best practices.
- Microsoft Zero Trust Architecture - https://www.microsoft.com/en-us/security/business/zero-trust
- NIST SP 800-207 Zero Trust Architecture publication - https://csrc.nist.gov/publications/detail/sp/800-207/final
- Microsoft Cloud Adoption Framework Govern Security Baseline discipline - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/security-baseline/
- Security in the Microsoft Cloud Adoption Framework for Azure - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/ The Secure methodology provides a vision of the complete end state to guide the improvement of your security program over time.
- Microsoft Service Trust Portal Home Page
- Azure compliance offerings - https://docs.microsoft.com/en-us/azure/compliance/offerings/
- Azure security baseline for Azure Active Directory - https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/aad-security-baseline?toc=/azure/active-directory/fundamentals/toc.json
- DevSecOps Info - https://www.microsoft.com/en-us/securityengineering/devsecops
- DoD DevSecOps Reference - https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
- Microsoft SACA - https://docs.microsoft.com/en-us/azure/azure-government/compliance/secure-azure-computing-architecture
- CISO cloud readiness guide & Security Baseline Discipline in CAF - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/policy-compliance/cloud-security-readiness

Recommendations

1. Review the Security design principles of the Well-Architected Framework - https://docs.microsoft.com/en-us/azure/architecture/framework/security/security-principles Application of these principles will dramatically increase the likelihood your security architecture will maintain assurances of confidentiality, integrity, and availability.
2. Provide CISO with cloud readiness guide & Security Baseline Discipline in CAF - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/policy-compliance/cloud-security-readiness
3. Review the Methodology, Best Practices, and Considerations in the CAF Secure section - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/
4. In particular:
   a) The Getting Started guide - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/security This guide outlines the key steps that will mitigate or avoid the business risk from cybersecurity attacks. It can help you rapidly establish essential security practices in the cloud and integrate security into your cloud adoption process.
   b) Azure security best practices - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-top-10 The top Azure security best practices that Microsoft recommends based on lessons learned across customers and our own environments.
5. Bookmark and share Microsoft security documentation - Security documentation | Microsoft Docs Review frequently for updates and additional insights

Security Learning Availability

BASIC

- Azure Fundamentals part 4: Describe general security and network security features - https://docs.microsoft.com/en-us/learn/paths/az-900-describe-general-security-network-security-features/(one of six learning paths for Azure Fundamentals)
- LinkedIn Learning Course Microsoft Azure: Security Concepts (1:09 total time)

INTERMEDIATE

- Exam AZ-900: Microsoft Azure Fundamentals - https://docs.microsoft.com/en-us/learn/certifications/exams/az-900
- Exam MS-900: Microsoft 365 Fundamentals - https://docs.microsoft.com/en-us/learn/certifications/exams/ms-900
- Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals - https://docs.microsoft.com/en-us/learn/certifications/exams/sc-900

ADVANCED

- Fundamentals of network security Learning Module https://docs.microsoft.com/en-us/learn/modules/network-fundamentals-2/ (part of AZ-104: Prerequisites for Azure administrators - Learn | Microsoft Docs)
- Manage security operations in Azure Learning Path - https://docs.microsoft.com/en-us/learn/paths/manage-security-operations/
- Threat Modeling Security Fundamentals Learning Path - https://docs.microsoft.com/en-us/learn/paths/tm-threat-modeling-fundamentals/
- Microsoft Certified: Azure Security Engineer Associate (Certification AZ-500) - https://docs.microsoft.com/en-us/learn/certifications/azure-security-engineer/

- Introduction to:
  - Zero Trust Architecture
  - Defense in Depth
  - Microsoft Cloud Adoption Framework (CAF) Secure
- Fulfill Your Security Responsibility
- Azure Security Benchmark
- SACA [Optional]
- Resources, Recommendations, & Learning availability

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM


THANK YOU!