

**WVD CAF Governance  
Security Policy Guidelines**

Table of Contents

[**1.** **Govern - Identity Baseline** 3](#_Toc42195163)

[1.1 Hybrid Identity 3](#_Toc42195164)

[1.2 Identity Requirements 4](#_Toc42195165)

[**2.** **Govern - Security Baseline** 4](#_Toc42195166)

[2.1 Compliance and risk 4](#_Toc42195167)

[2.2 Data Encryption 5](#_Toc42195168)

[2.3 Data Security - Encryption 5](#_Toc42195169)

[2.4 DDoS Protection 6](#_Toc42195170)

[2.5 Deployment Acceleration 6](#_Toc42195171)

[2.6 Hybrid Network Security/Identity 6](#_Toc42195172)

[2.7 Infrastructure Security 7](#_Toc42195173)

[2.8 Monitoring Alert, Audit/Diagnostic Logs and alerting 7](#_Toc42195174)

[2.9 Network Security 7](#_Toc42195175)

[2.10 Network Security - Internet connectivity Paths 8](#_Toc42195176)

[2.11 Network Security - Software defined networking models 9](#_Toc42195177)

[2.12 Resource Consistency 9](#_Toc42195178)

[**3.** **Govern - Security Baseline** 9](#_Toc42195179)

[3.1 Identity 9](#_Toc42195180)

[3.2 Information Protection 10](#_Toc42195181)

[3.3 Monitoring 10](#_Toc42195182)

[3.4 Threat Protection 11](#_Toc42195183)

[**4.** **Governance – Resource Consistency** 12](#_Toc42195184)

[4.1 Asset Classification 12](#_Toc42195185)

[4.2 Service Discoverability and Shadow IT 12](#_Toc42195186)

[4.3 Service Disturbance 12](#_Toc42195187)

**WVD Governance Security Policy Guidelines**

# **Govern - Identity Baseline**

## Hybrid Identity

In any environment, to improve access to solutions that span on-prem and cloud-based capabilities and platforms, an organization needs to create a common user identity that can be used for authentication and authorization to all such resources, including those on-prem and those in the cloud. This is called hybrid identity.

* **Azure ad connects**: The Azure AD Connect tool allows you to connect Azure AD instances with your existing identity management solutions, allowing synchronization of your existing directory in the cloud.
* **Password policy (Passthrough, password hash, Federation)**:
* **Password hash synchronization**: It is a sign-in method that is used as part of a hybrid identity solution. To accomplish a hybrid identity solution with PHS, a hash of user’s on-prem Active Directory (AD) password is synchronized to a cloud-based Azure AD instance. This feature is typically used for signing into Azure services such as Office 365 with the same password as an on-prem AD account. This is a preferable solution for end users because it creates a pleasant end user experience.
* **Pass-through Authentication**: Azure AD Pass-through Authentication allows users to sign in to on-prem apps as well as cloud-based apps, using the same password. However, pass-through authentication validates user passwords directly against the on-premises Active Directory.
* **Federation**: It consists of a collection of domains with an established trust. The trust typically includes authentication and almost always includes authorization. A typical federation configuration would include several organizations that have established trust for shared access to a set of resources.
* **SAS (azure shared access signature)**:

SAS is a URI (Uniform Resource Identifier). Instead of providing your storage access keys to authorized users, you can provide the SAS URIs to access the storage resources. As it is not recommended to share the storage access keys, it would be much easier to generate a SAS token and embed within your application for accessing the storage resources. With SAS, you can set a start time, expiry date, permitted permissions, allowed IP addresses, etc.

## Identity Requirements

Azure AD enables you to govern employee and business partner access to resources at enterprise scale with great compliance and auditing controls. Azure AD entitlement management removes barriers to internal and external collaboration by automating employee and partner access requests, approvals, auditing, and review for Office 365, for thousands of popular SaaS apps like ServiceNow, Workday, Google Apps, and Salesforce.com to any line of business app integrated with Azure AD.

* **Conditional access policy (MFA, failed login)**: Conditional Access policies by default apply to browser-based applications and applications that utilize modern authentication protocols. In addition to these applications, administrators can choose to include Exchange ActiveSync clients and other clients that utilize legacy protocols. To know about conditional access policy [click here](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions).
* **Configure MFA**: People are connecting to organizational resources in increasingly complicated scenarios. People connect from organization-owned, personal, and public devices on and off the corporate network using smart phones, tablets, PCs, and laptops, often on multiple platforms. To know about MFA [click here](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted)
* **Creation of authentication and authorization Policy (application identity, Shared Credentials, RBAC, MS365 App Security)** :
* **Authentication**: Authentication is the process of proving you are who you say you are. Authentication is sometimes shortened to AuthN. Microsoft identity platform implements the OpenID Connect protocol for handling authentication.
* **Authorization**: Authorization is the act of granting an authenticated party permission to do something. It specifies what data you're allowed to access and what you can do with that data. Authorization is sometimes shortened to AuthZ. Microsoft identity platform implements the OAuth 2.0 protocol for handling authorization. To know about authentication and authorization [click here](https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-vs-authorization)

# **Govern - Security Baseline**

## Compliance and risk

* **Compliance manager configuration, reporting, risk mitigation**: Compliance Manager uses several components to help you with your compliance management activities. These components work together to provide a complete management workflow and hassle-free compliance reports for auditors.
* **Policy and Industry Standard controls configuration**: Azure Security Center continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance controls and requirements. To know about policy and Industry Standard controls configuration [click here](https://docs.microsoft.com/en-us/azure/security-center/update-regulatory-compliance-packages)
* **Security Assessment - Secure score configuration**: Security Center continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level. Use the score to track security efforts and projects in your organization. To know about Security Assessment - Secure score configuration [click here](https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls)

## Data Encryption

* **Data at rest encryption is performed on the Azure platform**: Encryption at Rest is the encoding (encryption) of data when it is persisted. The Encryption at Rest designs in Azure use symmetric encryption to encrypt and decrypt large amounts of data quickly according to a simple conceptual model. To know about Data Encryption [click here](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest)

## Data Security - Encryption

**Azure Key Vault**: Azure Key Vault provides a centralized key management solution that offers a consistent management solution for many cloud-based and even on-premises services that use encryption.

* Configure Bring your own keys configuration per policy (BYOK)
* Configure HSM per company standard and policy
* Configure Key rotation policy
* configure internal/External CA per company standard and policy
* Key management policies
* Configuring customer-managed encryption keys for Azure Storage – Always encrypted

**Data at rest**: Encryption at Rest is a common security requirement. In Azure, organizations can encrypt data at rest without the risk or cost of a custom key management solution. Organizations have the option of letting Azure completely manage Encryption at Rest.

* Configure Encrypting - VM Disks (Windows and Linux VMs Bit locker/DM Crypt
* Configure Encrypting -Azure storage encryption
* Configure Encrypting SQL DB - TDE
* Configure Encrypting SQL DB -SQL Always Encrypted

**Encrypting data in use**: Azure Confidential computing for multi-tenant scenario

**Encryption data in transit**:

* Azure App Service - https://. azurewebsites.net - Custom domains and certificates
* Azure portal uses HTTPS
* Azure Storage REST endpoints - HTTPS is optional - SAS can enforce HTTPS
* Encryption of all public endpoints - VPN, Express routes encryption
* Security center alerts configuration

Security documents and emails: Azure information Protection (labeling and classification)

## DDoS Protection

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns facing customers that are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

* **Use Azure DDoS Protection Standard to minimize disruptions caused by DDoS attacks.** [Click here](https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview)

## Deployment Acceleration

Deploying Azure Information Protection from a technical standpoint is a fairly simple task. Where it becomes challenging is when you begin looking at the business requirements that must be in place prior to deployment of AIP.

* All assets deployed to the cloud should be deployed using templates or automation Scripts, where possible
* Azure Blueprints
* Azure DevOps Pipelines

## Hybrid Network Security/Identity

Redirect cloud authentication through on-premise firewall (if Azure AD connect environment is in place) i.e. Route and NSG configurations

## Infrastructure Security

* + - **Develop an Azure Blueprint**: Create and assign blueprints, you can define common patterns to develop reusable and rapidly deployable configurations based on Azure Resource Manager templates, policy, security, and more. In this tutorial, you learn to use Azure Blueprints to do some of the common tasks related to creating, publishing, and assigning a blueprint within your organization. To develop an azure blueprint [click here](https://docs.microsoft.com/en-in/azure/governance/blueprints/create-blueprint-portal)
    - **Naming conventions and tags**: Organize your cloud assets to support operational management and accounting requirements. Well-defined naming and metadata tagging conventions help to quickly locate and manage resources. [Click here](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging)
    - **Role-based access control model**: Access management for cloud resources is a critical function for any organization that is using the cloud. Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. [Click here](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview)
    - **Set up security and monitoring**: Azure security features and services that Azure provides to aid in the management and monitoring of Azure cloud services and virtual machines. [Click here](https://docs.microsoft.com/en-us/azure/security/fundamentals/management-monitoring-overview)

## Monitoring Alert, Audit/Diagnostic Logs and alerting

* **Azure Security Centre - Security Policy configuration**: A security policy defines the desired configuration of your workloads and helps ensure you are complying with the security requirements of your company or regulators. [Click here](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy)

## Network Security

* **Application Gateway**: Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. [Click here](https://docs.microsoft.com/en-us/azure/application-gateway/overview)
* **Creating user defined routes (UDR):** You can create custom, or user-defined(static), routes in Azure to override Azure's default system routes, or to add additional routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it. [Click here](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#user-defined)
* **DDoS configuration for internet endpoints**: DDoS is a type of attack that tries to exhaust application resources. The goal is to affect the application’s availability and its ability to handle legitimate requests. Attacks are becoming more sophisticated and larger in size and impact. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. [Click here](https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices#azure-offerings-for-ddos-protection)
* **Network access controls with NSGs and Azure Firewall**: NSGs and Azure Firewall work very well together and are not mutually exclusive or redundant. You typically want to use NSGs when you are protecting network traffic in or out of a subnet. An example would be a subnet that contains VMs that require RDP access (TCP over 3389) from a Jumpbox. Azure Firewall is the solution for filtering traffic to a VNet from the outside. For this reason, it should be deployed in it’s own VNet and isolated from other resources. Azure Firewall is a highly available solution that automatically scales based on its workload.
* **Network monitoring and threat detection:** Azure offers built in advanced threat detection functionality through services such as Azure Active Directory (Azure AD), Azure Monitor logs, and Azure Security Center. This collection of security services and capabilities provides a simple and fast way to understand what is happening within your Azure deployments. [Click here](https://docs.microsoft.com/en-us/azure/security/fundamentals/threat-detection)
* **Policy templates for networking**: Policy templates for networking [click here](https://docs.microsoft.com/en-us/azure/virtual-network/policy-samples#azure-virtual-network)
* **The hub spoke model**: The hub is a virtual network in Azure that acts as a central point of connectivity to your on-premises network. The spokes are virtual networks that peer with the hub and can be used to isolate workloads. Traffic flows between the on-premises datacenter and the hub through an ExpressRoute or VPN gateway connection. To know about the hub and spoke model [click here](https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke)

## Network Security - Internet connectivity Paths

* + - **Static virtual IP address**: To define and configure a specific internal IP address that can be statically assigned to an IaaS Virtual Machine deployed in a Virtual Network. To know about static virtual IP address [click here](https://azure.microsoft.com/en-us/blog/static-internal-ip-address-for-virtual-machines/)
    - **Web Application Firewall**: Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. To know about Web Application Firewall [click here](https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview)
    - **Web traffic load balancer**: Load balancing provides a higher level of availability and scale by spreading incoming requests across multiple virtual machines. In this tutorial, you learn about the different components of the Azure Standard Load Balancer that distribute internet traffic to VMs and provide high availability. To know about Web traffic load balancer [click here](https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-manage-portal)

## Network Security - Software defined networking models

* + - **Hybrid - Access to services from cloud to on-prem - Application Proxy**: Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal. [Click here](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy)
    - **Hybrid - Access to services in cloud from on-prem**: You can now protect your on-premises and cloud legacy authentication applications by connecting them to Azure AD with your existing application delivery controller or network. [Click here](https://docs.microsoft.com/en-in/azure/active-directory/manage-apps/secure-hybrid-access)
    - Infrastructure as a Service resources - NSGs, Monitoring agent, encryption configuration

## Resource Consistency

Cloud Adoption Framework outlines how to develop a Resource Consistency discipline as part of your cloud governance strategy. The primary audience for this guidance is your organization's cloud architects and other members of your cloud governance team.

* + - Develop resource template - ARM
    - Discoverable to IT operations - Tag, alerts based on tags for non-compliant resource
    - Included in recovery planning
    - Part of repeatable operations processes

# **Govern - Security Baseline**

## Identity

Identity is increasingly considered the primary security perimeter in the cloud, which is a shift from the traditional focus on network security. Identity services provide the core mechanisms supporting access control and organization within IT environments, and the Identity Baseline discipline complements the Security Baseline discipline by consistently applying authentication and authorization requirements across cloud adoption efforts. To know about identity security baseline [click here](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/identity-baseline/). Please follow below identities and configure the policies.

* Ensure admin accounts are not licensed
* Ensure all admin accounts are enabled for multi-factor authentication (MFA)
* Ensure no service accounts are assigned admin role in the tenant
* Ensure on-premise synchronized accounts are not assigned admin roles in the Tenant
* Implement a process for disabling and deleting accounts that are no longer used
* Implement Azure Active Directory (Azure AD) Privileged Identity Management
* Implement privileged access management in Office 365
* Reduce the number of global administrator accounts to less than five
* Require multi-factor authentication for all users
* Review and optimize your conditional access and related policies to align with your objectives for a zero-trust network.
* Setup multi-factor authentication and use recommended conditional access policies, including sign-in risk policies
* Implement Privileged Access Workstations (PAW)

## Information Protection

Azure Information Protection (sometimes referred to as AIP) is a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. To know about information protection, [click here](https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection). Please follow below identities and configure the policies.

* Configure data loss prevention policies for sensitive data
* Disable Anonymous external calendar sharing policy
* Disable external email forwarding
* Implement data classification and information protection policies
* Protect data in third-party apps and services by using Cloud App Security
* Use AIP Scanner to identify and classify information across servers and file shares
* Use Microsoft Defender ATP to identify if users store sensitive information on their desktops

## Monitoring

To enable Azure Monitor for VMs on your virtual machines to monitor health and performance. Discover application dependencies that run on Azure virtual machines (VMs) and virtual machine scale sets, on-premises VMs, or VMs hosted in another cloud environment. To know about information protection, [click here](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-overview). Please follow below identities and configure the policies.

* Ensure the Office 365 audit log is turned on
* Review risky logins weekly
* Review Secure Score weekly
* Review Top malware, spam users weekly
* Use Microsoft Azure Sentinel or your current SIEM tool to monitor for threats across your environment.
* Use Microsoft Cloud App Security to detect unusual behavior across cloud apps
* Use Microsoft Defender ATP
* Use Office 365 ATP tools
* Use the Azure Security Center to monitor for threats across hybrid and cloud workloads.

## Threat Protection

When Security Center detects a threat in any area of your environment, it generates an alert. These alerts describe details of the affected resources, suggested remediation steps, and in some cases an option to trigger a logic app in response. To know about threat protection [click here](https://docs.microsoft.com/en-us/azure/security-center/threat-protection)

* Block connections from countries that you do not do business with
* Disable POP, IMAP, and SMTP protocols
* Protect against ransomware
* Protect your email from targeted phishing attacks
* Raise the level of protection against malware in mail
* Retire servers and applications that are no longer used in your environment
* Block access to the Microsoft Azure Management portal to all non-administrators
* Configure Defender Advanced Threat Protection capabilities
* Configure Office 365 Advanced Threat Protection (Office ATP)
* Deploy Azure ATP to monitor and protect against threats targeted to your on-premises Active Directory environment.
* Disable Remote PowerShell for all users
* Do not whitelist sender domains, individual senders, or source IPs as this allows these to bypass spam and malware checks
* Enable Outbound spam notifications
* Open Teams Federation only to Partners you communicate with
* Secure partner channel communications like emails using TLS
* Use Microsoft Cloud App Security to discover and monitor SaaS apps

# **Governance – Resource Consistency**

## Asset Classification

**Establish resource tagging standards and ensure IT staff apply them consistently to any deployed resources using Azure resource tags**: You apply tags to your Azure resources, resource groups, and subscriptions to logically organize them into a taxonomy. Each tag consists of a name and a value pair. For example, you can apply the name "Environment" and the value "Production" to all the resources in production.

## Service Discoverability and Shadow IT

Shadow IT helps you know and identify which apps are being used and what your risk level is. 80% of employees use non-sanctioned apps that no one has reviewed and may not be compliant with your security and compliance policies. And because your employees can access your resources and apps from outside your corporate network, it's no longer enough to have rules and policies on your firewalls. Please follow below identities and configure the policies.

* Configure policy for resource tagging

## Service Disturbance

* **Microsoft Cloud services audit report and service alert configuration**: Microsoft cloud services include several auditing and reporting features you can use to track user and administrative activity within their tenant