MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Cloud Governance & Security in the Swiss Public Sector

Version 1.4

Microsoft

Related documents

Document name	
Microsoft Public Sector Cloud Design	
Document: Cloud Governance & Security in the Swiss Public Sector V1.4	
Identification: Governance and Security Guideline Swiss Public Sector_V1.4	
Azure Blueprints for Public Sector (ISO 27001)	Microsoft Docs

Microsoft

Contents

Figures

Disclaimer

This document covers the questions often asked by our customers on the use of cloud computing solutions. It should enable you to better understand the technical and legal contexts involved in the use of a cloud computing solution. This document does not include a specific examination of an individual legal situation. You will have to seek separate legal advice to obtain an individual and definitive legal assessment on the acceptability of the use of Microsoft Cloud solutions specific to your situation.

1 PURPOSE OF THIS DOCUMENT

This document serves as a guide and recommendation to implement and operate a standardized cloud platform environment. It considers the risks identified in Microsoft Public Sector Cloud Design. The ISO 27001 safety standard serves as a reference for the measures and controls.

2 CONTENT AND STRUCTURE

To achieve a standardized landing zone in the Azure public cloud in accordance with ISO 27001, we provide deployment models of the required components and employ control mechanisms. To this end, we first take into account the basic concepts of the components and then the various controls that verify their effectiveness.

Any risk that is identified and removed from Microsoft Public Sector Cloud Design is noted.

3 BASIC PRINCIPLES

The ISO 27001 templates used to deploy the landing zone components are based on Azure Blueprints[1] applied to one or more subscriptions. Resource groups, resources, permissions and policies are created for this purpose.

- ISO 27001[2] → This blueprint includes general strategies to implement metrics on existing or new application resources.
- ISO 27001: Shared services[3] → This blueprint creates the central and shared resources that are required to support landing zone operations, including default permissions.
- ISO 27001: ASE/SQL workloads[4] → This optional blueprint provides one or more standardized, web-based application environments that rely on "App Service" and "SQL DB" PaaS resources.

Reporting on compliance with ISO 27001 controls is done with the assistance of the Microsoft Defender for Cloud, which reports all control discrepancies in the resources of the associated subscriptions. To do this, it applies a compilation of strategies where only the audit result per policy is kept.

3.1 LAYOUT OF THE LANDING ZONE

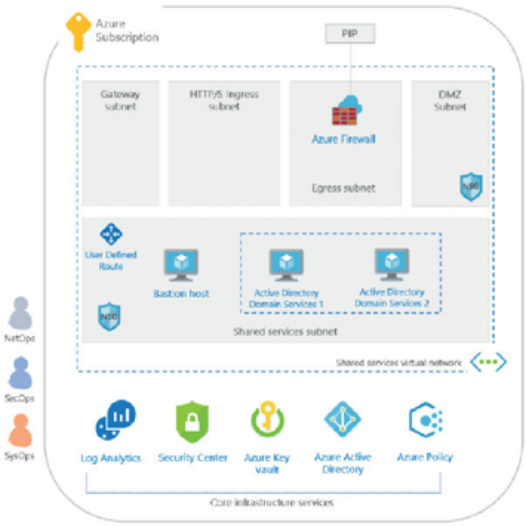


Figure 1 – Blueprint ISO 27001 Shared Services

The landing zone based on ISO 27001 is an architectural approach and an enterprise level implementation. It is used to create and operationalize target zones in Azure at scale. It is aligned with the Azure Roadmap and the Cloud Adoption Framework[5] for Azure.

The architecture provides for a divided central area, which is covered by a subscription, and other areas dedicated to applications (such as ISO 27001: ASE/SQL workloads), which are subject to specific subscriptions. The different components of the central area are described in the following chapters.

Depending on the technical considerations and layout recommendations of this architecture, it is possible to consider different compromises depending on your business scenario. A slight divergence is permissible, but if you follow the basic recommendations, the resulting target architecture will lead your organization along the path of sustainable development.

[1] https://docs.microsoft.com/en-us/azure/governance/blueprints/overview
[2] https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso-27001-2013
[3] https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared
[4] https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-ase-sql-workload
[5] https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/

3.2 ROLES AND ORGANIZATION

Only staff who are competent and authorized to perform the tasks entrusted to them will be able to properly set up a cloud platform that meets the well-defined objectives of the company. To be effective, this operating model must be based on a well-structured organization in which the various responsibilities are attached to predefined roles, which, in turn, are assigned to trained teams and well-identified staff members.

The IT department usually has its own structure that will only need to be adapted to the new circumstances and tasks presented by a cloud platform like Azure. The following cloud functions outline the disciplines that are required to encourage cloud adoption and should be assigned to roles that are well established in the organization.

- Cloud Strategy → Adaptation of new technical conditions to the needs of the company
- Cloud Governance → Detection of business risks and definition of compliance measures
- Cloud Platform Operations → Maintenance and operation of the cloud platform landing zone and its basic services
- Cloud Application Operations → Implementation and operation of migrated applications and new cloud solutions
- Cloud Competence Center → Development, implementation and consulting in the area of new approaches and cloud technologies
- Cloud Automation → Accelerating the adoption of the cloud and its new processes
- Cloud Data → Development and definition of enterprise data flows to and from the cloud, and analytical enrichment of data in the cloud through defined architectures
- Cloud Security → Protection of information and performance of security-related tasks in the cloud

Migration to the cloud generally requires the use of all of these functions and disciplines, but the involvement level of the different roles varies depending on the development stage. The more the adaptation progresses and grows, the more these roles and their responsibilities are defined and should be anchored within a RACI matrix.

3.3 ACCESS CONTROL (RBAC)

Azure's "Role Based Access Control" RBAC enables you to distribute the tasks of managing your organization across different teams and limit access of the different user accounts only to the Azure resources that they need to accomplish their tasks. Rather than granting unlimited access rights to all accounts in your subscription or resources, it is preferable to limit access rights to certain actions of a specific domain (management group; subscription; resource group).

In terms of an access rights policy, experience has shown that it is better to grant users the fewest possible rights for the performance of their tasks. Avoid assigning relatively large roles in broad areas, although this may initially seem more practical. When you create user roles, be sure to include only essential access rights. By restricting roles and domains, you limit the resources that are at risk if a primary security guard is compromised.

The diagram below proposes a nesting of the elements in terms of access rights:

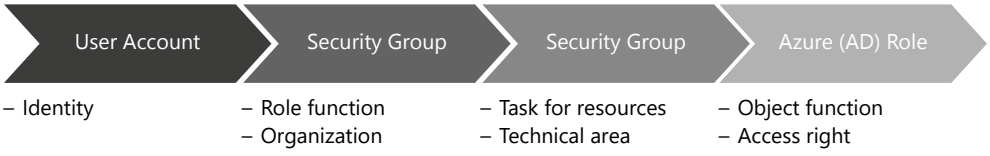
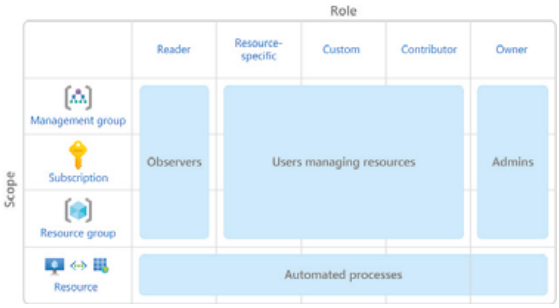


Figure 2 – RBAC nesting



The following diagram shows the possible domains for which a user may obtain access rights through their group assignment.

Figure 3 – Scope of RBAC application

3.4 AZURE ARC

Typically, all computing resources do not migrate to the cloud at once. Some resources may even be migrated to another vendor's data centers for a multi-cloud strategy. For such hybrid and multi-cloud scenarios, Azure Arc offers centralized management options. Customers can then also use the security and compliance offers for resources that are not (or not yet) in Azure.

Use cases and scenarios

– Central visibility across a wide range of resources (Windows, Linux, Kubernetes)

– Organization and inventory of all management group resources, subscriptions, resource groups or tags

– Automation development and configuration management

– Security policy management

– Access management with role-based access control and Azure Lighthouse

– Provisioning of databases (SQL, PostgreSQL) in Kubernetes clusters, whether locally or in another cloud

– Searching across multiple environments using Azure Resource Graph

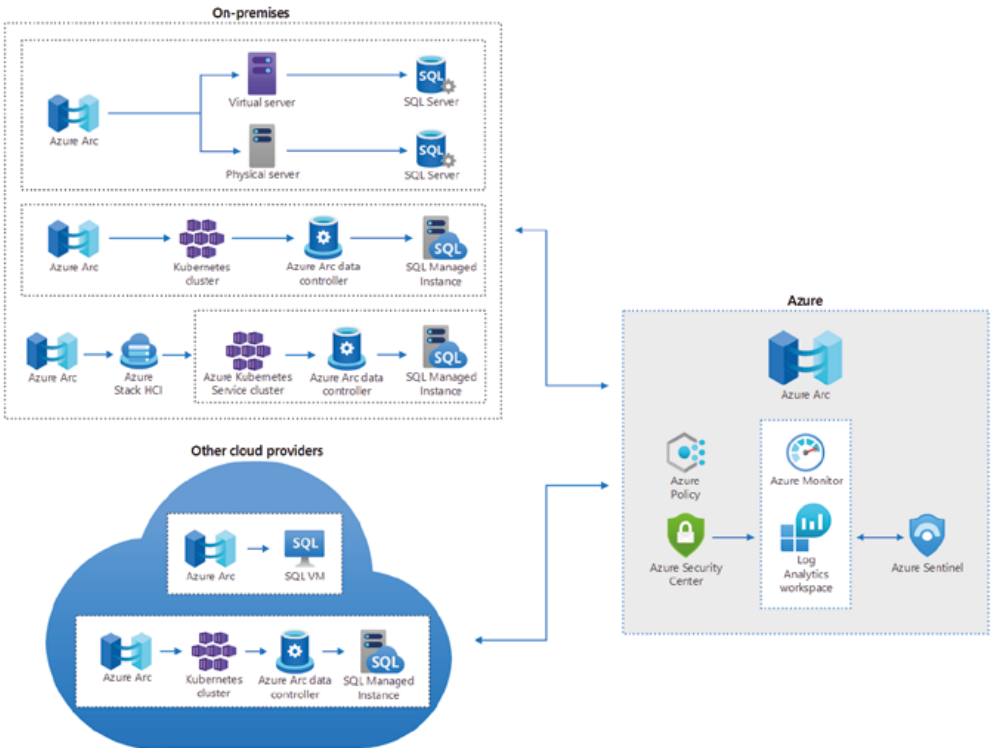


Figure 4 – Overview of the Azure Arc functions

3.5 POLICIES AND SECURITY SETTINGS

Azure Policy helps enforce organizational standards and assess compliance, as needed. Using its compliance dashboard, this service provides an aggregated view to assess the general situation of the environment and to launch an exploration for a granular assessment by resource and policy. It also helps you bring your resources into compliance thanks to the bulk maintenance of existing resources and the automatic maintenance of new resources.

Azure Policy is often used as part of an implementation of governance for resource consistency, regulatory compliance, security, costs and management. The policy definitions for these common use cases are already built into your Azure environment to make getting started easier.

Azure Policy does not necessarily imply a restriction of actions but ensures that the status of resources complies with your company policies, regardless of who made the changes or has permission to do so.

To get an overview of the current status of the policies, Azure Policies overview can be used to provide information on the current status of the policies deployed.

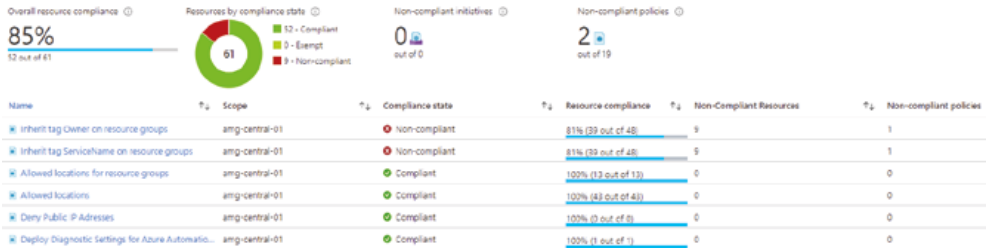


Figure 5 – Compliance Summary Report

Recommendations:

- Start with an audit effect instead of a deny effect to track the impact of your policy definition on the resources in your environment. If you have scripts already in place to autoscale your applications, setting a deny effect may hinder such automation tasks already in place.
- We recommend creating definitions at higher levels such as at the management group or subscription level. A definition created at the management group level can be assigned to a subscription or resource group within that management group.
- We recommend creating and assigning initiative definitions even for a single policy definition. For example: you have policy definition policyDefA and create it under initiative definition initiativeDefC. If you later create another policy definition for policyDefB with goals similar to policyDefA, you can add it under initiativeDefC and track them together.
- Once you have created an initiative assignment, policy definitions added to the initiative also become part of that initiative's assignments.
- Evaluating an initiative assignment involves evaluating all of the policies grouped within that initiative. If you need to evaluate a policy individually, it is better to not include it in an initiative.

3.5.1 Allowed Location Policy

Built-in policies help ensure that Azure resources are only deployed to specific locations:

- Allowed locations
- Allowed locations for resource groups

These policies allow us to prevent the deployment of resources to other regions.

3.6 MONITORING

Azure Monitor helps you maximize the availability and performance of your applications and services. This comprehensive solution collects, analyzes and processes telemetry data from your cloud and on-premise environments. This information helps you understand how your applications are performing and actively identify issues.

Azure Monitor can collect data from a variety of sources. This ranges from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

- Application monitoring data
- Guest OS monitoring data
- Azure resource monitoring data
- Azure subscription monitoring data
- Azure tenant monitoring data

Log data and the metrics from most Azure resources can be sent through Diagnostic Settings to centralized data management such as Log Analytics Workspace. The Log Analytics agent is deployed on Azure virtual machines, the deployment can be done using the Defender for Cloud.

Monitoring scenarios:

- Ensure that there are no problems in the system.
- Track the availability of the system and its components.
- Manage performance to prevent an unexpected drop in data flow in the event of a load increase.
- Ensure that the system complies with the SLAs (Service Level Agreements) signed with the customer.
- Protect the privacy and security of the system, the users and their data.
- Track operations performed for control or legal purposes.
- Monitor daily system usage and identify trends that could lead to issues if left unaddressed.
- Track issues that arise from the first report through to root cause analysis, rectification, the ensuing software updates and deployment.
- Monitor workflow and debug software releases.

3.7 NETWORK

Azure Network Services provide a variety of network capabilities that can be used together or separately.

3.7.1 What is a virtual network in Azure?

Azure Virtual Network (VNET) is the fundamental building block for your private network in Azure. VNET enables many types of Azure resources (such as Azure Virtual Machines) to communicate with each other, the Internet and on-premise networks. VNet is similar to a traditional network that you would operate in your own data center, but offers the additional benefits of Azure's infrastructure such as scale, availability and isolation.

Azure offers you different approaches to create your network. It is recommended to deploy a hub and spoke network topology, which offers benefits such as cost reduction, workload isolation and the circumvention of the technical limitations of Azure subscriptions.

Hub-spoke network topology in Azure - Azure Reference Architectures | Microsoft Docs

3.7.2 Network segmentation

Segmentation is a model in which you take your networking footprint and create software-defined perimeters using tools available in Microsoft Azure. You then set rules that govern the traffic from/to these perimeters so that you can have different security postures for various parts of your network. This solution is interesting when you place different applications (or parts of a given application) into these perimeters because you can govern the communication between these segmented entities. This model offers an additional advantage: if a part of the application stack is compromised, you can better contain the impact of this security breach, and prevent it from laterally spreading through the rest of your network. This is a key principle of the Microsoft's Zero Trust model that offers a world-class security solution to your organization.

Azure presents the following tools for this purpose:

3.7.2.1 Network Security Groups (NSG)

NSGs are access control mechanisms to regulate traffic between resources within a virtual network and with external networks (Internet, other virtual networks, etc.). It is possible apply a more granular segmentation policy using NSCs by creating perimeters for a subnet, a group of virtual machines, or even a single virtual machine.

3.7.2.2 Application Security Groups (ASG)

ASGs provide control mechanisms similar to NSGs but are referenced with an application context. An ASG allows you to group a set of virtual machines under an application tag. It can define traffic rules that are then applied to each of the underlying virtual machines.

3.7.2.3 Azure Firewall

Azure Firewall is a cloud-native service that can be deployed in virtual networks or in Azure Virtual WAN hub deployments to filter traffic that flows between cloud resources, the Internet, and on-premise. You create rules or policies (using Azure Firewall or Azure Firewall Manager) specifying allow/deny traffic using layer 3 to layer 7 controls. For advanced filtering and user protection, you can also filter traffic that comes from the Internet using Azure Firewall or third-party solutions. Direct some or all of traffic to third-party security providers to do this.

3.7.3 Network connection in Azure

There are two ways to connect on-premise sites with the Azure network:

– ExpressRoute (Azure ExpressRoute Overview: Connect over a private connection | Microsoft Docs)

– Site-to-Site VPN (About Azure VPN Gateway | Microsoft Docs)

The main difference between these two technologies is that ExpressRoute establishes the connection through a private, paid Microsoft backbone connection while VPN travels through the public Internet. However, these connections are both encrypted.

3.8 ACTIVE DIRECTORY

In the event that Windows domain member servers continue to be operated in Azure as IaaS virtual machines, the ISO 27001 blueprint provides for domain controllers in the core area of the Active Directory that ensure Kerberos authentication and authorization into the virtual network. Using an on-premise connection through a VPN gateway or ExpressRoute in the Gateway Subnet, the domain controllers replicate and synchronize data with the existing Active Directory.

Azure Bastion is also available to provide secure remote access to these virtual machines without a public IP address.

3.9 KEY VAULT

For any type of data encryption with customer-managed keys (CMK), Azure Key Vault partners with an HSM (hardware security module, whether on-premise or within the Azure management service). It stores encryption keys, passwords and certificates for transmission only to applications that are authorized by their service accounts. The human risk factor inherent in manipulating these security features is thus eliminated and security is enhanced since these "secrets" do not have to be entered manually or openly recorded in code.

3.10 COST CONTROL

Azure Cost Management offers tools that allow you to plan, analyze and reduce your expenses and thus maximize the profits you derive from the cloud. This cost control makes it possible to optimize the cloud solution to reduce costs and better take advantage of the advantages offered by the cloud.

- The **Cost analysis** feature helps you analyze costs. Different visualizations allow you to display the accumulated costs in different ways.
- The **Budgets** feature allows you to configure different types of alerts that will notify you if a certain limit value is exceeded.
- The **Recommendations** feature helps you identify resources that are used infrequently or not at all and thus take measures to avoid wasting them.

For cost management, it is possible to rank the different resources in order to assign costs to them, which can be done through tagging where each resource is attached to its metadata.

Tagging is the best way to understand the data as part of the cost report. It is essential for any well-managed environment but is also the first step in the governance of an environment.

A tagging standard must first be defined to ensure the accurate tracking of cost information at the business unit, environment and project levels. The second step is to ensure the consistent application of this tagging standard. Using Azure Policy, we can ensure that all resources are actually assigned a tag. To do this, the tags are automatically inherited or tags are automatically applied according to certain indicators.

3.11 DEFENDER FOR CLOUD

Microsoft Defender for Cloud plays an important role in your governance strategy. It helps monitor your security posture in Azure:

- It provides a consistent view of security for all workloads.
- It collects, researches and analyzes security data from various sources, including from firewalls and other partner solutions.
- It provides security recommendations to concretely resolve issues before they can be exploited.
- It can be used to apply security policies to your hybrid cloud workloads in order to ensure that security standards are met. The ISO 27001 standards can thus be implemented using Microsoft Defender for Cloud.

Many security features, such as security policies and recommendations, are available for free. Some of the advanced features, such as just-in-time virtual machine access and support for hybrid workloads, are available at the standard level of Defender for Cloud. Just-in-time VM Access can help reduce network exposure to attack by controlling access to Azure virtual machines' management ports.

Microsoft Defender for Cloud allows you to strengthen your security posture. This service helps you identify and perform hardening tasks recommended as security best practices and implement them on your machines, data services and applications. It also manages and enforces your security policies and ensures the compliance of your Azure virtual machines, non-Azure servers and Azure PaaS services. Defender for Cloud gives you the tools you need to get a comprehensive view of your workloads and, in particular, your network security space.

4 ISO 27001 CONTROLS

Each control below is associated with one or more Azure Policy definitions. These policies can help you assess **compliance** with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves; this does not ensure that you are fully compliant with all of the requirements of a control. In addition, the compliance standard includes controls that are not addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and the Azure Policy Regulatory Compliance definitions for these compliance standards may change over time.

The following chapters list the ISO 27001 controls for which Microsoft has implemented appropriate policies in the Defender for Cloud for technical assessment. In addition to the basics, other potential measures and controls derived from the Microsoft Public Sector Cloud Design risk assessment are also offered.

4.1 A.6.1.2 PARTITIONING OF TASKS

Conflicting duties and areas of responsibility must be segregated in order to reduce the opportunities for the unauthorized or unintentional modification or misuse of any of the organization's assets.

Documentation about the ISO standard:
https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/

Blueprint content

If you have only one owner of Azure subscriptions, you have no risk of administrative redundancy. By contrast, a high number of subscription owners increases the risk of a breach from a compromised user account. This blueprint helps you maintain an appropriate number of Azure subscription owners by assigning two Azure Policy definitions that verify the exact number of them. Managing subscription owner permissions can help you implement appropriate separation of duties.

– A maximum of three owners should be designated for your subscription.

– There should be more than one owner assigned to your subscription.

Additional measures and strategies

– Limit the number of existing global administrators to a minimum for emergencies (recommendation: two to three)

– Implement the concept of roles without relying on a global administrator or the subscription owner.

4.2 A.8.2.1 CLASSIFICATION OF INFORMATION

Information must be classified in terms of legal requirements, value, criticality and sensitivity to any unauthorized disclosure or modification, ideally classified to reflect business activity rather than inhibit or complicate it.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-8-asset-management/

Blueprint content

The Azure SQL vulnerability assessment service helps you detect sensitive data that is stored in your database and provides recommendations on the classification of this data.

– Security vulnerabilities in your SQL databases should be removed.

Additional measures and strategies

– Resources that include data should be classified with resource tags.

– Azure Purview enables a general classification of the data content of supported resources and enters the data into a data catalog for review.

4.3 A.9.1.2 ACCESS TO NETWORKS AND NETWORK SERVICES

The principle of least access is the general approach: it is favored for protection, rather than unlimited access and super-user rights without careful consideration.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-9-access-control/

Blueprint content

Azure implements role-based access control (Azure RBAC) to manage the access rights to Azure resources. This blueprint helps you control access to Azure resources by assigning Azure policy definitions. These policies verify the use of resource types and configurations that can be more easily accessed. Understanding which resources violate these policies can help you take corrective action to ensure that access to Azure resources is limited to authorized users.

– Add a system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities

– Add a system-assigned managed identity to enable Guest Configuration assignments on virtual machines with a user-assigned identity

– Audit Linux machines that allow remote connections from accounts without passwords

– Audit Linux machines that have accounts without passwords

– Audit virtual machines that do not use any managed data carrier

– Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux virtual machines

– Storage accounts should be migrated to new Azure Resource Manager resources

– Virtual machines should be migrated to new Azure Resource Manager resources

Additional measures and strategies

– Enable access rights to virtual network components only to responsible roles (groups).

– Prevent the free creation of public IP address resources.

4.4 A.9.2.3 MANAGEMENT OF PRIVILEGED ACCESS RIGHTS

The allocation and use of privileged access rights has to be tightly controlled given the extra rights usually conveyed over information assets and the systems controlling them.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-9-access-control/

Blueprint content

This blueprint helps you limit and control privileged access rights by assigning Azure policy definitions to verify accounts with owner permissions and/or write permissions that are external or have no multi-factor authentication (MFA) enabled. Azure role-based access control (Azure RBAC) helps you manage access rights to Azure resources. This blueprint also assigns Azure policy definitions to verify the use of Azure Active Directory authentication for SQL Server and Service Fabric. The use of Azure Active Directory authentication simplifies rights management and centralizes identity management for users of databases and other Microsoft services. This blueprint also assigns an Azure policy definition to audit the usage of custom Azure RBAC rules. Knowing where custom Azure RBAC rules are implemented helps you verify that they are being correctly implemented because these rules are prone to errors.

- We recommend deploying an Azure Active Directory administrator for the SQL server.
- Audit usage of custom RBAC rules
- External accounts with owner permissions should be removed from your subscriptions.
- External accounts with write permissions should be removed from your subscription.
- MFA should be enabled on accounts with write permissions on your subscriptions.
- MFA should be enabled on accounts with owner permissions for your subscriptions.
- Service Fabric clusters should only use Azure Active Directory for client authentication.

Additional measures and strategies

- Implementation of Azure AD Privileged Identity Management (PIM) to enable privileged roles and usage rights based on time and permissions.
- Implementation of Azure AD Entitlement Management for identity and access lifecycle management.

4.5 A.9.2.4 MANAGING SECRET USER AUTHENTICATION INFORMATION

Secret authentication information is a gateway to access valuable assets. It typically includes passwords, encryption keys, etc., so such information needs to be controlled through a formal management process and needs to be kept confidential to the user.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-9-access-control/

Blueprint content

This blueprint assigns three Azure policy definitions to audit accounts that have not enabled multi-factor authentication. Multi-factor authentication helps ensure account security even if part of the authentication information is compromised. By monitoring accounts that have not enabled multi-factor authentication, you can identify those that are more likely to be compromised. This blueprint also assigns two Azure policy definitions that check the Linux virtual machine password file permissions to warn if they are improperly created. This configuration allows you to take corrective actions to ensure that the authenticators are not compromised.

- Add a system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities
- Add a system-assigned managed identity to enable Guest Configuration assignments on virtual machines with a user-assigned identity
- Audit Linux machines that do not have the password file permissions set to 0644
- Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux virtual machines.
- MFA should be enabled on accounts with write permissions on your subscriptions
- MFA should be enabled on accounts with owner permissions for your subscriptions.
- MFA should be enabled on subscription accounts with read permissions.

4.6 A.9.2.5 REVIEW OF USER ACCESS RIGHTS

Asset owners must review users' access rights at regular intervals, both around individual change (on-boarding, change of role and exit) and broader audits of the systems access. Authorizations for privileged access rights should be reviewed at more frequent intervals given their higher risk nature.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-9-access-control/

Blueprint content

Azure role-based access control (Azure RBAC) helps you manage access rights to Azure resources. Using the Azure portal, you can verify who has access to Azure resources and their permissions. This blueprint assigns four Azure policy definitions to verify which accounts should be reviewed first, including inactive accounts and external accounts with elevated permissions.

- Obsolete accounts should be removed from your subscriptions.
- Obsolete accounts with owner permissions should be removed from your subscriptions.
- External accounts with owner permissions should be removed from your subscriptions.
- External accounts with write permissions should be removed from your subscriptions.

Additional measures and strategies

- We recommended using Azure AD Access Review to conduct a regular review of the permissions of the existing roles to ensure that no unauthorized access can occur.

4.7 A.9.2.6 REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS

The access rights of all employees and external party users to information and information processing facilities need to be removed upon the termination of their employment, contract or agreement (or adjusted upon a change of role if required).

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-9-access-control/

Blueprint content

Azure role-based access control (Azure RBAC) helps you manage access rights to Azure resources. Azure Active Directory and Azure RBAC allow you to update user roles to adapt to changes in the organization. Accounts can be made inaccessible (or deleted) upon login, if necessary, which also immediately removes access rights to Azure resources. This blueprint assigns two Azure policy definitions to review an inactive account that may be deleted.

– Obsolete accounts should be removed from your subscriptions.

– Obsolete accounts with owner permissions should be removed from your subscriptions.

Additional measures and strategies

– We recommended using Azure AD Access Review to conduct a regular review of the permissions of the existing roles to prevent any unauthorized access.

4.8 A.9.4.2 SECURE LOG-ON PROCEDURES

Access to systems and applications must be controlled by a secure log-on procedure to prove the identity of the user. This can go beyond the typical password approach into multi-factor authentication, biometrics, smart cards, and other means of encryption based on the risk being considered.

Secure log on should be designed so it cannot be easily circumvented and to ensure that any authentication information is transmitted and stored encrypted to prevent interception and misuse.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-9-access-control/

Blueprint content

This blueprint assigns three Azure policy definitions to audit accounts that have not enabled multi-factor authentication. Azure Multi-Factor Authentication provides additional security as it requires a second form of authentication and ensures strong authentication. By monitoring accounts that have not enabled multi-factor authentication, you can identify those that are more likely to be compromised.

– MFA should be enabled on accounts with write permissions on your subscriptions

– MFA should be enabled on accounts with owner permissions for your subscriptions.

– MFA should be enabled on subscription accounts with read permissions.

Additional measures and strategies

– Thanks to Azure AD Conditional Access, different connection limits may be implemented following application and user risk assessment.

– Storage accounts should not allow anonymous access.

4.9 A.9.4.3 PASSWORD MANAGEMENT SYSTEM

The purpose of a password management system is to ensure that passwords meet the required quality level.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-9-access-control/

Blueprint content

This blueprint helps you enforce strong passwords by assigning Azure policy definitions that check for Windows virtual machines that do not meet minimum password strength and other requirements. Knowing which virtual machines violate the password strength policy will help you take corrective action to ensure that all passwords for all virtual machine user accounts comply with the policy.

- Add a system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities
- Add a system-assigned managed identity to enable Guest Configuration assignments on virtual machines with a user-assigned identity
- Audit Windows machines that allow re-use of the previous 24 passwords
- Audit Windows computers that do not enforce a maximum password age of 70 days
- Audit Windows computers that do not enforce a one-day minimum password age
- Audit Windows computers where the password complexity setting is not enabled
- Audit Windows computers where a minimum length of 14 characters is not set for passwords
- Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows virtual machines.

Additional measures and strategies

- Azure AD passwords must meet length and character requirements
- Enable Azure AD Password Protection to prevent poor quality passwords derived from dictionaries

4.10 A.10.1.1 POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

Proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-10-cryptography/

Blueprint content

This blueprint helps you enforce your policy on the use of cryptographic controls by assigning 13 Azure policy definitions that enforce specific cryptographic controls and verify whether weak cryptographic settings are used. By understanding where the cryptographic configurations of your Azure resources might not be optimal, you can take corrective actions to ensure that your resources comply with your information security policy. In particular, the policies assigned by this blueprint require the encryption of Blob and Data Lake storage accounts; require the transparent data encryption of SQL databases; verify the absence of encryption of storage accounts, SQL databases, hard disks of virtual machines and variables of Automation accounts; verify insecure connections to storage accounts, functional apps, web apps, API apps and Cache for Redis; verify the weak encryption of virtual machine passwords; and verify unencrypted Service Fabric communications.

- Functional applications should only be accessible over HTTPS
- Web applications should only be accessible over HTTPS
- API applications should only be accessible over HTTPS
- Deploy the requirements necessary to audit Windows virtual machines that do not store passwords using reversible encryption
- View the audit results for Windows virtual machines that do not save passwords
- Hard disk encryption should be applied to virtual machines
- Automation account variables should be encrypted
- Only secure connections to your Azure Cache for Redis should be enabled
- Secure transfer to storage accounts should be enabled
- Service Fabric clusters should have the Cluster Protection Level property set to Encrypt and Sign
- Transparent data encryption for SQL databases should be enabled

Additional measures and strategies

- Storage account encryption should be enabled
- Storage accounts should only be accessible over HTTPS
- TLS 1.2 should be consistently used on storage accounts

4.11 A.12.4.1 EVENT LOGGING

Event logs recording user activities, exceptions, faults and information security events need to be produced, kept and reviewed regularly.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Blueprint content

This blueprint helps you ensure that system events are logged by assigning seven Azure policy definitions that verify the log settings for Azure resources. The diagnostic logs provide insight into the operations that were performed within an Azure resource.

- Dependency agent audit initiation - Image of the virtual machine (OS) not listed
- Dependency agent audit deployment in the Virtual Machine Scale Set - Image of the virtual machine (OS) not listed
- Log Analytics agent audit deployment - Image of the virtual machine (OS) not listed
- Log Analytics agent audit initiation in VM Scaling Sets - Virtual Machine (OS) Image Not Listed
- Audit diagnostic setting
- New audit should be enabled on the SQL server

Additional measures and strategies

- Azure Policies not only makes it possible to verify whether the relevant resources are using the necessary logging options, but also to apply them immediately.

4.12 A.12.4.3 ADMINISTRATOR AND OPERATOR LOGS

System administrator and system operator activities need to be logged and the logs protected and regularly reviewed. Special consideration should be given to greater levels of logging for privileged accounts such as system administrators and operators.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Blueprint content

This blueprint helps you ensure that system events are logged by assigning Azure policy definitions that verify the log settings for Azure resources. The diagnostic logs provide insight into the operations that were performed within an Azure resource.

- Monitoring of the diagnostic setting
- Monitoring in the SQL server should be enabled
- Monitoring in the SQL server should be enabled
- The Dependency agent should be enabled for the listed virtual machine image repositories.
- The Dependency agent must be enabled in the virtual machine scale groups for the virtual machine listed images.
- The Log Analytics agent should be enabled for the listed virtual machine images.
- The Log Analytics agent should be enabled in the virtual machine scale groups for the listed virtual machine images

Additional measures and strategies

- Monitoring of Azure AD login and audit logs

4.13 A.12.4.4 CLOCK SYNCHRONIZATION

The clocks of all relevant information processing systems within an organization or security domain must be synchronized to a single reference time source.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Blueprint content

This blueprint helps you ensure that system events are logged by assigning Azure policy definitions that verify the log settings for Azure resources. Azure logs rely on synchronized internal clocks to provide time-correlated event records for all resources.

- Monitoring of the diagnostic setting
- Monitoring in the SQL server should be enabled
- The Dependency agent should be enabled for the listed virtual machine image repositories
- The Dependency agent must be enabled in the virtual machine scale groups for the virtual machine listed images
- The Log Analytics agent should be enabled for the listed virtual machine images
- The Log Analytics agent should be enabled in the virtual machine scale groups for the listed virtual machine images

4.14 A.12.5.1 INSTALLATION OF SOFTWARE ON OPERATING SYSTEMS

Procedures must be implemented to control the installation of software on operational systems.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Blueprint content

Adaptive application control is a solution from Microsoft Defender for Cloud that lets you control which applications can run on your virtual machines hosted in Azure. This blueprint assigns an Azure policy definition that monitors the set of permitted applications. This capability helps you control the installation of software and applications on Azure virtual machines.

- Adaptive Application Control intended to define safe applications should be enabled on the computers

4.15 A12.6.1 MANAGEMENT OF TECHNICAL VULNERABILITIES

Information about technical vulnerabilities of information systems being used must be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Blueprint content

This blueprint helps you manage information system vulnerabilities by assigning Azure policy definitions that monitor missing system updates and operating system, SQL, and virtual machine vulnerabilities in Microsoft Defender for Cloud. Microsoft Defender for Cloud offers reporting capabilities that allow you to see the security status of the deployed resources in real time.

- A vulnerability assessment solution should be installed on your virtual machines
- Monitor missing protection with Endpoint Protection in Microsoft Defender for Cloud
- Security risks to SQL databases should be addressed
- System updates should be installed on your computers
- Security risks for your computers should be eliminated

4.16 A.12.6.2 RESTRICTIONS ON SOFTWARE INSTALLATION

Software installation should be subject to rules that are defined and implemented by the user. This control focuses on reducing the ability of users to install software, especially in on-premise terminals (workstations, laptops, etc.).

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-12-operations-security/

Blueprint content

Adaptive application controls is a solution from Microsoft Defender for Cloud that lets you control which applications can run on your virtual machines hosted in Azure. This blueprint assigns an Azure policy definition that monitors the set of permitted applications. Software installation restrictions can help you minimize the likelihood of introducing software vulnerabilities.

- Adaptive Application Control intended to define safe applications should be enabled on the computers

Additional measures and strategies

- Secondary Source Control Management (SCM) interfaces (Kudu, GitHub integration, etc.) of the supported resources should be secured.

4.17 A.13.1.1 NETWORK CONTROLS

Networks must be managed and controlled in order to protect information within systems and applications.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-13-communications-security/

Blueprint content

This blueprint helps you manage and control networks by assigning an Azure policy definition that monitors network security groups endowed with permissive rules. Overly permissive rules might expose your network to unwanted access and should be reviewed. This blueprint also assigns three Azure policy definitions to monitor unprotected endpoints, applications and storage accounts. Endpoints and applications that are not protected by a firewall as well as storage accounts with unrestricted access are likely to expose information contained in the information system to unwanted access.

- Access though an internet-facing endpoint should be restricted.
- Storage accounts should limit network access.

Additional measures and strategies

- Forced NSG assignment on subnets to limit permissible traffic.
- Forced assignment of route tables on subnets to control outbound data traffic through a firewall.
- Implementation of private endpoints for all supported PaaS services to limit network communication between application components to private networks
- Use of secure network features to publish web applications onto the Internet or access them from the Internet:
  - Application Gateway (for web applications)
  - Azure Front Door (for multi-region web apps)
  - Load Balancer (for a public IP for applications)
  - NAT Gateway (public IP for outgoing Internet traffic)
  - Bastion Host (for remote desktop access to virtual machines)

4.18 A.13.2.1 INFORMATION TRANSFER POLICIES AND PROCEDURES

Formal transfer policies, procedures and controls must be in place to protect the transfer of information through the use of all types of communication facilities.

Documentation about the ISO standard: https://www.isms.online/iso-27001/annex-a-13-communications-security/

Blueprint content

The blueprint helps you ensure the secure transfer of information with Azure services by assigning two Azure policy definitions that check insecure connections to storage accounts and your Cache for Redis.

- Only secure connections to your Azure Cache for Redis should be enabled.
- Secure transfer to storage accounts should be enabled.

Additional measures and strategies

- Only transfer via HTTPS should be enabled in App Services.
- Only transfer via HTTPS should be enabled in Front Door.
- Only transfer via HTTPS should be enabled in Application Gateway.

Microsoft

Thank you
Danke
Grazie
Engraziel