13 Effective Security Controls for ISO 27001 Compliance

When using Microsoft Azure

Microsoft

Disclaimer

Published January 2016

Acknowledgements

Authors: Frank Simorjay

Contributors: Tom Shinder, Joel Sloss, Leslie Sistla

Reviewers: David Cross, Alison Howard (LCA) Steve Wacker

Table of Contents

Introduction

Microsoft® Azure™ provides services that can help meet the security, privacy, and compliance needs of Microsoft customers. In addition, Microsoft works with customers to help them understand their responsibilities to protect their data and environment infrastructure after their service has been provisioned. This infrastructure includes applications, data content, virtual machines, access credentials, and compliance issues requirements.

This paper provides insight into how organizations can use thirteen security principles to address critical security and compliance controls, and how these controls can fast track an organization's ability to meet its compliance obligations using cloud-based services.

The thirteen principles are designed on best practices that are aligned to International Organization for Standardization (ISO) 27001, the Microsoft Security Development Lifecycle (SDL), and operational security for Microsoft online services.

Considerations and tools for success

Global adoption of cloud services continues to accelerate, yet many organizations remain wary of trusting multi-tenant platforms with their data, applications, or infrastructure. At Microsoft, trust is a focal point for services delivery, contractual commitments, and industry accreditation.

To help establish this trust, Microsoft Azure operates services according to three fundamental tenets:

- Experience that facilitates innovation and the development of reliable software and services that customers can use to build their own secure, private, and compliant solutions.
- Transparency that provides insight into how Microsoft achieves security and privacy for its customers and meets compliance standards.
- Shared responsibility that helps ensure both individuals and organizations can manage their cloud computing experiences in accordance with their security and privacy needs.

Azure is hosted in Microsoft datacenters around the world, and is designed to offer the performance, scalability, security, and service levels that enterprise customers expect. Microsoft has applied state-of-the-art technology and processes to maintain consistent and reliable access, security, and privacy for every user. Azure has built-in capabilities for compliance with a wide range of regulations and privacy mandates.

Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web—for moving faster, achieving more, and saving money. Azure serves as a development, service hosting, and service management environment, providing customers with on-demand compute, storage, networking, and content delivery capabilities to host, scale, and manage applications on the Internet.

To get the most out of this paper, readers should be familiar with basic Azure and cloud computing concepts, as well as security and compliance fundamentals—they will not be covered here. Links to additional materials can be found on the Get started with Azure webpage as well as through the Azure Trust Center

Experience

Microsoft has considerable experience in delivering consumer and enterprise cloud services at global scale. Since the launch of MSN® in 1994, the Microsoft cloud infrastructure has grown to support more than one billion customers and 200 million organizations in 76 markets worldwide. Microsoft uses the knowledge it gains by operating its own cloud infrastructure and by providing its customers with cloud-based solutions to develop best practices and technology innovations that support optimized security, privacy, compliance, and reliability.

Microsoft enables organizations to adopt cloud computing rapidly via its cloud services such as Azure, Office 365™, and Microsoft Dynamics® CRM and takes an industry-leading approach to security, privacy, and reliability.

Transparency

Microsoft is committed to transparency and openness in all aspects of its cloud services. It shares details about its efforts in the areas of security and privacy through several portals and reports, including:

- Microsoft Trust Centers, which are used to address key issues and concerns expressed by Microsoft customers about specific Microsoft services.

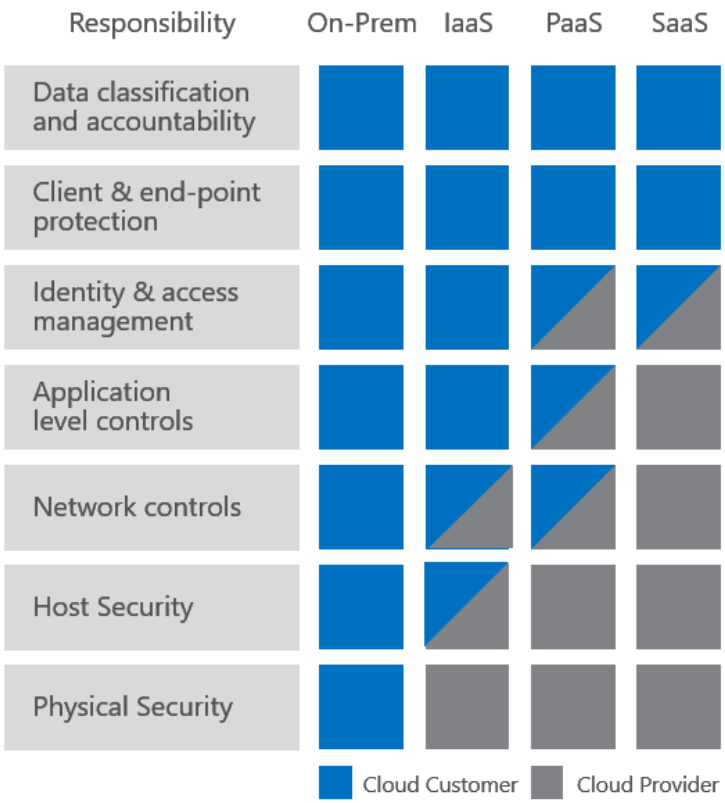
- Law Enforcement Requests Report. In March of 2013, Microsoft began publishing the number of demands it receives from law enforcement agencies as well as how many entities may be affected by such demands.
- Cloud Security Alliance. Microsoft is committed to transparency through its work with and support for CSA, who launched the Security, Trust & Assurance Registry (STAR) initiative in 2011 to promote transparency in cloud computing.

Shared responsibilities

Microsoft understands how different cloud service models affect the ways that responsibilities are shared between cloud service providers (CSPs) and customers.

The three primary cloud service models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The left-most column in the following figure shows seven responsibilities, all of which contribute to the overall security, privacy, and reliability of cloud computing environments. Two of the responsibilities are solely in the domain of customers, and two other responsibilities are in the domain of cloud providers. The remaining three responsibilities are shared between customers and cloud providers, depending on which cloud service model is being used.

The figure shows how customers and providers share the identity and access management responsibility for both Office 365 (a SaaS offering) and Azure (an IaaS/PaaS offering). It also shows how customers and providers share the application-level controls and network controls for Azure, but that these responsibilities fall completely in the domain of the provider for SaaS services such as Office 365.



- The customer is completely responsible for all aspects of operations when solutions are deployed on-premises.
- With IaaS, the lower levels of the stack (physical hosts or servers) and host security are managed by the platform vendor. The customer is still responsible for securing and managing the operating system, network configuration, applications, identity, clients, and data. For the developer, an obvious benefit with IaaS is that it reduces the developer requirement to configure physical computers.
- With PaaS, everything from network connectivity through the runtime or identity service may be provided and managed by the platform vendor. PaaS offerings further reduce the developer burden by additionally

supporting the platform runtime and related application services. With PaaS, the developer can almost immediately begin creating the business logic for an application.

- With SaaS, a vendor provides the application and abstracts customers from all of the underlying components. Nonetheless, the customer continues to be responsible to ensure that data is classified correctly and that user devices are secured and protected when connected to the service.

Considerations in meeting compliance requirements

This guidance is rooted in ISO, as a foundation for establishing an information security management system (ISMS). After such a system is set and the key ISMS best practices are established, the focus incorporates three key areas:

- Governance and compliance considerations
- Adopting secure development processes
- Establishing secure operations principles

The intention is to ensure that standard security development and operations best practices are incorporated from the beginning of a cloud project, and that key activities are communicated effectively with all the stakeholders in the context appropriate for their roles. These roles include: compliance officers, legal advisors, risk managers, solution architects, developers, and operations personnel.

Best practices and recommendations will be presented in the subsequent sections. The following list specifies the sections and their alignment to the standards ISO:

Foundation

- Establishing an ISMS | Aligned to ISO 27001
- Establishing standard operating procedures that align to the ISMS | Aligned to ISO 27001

Compliance considerations

- Compliance regulations such as SOC, PCI, and EU DPD (European Union Data Protection Directive) with clearly defined physical, technical, and administrative safeguards | Aligned to ISO 27001

Tools for solution design

- Adopt data governance practices | Aligned to ISO 27001
- Security Development Lifecycle | Aligned to ISO 27001
- Operational security for Microsoft online services | Aligned to ISO 27001 and NIST
- 13 key security principles for designing and securing solutions for Azure are presented, with recommendations | Aligned to ISO 27001

Use cases – principles applied in an industry-focused scenario

Aligning using ISO

Initially, organizations should consider adopting an information security management system. One example is ISO 27001, an auditable, international, information security management standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that formally defines requirements for a complete ISMS to help protect and secure an organization's data. ISO 27001 details a set of best practices and is intended to be applicable to all organizations, regardless of their type or size.

For organizations that deal with sensitive information, the ratified ISO 27018, an extension of the ISO 27001 standard, governs the processing of personally identifiable information (PII) by cloud service providers acting as PII processors. ISO 27018 details controls that address protecting PII in public cloud services. Azure was the first global cloud service to adopt ISO 27018, which provides an additional set of controls for an organization to consider when adopting an ISMS.

ISO 27002 is a complementary collection of 114 controls and best practice guidelines designed to meet the requirements detailed within ISO 27001. The controls are organized into 14 groups, and when properly implemented can help an organization achieve and maintain information security compliance by addressing specific issues that are identified during formal, periodic risk assessments. These 14 groups are:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition
- Development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management

Establishing or re-invigorating an ISMS is a very deep and broad topic with complex challenges, and there are many resources available to assist organizations in this endeavor. Organizations should consider conducting a risk assessment and aligning risk management and mitigation to that assessment. A second area of focus that organizations should consider is establishing standard operating procedures for each of the 14 ISO groups to establish core principles for the entire organization to follow.

Key principles and recommendations for secure development and operations

The following 13 key security principles align with ISO 27001 controls. Of the 14 ISO 27001 groups and 114 controls, these key principles have the most relevance to secure development and operations and so are highlighted with recommendations.

These security principles are designed to make cloud-based solutions more resilient to attack by decreasing the amount of time needed to prevent, detect, contain, and respond to real and potential Internet-based security threats, thereby increasing the security of related services.

By incorporating these principles and recommendations, customers can help mitigate and manage security risks from early stages of their adoption of cloud computing.

1. Enable identity and authentication solutions

Identity and authentication are essential to implement the SDL effectively and securely. The implementation of these capabilities is important for identifying unique users of a service because they help ensure that only the right person accesses the service. The correct implementation will help ensure that the user who is logging in is actually the user who was assigned access rights.

Identity management remains a priority, even as business networks change. Identity management is as much about preventing unauthorized access to data as it is about controlling the authorized use of data. Identity management helps systems control the amount and type of data that users can access. A well-implemented solution helps ensure that users who are performing necessary functions are doing so at the appropriate privilege level. Identity management is also critical for maintaining separation of roles and duties, which may be required by specific regulatory and compliance standards. Knowing who a user is lets an application determine how it should interact with that user. Managing identity is just as important in the public cloud as it is in on-premises environments.

Azure provides services to help track identity as well as integrate it with identity stores that may already be in use. Azure Active Directory (Azure AD) is a comprehensive identity and access management service for the cloud that helps secure access to data in on-premises and cloud applications; it also simplifies the management of users and groups. It combines core directory services, advanced identity governance, security, and application access management.

Azure AD provides developers an effective way to integrate identity management in their applications. Identity and authentication as referenced in this MSDN video are the first line of security defense at the organizational level and have the potential to be the weakest link in the security chain because they are the primary control that opens the 'door' to access management on which many aspects of security rely.

Recommendations:

- Identities should be kept up-to-date and managed for changes, additions, and removals. Ensure that only qualified individuals are made administrators. In addition, consider creating a unique user group to manage and log identities. Store customer identities in custom repositories such as Azure Active Directory.

- Connections between services should be implemented through a virtual private network. Azure supports both site-to-site or point-to-site VPN connectivity. Additional services such as ExpressRoute (which provides a dedicated WAN link to Azure) can also be implemented.
- Grant appropriate access to Azure AD users, groups, and services by assigning roles to them using Azure AD Role-based Access Control (RBAC).
- Because a compromised user account with privileged access (admin access) could affect overall cloud security, lessen risks by monitoring admins using Azure AD Privileged Identity Management. Manage the identities of portal administrators by adding or removing permanent or temporary administrators to each role using Privileged Role Management.
- Enable on-demand, "just in time" administrative access to directory resources.
- Ensure that permissions to sensitive data follow the least privilege principle and grant access for only the minimum necessary time needed for each role.
- Understand the core architecture of cloud identity by reading the The fundamentals of Azure identity management.

Authentication is essential for managing user identities. Authentication is the process of proving identity, typically through credentials, such as a user name and password. A growing number of employees, partners, and vendors require access from outside the office walls. And because of the bring your own device (BYOD) movement, that access is no longer limited to company-owned and managed laptops.

Users often connect from personal and mobile devices across unsecured networks. Organizational data and applications are on the move over these networks. With escalating IT security threats and a growing number of users, applications, and devices, multi-factor authentication has become the new standard for securing access.

Recommendations:

- Enable multi-factor authentication functionality for both cloud and on-premises applications.
- Establish strong password policies to manage user accounts stored in Azure AD. It is important that passwords and secrets be securely generated and changed at regular intervals to prevent password guessing and brute force attacks.
- If your corporate account has become compromised or if a device that has cached credentials is lost or stolen, suspend MFA for remembered devices and browsers.
- Set up Azure Conditional Access for SaaS applications, which allows the configuration of per-application multi-factor authentication access rules.
- Configure app passwords for non-browser clients.

2. Use appropriate access controls

Access control is a mechanism for providing a user who has a valid identity, and who has authorized rights and/or privileges, to access and perform functions using information systems, applications, programs, or files. Comprehensive access control strategies need to be in place, especially when considering the fact that corporate employees expect to work from any location, on devices of their choice, and to seamlessly connect and access business applications.

Microsoft Azure Active Directory Access Control (ACS) is a cloud-based service that provides a way to authenticate and authorize users to gain access to web applications and services, while allowing authentication and authorization to be factored out of code. Instead of implementing an authentication system with user accounts that are specific to an application, it's possible to let ACS orchestrate the authentication and much of the authorization of users.

Common ACS functionalities include:

- Federation
- Authentication
- Authorization
- Single Sign-out
- Security Token Flow and Transformation
- Trust Management
- Administration
- Automation

Role-based access control (RBAC) features can be used to restrict access and permissions for specific cloud resources. To help detect suspicious access, Azure Active Directory offers reports that provide alerts about anomalous activity, such as a user logging in from an unknown device. In addition, operational management suite capabilities can notify customers if someone stops a website, or if a virtual machine is deleted.

Recommendations:

- Secure inbound Internet communications to services using SSL.
- Register corporate devices with Azure AD.
- Set up Azure Conditional Access for SaaS applications, which allows the configuration of per-application multi-factor authentication access rules.
- Improve the quality of implementation from a security perspective by adhering to the ACS Security Guidelines. Also consider implementing retry logic when token requests to endpoints fail. Become familiar with ACS best practices for secure operations and development.
- Communication between on-premises hosts and cloud services should be authenticated, authorized, and encrypted using virtual Site-to-Site or Point-to-Site VPNs.

3. Use an industry-recommended, enterprise-wide antimalware solution

Malware, also known as malicious code and malicious software, refers to programs that are inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system to annoy or disrupt the victim. Malware such as viruses, trojans, and worms are usually designed to perform nefarious functions in such a way that users are unaware of them, at least initially.

Microsoft Antimalware for Azure is a security solution that extends antimalware protection to virtual machines and to cloud services. The antimalware software used by Microsoft cloud services supports a fully centrally managed solution that includes real-time scanning of incoming files, automatic checks for updated signature files and software updates, and alerts to the Microsoft Operations Center (MOC) of detected malicious code.

Microsoft also employs intrusion detection, distributed denial-of-service (DDoS) attack prevention, regular penetration testing, data analytics, and machine learning tools to help mitigate threats to the Azure platform. Azure offers three options for antivirus/antimalware solutions on Azure virtual machines:

- Symantec Endpoint protection
- Trend Micro Deep Security as a Service
- Microsoft Antimalware solution

Recommendations:

- Use the Azure Security Center to manage and deploy antimalware application, and all it's pertinent updates.
- Deploy antimalware solutions on Azure VMs.
- Use the Antimalware solution in Microsoft Azure Operational Insights to report on the status of antimalware protection in organizational infrastructure.
- Use Azure Security Center to help deploy and monitor antimalware solutions on IaaS and PaaS virtual machines.
- Establish and maintain general malware awareness programs for all users, as well as specific awareness training for the IT staff directly involved in activities that relate to malware prevention.

4. Effective certificate acquisition and management

A certificate is a form of identification for websites and web applications that is used to verify authenticity. Websites rely on TLS and Secure Socket Layer (SSL) to encrypt data communications. To securely configure TLS or SSL for an application requires a TLS or SSL certificate. Self-signed certificates can be acceptable in some restricted use cases (dev and test). However, a signed and authorized certificate that is issued by a certification authority (CA) or a trusted third-party who issues certificates for this purpose is recommended. Certificates can be obtained from a company that provides TLS and SSL certificates, such as the Windows root certificate program members list.

Azure uses certificates in several ways. For example:

- Management certificates. Stored at the subscription level, these certificates are used to enable the use of the SDK tools, the Windows Azure Tools for Microsoft Visual Studio, or the Service Management REST API Reference. These certificates are independent of any cloud service or deployment.
- Service Certificates. Stored at the cloud service level, these certificates are used by deployed services.
- Secure Shell (SSH) Keys. Stored on the Linux virtual machine, SSH keys are used to authenticate remote connections to the virtual machine.
- Point-to-site and site-to-site VPNs into Azure resources require certificates for authentication and encryption.
- RDP connections to Windows-based virtual machines.

Recommendations:

- Certificates used in production systems should only be acquired from one of the reputable certification authorities (CAs).
- Certificates need to be configured with traceable information, including designated contacts, from a limited set of authorized users.
- Self-signed certificates as well as general certificates should not be shared with or reused on systems that have a different application context.
- It is essential that certificates are treated as highly valued assets.
- Track expiration dates of certificates and keys. Because certificates and keys expire by design, it is important to track the expiration dates and take appropriate action prior to expiration so that applications that use ACS continue to function properly without interruption.
- Avoid embedding the IDs and secrets into applications. Consider applying the guidance provided as best practices for deploying passwords and other sensitive data in applications.
- Secure keys by protecting them in a Key Vault, which encrypts keys and small secrets like passwords with keys stored in hardware security modules (HSMs).

5. Encrypt all customer data

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information is encrypted using an encryption algorithm, which generates cipher text that can only be read if decrypted. An encryption scheme usually uses an encryption key generated by an algorithm. BitLocker encryption can be used to protect data at rest, and Transport Layer Security (TLS) can be used to protect data in transit.

Azure offers rich security functionality, including deep support for standardized encryption protocols. Developers can use the cryptographic service providers (CSPs) built into the Microsoft .NET Framework to access Advanced Encryption Standard (AES) algorithms, along with Secure Hash Algorithm (SHA-2) functionality to handle such tasks as validating digital signatures. Moreover, the Azure platform builds on the straightforward key management methods incorporated into the .NET security model, so developers can retain custom encryption keys within the Azure storage services.

Azure allows customers to encrypt data and manage keys, and safeguards customer data for applications, platforms, systems, and storage in the following ways:

- Protecting data at rest. Azure offers a wide range of encryption capabilities that provide customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps streamline key management and maintains control of keys used by cloud applications and services to encrypt data.
- Protecting data in transit. For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure strives to use industry-accepted standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves when possible.

Recommendations:

- Encrypt data in storage and in transit to align with best practices for protecting confidentiality and data integrity.
- Ensure all devices, including BYOD devices, use protected transmission and storage capabilities.
- Encrypt traffic between web client and server by implementing TLS on IIS.
- Choose HTTPS for REST API for storage.
- Use well-known encryption algorithms as provided in the .NET CSPs. These are proven and tested for security.
- Authentication tokens are often the target of eavesdropping, theft, or replay-type attacks. To reduce the success of these attacks, encrypt the communication channels.
- When designing web applications, use the secure design guidelines.
- Use Azure Key Vault to store secrets such as passwords with keys stored in hardware security modules (HSMs).

6. Penetration testing

Designers need to think like attackers when planning and designing an organization's network and services. Penetration testing is not about verifying functionality, but about verifying the absence of unsecured functionality. Effective penetration testing is about finding properties in software and its environment that can be varied, varying them, and seeing how the software responds. The goal is to ensure that software performs reliably and securely under reasonable and even unreasonable production scenarios.

Recommendations:

- Work with a reputable penetration solution vendor.
- Perform tests on endpoints to uncover OWASP top 10 web vulnerabilities.
- When using Azure services, request for permission to execute penetration tests.
- Review methods in penetration testing also called red teaming.
- Help Azure become resilient to attacks by reporting potential security flaws related to Microsoft services.

7. Threat modeling services and applications

Organizations need to properly define threats and classify information assets with a threat-modeling process. The Microsoft Security Development Lifecycle (SDL) provides an effective threat-modeling process that is used to identify threats and vulnerabilities in software and services. Threat modeling is usually done during the project design phase but can be done anytime to bring exposure to possible threats.

Threat modeling is a team exercise, encompassing the operations manager, program/project managers, developers, and testers, and represents a key security analysis task performed for solution design.

Threat modeling activities include:

- Completing threat models for all functionality using the SDL Threat Modeling Tool, which can be used to identify high-risk issues.
    - Modeling the service design and enumerating STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) threats across all trust boundaries has proven an effective way to catch design errors early.
- Threat modeling all services and projects. All code exposed on the attack surface and all code written by or licensed from a third party should be included in a threat model.
- Ensuring that threats can be mitigated and reviewed by the team.
- Reviewing a threat model when software is updated. New features or functionality can change the solution's threat profile.
- Endeavoring to build secure solutions with the mindset that they are trying to protect their customer's assets.

Recommendations:

- Use approved tools, software, and services. Ensure that only verified tools are used in solutions.
- Remove and deprecate unsafe functions, processes, and designs.
- Perform fuzz testing, static, and dynamic analysis of services and software solutions.
- Conduct attack surface analysis and reviews.
- Learn and understand how exploits and vulnerabilities might affect an organization by reviewing security threat intelligence.
- Apply threat modeling best practices as appropriate to current, new, and third-party services and applications.

8. Log security events, implement monitoring and visualization capabilities

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries. Each entry contains information related to a specific event that has occurred within a system or network. A forensic analysis uses a security and audit solution to seek out evidence that potentially malicious users leave behind. Regardless of what users do in their IT environment, many of the activities they participate in generate security artifacts. Evidence about their use is stored in event logs.

Azure Security Center provides a single place to help prevent, detect and respond to threats with increased visibility into and control over Azure resources. The Security Center provides your DevOps a quick and effective means to protect Azure assets when deploying them. The Security Center also provides alerting, and analysis of security events in a glance.

Azure Operational Insights collects these artifacts *as soon as they occur*, before anyone can tamper with them, and allows different types of analysis by correlating data across multiple computers. Azure enables customers to perform security event generation and collection from Azure IaaS and PaaS roles to central storage in their subscriptions. These collected events can be exported to on-premises security information and event management (SIEM) systems for ongoing monitoring. After the data is transferred to storage, there are many options to view the diagnostic data.

Azure built-in diagnostics can help assist with debugging, and Azure security and audit log management refers to how you can set up logging effectively to monitor your Azure subscription. For applications that are deployed in Azure, a set of operating system security events are enabled by default. You can add, remove, or modify events to be audited by customizing the operating system audit policy.

Recommendations:

- Refer to the Security Policy Settings guidelines to implement and manage security policies for Windows-based virtual machines running in Azure IaaS.
- Deploy Azure Security Center to help prevent, detect and respond to security threats.
- Enforce the right settings to ensure that Azure instances are collecting the correct security and audit logs.
- Monitor the overall health of an Azure instance through *Azure Status*.
- Monitor Media Services through the *Azure Media Services Dashboard*.
- Monitor cloud services and storage accounts through the *Azure Management Portal*.
- Monitor Web Apps in *Azure App Service*.
- Monitor Hadoop clusters in HDInsight using the *Ambari API*.
- Store service data and security log data in separate storage accounts. This isolation ensures that saving security log data does not affect the storage performance for production service data.
- Monitor Azure data factories using *Data Factory .NET SDK*.
- Protect and audit log files in virtual machines running in Azure IaaS using Windows access control lists (ACLs).

9. Determine the root cause of incidents

Root cause analysis (RCA) is a structured and facilitated team process used to identify root causes of an event that resulted in an undesired outcome. The end result of this exercise is to develop corrective actions that can be driven back into policy. The RCA process provides a way to identify breakdowns in processes and systems that contributed to the event and how to prevent future events. The purpose of an RCA is to find out what happened, why it happened, and determine what changes need to be made. Organizations need to be prepared to investigate a breach and provide an RCA of the breach – that is, thoroughly documenting the breach, how it happened, and specifically what has been done to address the security issue so that a breach doesn't happen again.

Operational Insights, as part of the Microsoft Operations Management Suite, is a software as a service (SaaS) solution tailored for IT operations teams. This service uses the power of Azure HDInsight to collect, store, and analyze log data from virtually any Windows Server and Linux source, from any datacenter or cloud, and turn it

into real-time operational intelligence to enable better-informed decisions.

Recommendations:

- Monitor high-risk Windows events within virtual machines running in Azure IaaS for better root cause analysis.
- Establish aggressive audit policies within virtual machines running in Azure IaaS.
- Adhere to and understand best practices for forensic analysis, security breach pattern investigations, and audit scenarios.
- Use the Azure Security Center to conduct security investigation for a suspicious executable.

10. Train all staff in cyber security

If a development team does not understand the basics of secure design and development or the risks of running web-based solutions and services, security training is imperative and should be completed before any Azure-based application is designed, built, tested, or deployed. All members of the operations and development teams should be informed about security basics and recent trends in security and privacy, and they should attend at least one relevant security training class every year at a minimum.

Staff and vendors should be encouraged to seek opportunities for additional security and privacy education when possible. Employees that are well-versed and up-to-date on security issues are better able to design, develop, and operate software with security in mind first.

Organizations must ensure that the software they create or acquire includes the security properties that are required to meet their current and evolving business and compliance needs. Accomplishing this goal requires that skilled individuals have a clear understanding of software security with respect to applicable business objectives and technologies in use, along with the skills required to specify, develop, test, and field the software appropriately.

A commitment to understanding security basics and the latest developments in security and privacy can greatly help organizations reduce the number and severity of exploitable software vulnerabilities, as well as to react appropriately to ever-changing threat landscapes.

Recommendations:

- Create an internal security awareness website to provide resources to communicate policy best practices and safety tips throughout the organization. Brief email bulletins can help reinforce and promote key security concepts, including step-by-step guidelines.
- Remember to keep it simple, and recognize that most employees are hired to support the business and not for their IT expertise. The key concepts of security, privacy, and information protection must be taught.
- Executive-backed security policies that all employees must comply with will help protect customer and company data.
- Make security interesting. Intranet webpages can teach users home safety in avoiding scams, malware attacks, and information disclosure. Help users take their security training home. Teach users to keep their home systems up-to-date and secure, which will help improve the organization's overall security posture.
- Provide brief, highly focused training sessions that are based on real events. Sharing key learnings can help users understand the risks.

11. Patch all systems and ensure security updates are deployed

Software systems need to be updated with necessary security updates regularly. Organizations need to watch for security threats and maintain stability of software environments. Minimizing security threats requires properly configured systems that use the latest software and have the recommended software updates/patches installed.

Microsoft has developed various solutions to help organizations that have varying needs to stay as up-to-date as possible within their own specific environments. Through the Automatic Updates feature, and when customers opt in through Windows Update, Windows can automatically keep computers up-to-date with the latest security updates for all Microsoft products. Users do not have to search for updates and information. Azure Security Center provides a single interface to help understand the deployment of updates and helps manage the distribution and installation of security updates for Microsoft software.

Recommendations:

- Enable Windows Update or use Windows Server Update Services, which provide recommendations to upgrading systems and to ensure they are up-to-date.
- Update all third-party applications, and use their patching capabilities when possible.
- Get security updates from the Microsoft Download Center.
- Review the best practices for applying service packs, hotfixes and security patches.
- Get updates for consumer platforms, such as Microsoft Update designed to update Microsoft products.
- Get the latest information on security-related patches.
- Follow the Security Development Lifecycle (SDL) recommendations to build more secure software and address security compliance requirements while reducing development cost.
- Enable notifications for new updates and reporting functionality based on update status, computer status, computer compliance status, and update compliance status.
- Review the Microsoft Security Update Guide to learn more about Microsoft Updates and Windows Server Update Services.
- Follow the Software Updates Security Best Practices.
- Use the Azure Security Center to report on the status of updates applied to infrastructure.

12. Keep service and server inventory current and up-to-date

Service and server inventory is about knowing what subscriptions, domains, services, networks, and hosts are owned and managed. Keeping track of the services and mitigating the risks that come with those services is key for secure operations. In addition, have an understanding and priority of the data that is being protected by implementing a data classification effort, as described in the Data classification for cloud readiness white paper.

Recommendations:

- Establish information classification.
- Identify data flows between integrated systems.
- Maintain documentation to reflect changes in inventory.
- Run network discovery to help identify hosts and networks in the organization's IP range.

13. Maintain clear server configuration with security in mind

Server misconfiguration is one of the most common causes for unauthorized users accessing and compromising the host. Because of the potentially complex security configuration requirements, it's essential to use a master server image that has security measures in place. Azure provides customers a marketplace with a gallery of

servers that have been configured with security in mind. However, the use of the servers in the marketplace requires attention when organizations require custom security modifications and to prevent security configuration drift.

If a custom virtual machine image is created, it's essential that the virtual machines have a standard set of baselines applied to them. The Microsoft Security Compliance Manager provides a means to create a standard baseline and deploy the baseline to existing servers, as well as create a master, or gold, image that enables security capabilities.

The Microsoft Baseline Configuration Analyzer (MBCA) can help identify and maintain optimal system configuration by analyzing configurations of computers against a predefined set of baselines designed by the security configuration manager, reporting results of the analyses. Best practices are packaged in the form of a best practice model kits. The kits are set of best practice configurations recommended for customers to use. Models are available as separately downloadable packages that can be run and analyzed by MBCA.

It's possible to test deployments using the Azure Best Practices Analyzer (BPA) for Azure Pack. BPA is a tool that analyzes the components of Azure Pack. It helps immediately identify many configuration, security, and performance issues, and it recommends best practices to resolve them. BPA for Azure Pack works within the Microsoft Baseline Configuration Analyzer (MBCA) to scan the software configurations of the computer on which it is installed. It automatically detects all components that are installed in Azure Pack and compares their configurations against a set of rules. MBCA then lists all noncompliant issues.

Recommendations:

- Protect domain and local administrative accounts with strong passwords and MFA.
- Use the Secure Administrative Hosts feature to administer servers.
- Allow RDP connections only from specific IPs by enabling Azure MFA white listing of administrative computers.
- Configure auditing events, monitor the failed logon attempts, and block the IPs.
- Configure auditing for failed logon events such as 4625 and 4648 and configure alerts or schedule tasks to run a batch file to extract the IP from the event log entry and block it by adding a firewall rule.
- Don't use the same password for all virtual machines. Change the passwords frequently.
- Run the Best Practices Analyzer and take appropriate action to fix security issues reported by the tool.

Conclusion

Cloud computing offers tremendous opportunities to enable increased quality and greater access at lower cost of services. When organizations consider moving a portion of their infrastructure to Microsoft Azure, they have to evaluate their overall privacy, security, and regulatory compliance posture. This guidance is provided as a way to approach such a migration with the use of international standards, understanding of compliance requirements, the principle of shared responsibilities, and rationalized mapping to address necessary controls.