Acme Information Technology Corp – InfoSec Policy Audit

Team Project Progress

Team 2

Anil Erturk

([erturkanil@cityuniversity.edu](mailto:erturkanil@cityuniversity.edu))

Bhavana Honnappa

([honnappabhavana@cityuniversity.edu](mailto:honnappabhavana@cityuniversity.edu))

Dave Lonack

([lonackdave@cityuniversity.edu](mailto:lonackdave@cityuniversity.edu))

Jiongjie Jiang

([BillJJJ@cityuniversity.edu](mailto:BillJJJ@cityuniversity.edu))

Sreelekha Sangitha

([sangithasreelekha@cityuniversity.edu](mailto:sangithasreelekha@cityuniversity.edu))

Yi Zhou

([Garren@cityuniversity.edu](mailto:Garren@cityuniversity.edu))

Zhijian He

(Zhijian-He@cityuniversity.edu)

City University of Seattle

ISEC 505 – Systems Security

James Taylor (jataylor@cityu.edu)

**Abstract**

Information Security Policy should be at the cornerstone of every organization to ensure the confidentiality, integrity, and availability (CIA) of systems and data, including employees and customers. In addition to the CIA domains, organizations should also focus on resiliency, which has become a focus for both government and non-government organizations. The following paper outlines specific security policy audit considerations for a fictitious IT organization (Acme Corp) as a case study. This organization operates globally with a complex hybrid IT architecture. This paper will provide details related to Acme’s IT architecture, required components of security policy aligned with one or more security frameworks/standards, and strategy around conducting an audit of Acme’s information security policy.

**Keywords:**  Security policy audit, ISO/IEC 27001:2013, NIST SP 800-53, FIPS 140-2, IT industry, security compliance, information security

**1.** **INTRODUCTION**

The following paper is an information security policy audit proposal for a fictitious global IT organization called Acme Information Technology Corp (“Acme”). Specifically, Acme wishes to retain our team to audit their information security policy program against a known standard that is globally recognized that focuses on security policy program best practices. Our team has decided to align our audit with ISO/IEC 27001:2013 and leverage aspects NIST SP 800-53 and FIPS 140-2 as appropriate for technical security controls. For this audit, Acme would also like to focus on resiliency, in addition to confidentiality, integrity, and availability domains.

Details about Acme –

* Provides custom application development and hosting services to its global customer base. Acme currently employs approx. Five thousand full-time and contract employees across 50 offices globally. Acme’s offices are located throughout the United States, Canada, Europe, Japan, Asia, and the United Arab Emirates.
* The IT environment is a hybrid between on-prem and cloud environments, which leverages Azure for authentication services and Amazon Web Services (AWS) for compute and storage and hosting other internal and external applications. AWS is also used for hosting customer applications.
* Employees are welcome to use Windows or macOS for their workstations
* Certain services are permitted on employee BOYD devices (e.g., E-mail, timekeeping)
* Employees can access internal services via VPN

This paper will outline how to conduct an audit of an organization IT security policy program, describe what sections or components should be included based on the applicable sector, and align with industry-recognized standards. Specifically, the following security policies will be described within the final deliverable:

* Encryption Management
* Group Management
* Recovery and Restoration
* Network Security Controls and Administration
* System Hardening and Security
* Backup
* Software Development Management

**2. POLICIES**

**1.Encryption Management Policy**

Currently, Acme can deploy encryption on many different software or systems, including websites, email communications, user and organizational data security. Encryption is the process of packaging data, so only the target organization or user can access it. Typically, administrators use security tools (such as encryption keys) to complete this process. Each key will contain a randomly generated code to encrypt/decrypt data. The encryption management strategy will cover all processes and methods related to encryption (from key production to destruction). Encryption management will include:

* Develop and implement various strategies, systems, and standards to manage key processes.
* Perform necessary key functions, such as key generation, activation, expiration, and destruction.
* Restrict users from accessing encryption keys. Only allow users to access data directly.
* Ensure physical and virtual access to key servers.

A strong encryption management strategy to store keys is essential. The strength of the encryption algorithm can be determined by the complexity of the mathematical algorithm. However, what is more important is how to store and manage keys. Before considering encryption management, security personnel needs to determine what kind of data to encrypt. Therefore, not all content needs to be encrypted, which will consume a lot of CPU calculation and workload.

According to Thakkar, J. Best Practice Policy for Encryption Management.

* Centralized organization of encryption key management system. The key manager completes the key generation, and the key manager is not in the data location.
* Use automation to give full play to their advantages. Administrators relying solely on manual key management are time-consuming and expensive, and they often cause errors, especially for enterprises and other large organizations.
* Centralize user roles and access permissions to ensure that no single user or administrator has unique access to the key. This is to prevent the administrator from leaving accidentally or the user from leaving.
* Support multiple encryption standards, such as AES, RSA, etc.
* Have good log records and audits.
* Create encryption key management strategies for employees.
* To implement the principle of least privilege, organizations should avoid assigning as many administrative privileges as possible to applications, as this will make applications extremely vulnerable to internal and external threats. Instead, what they should do is grant access based on user roles. This is called “the principle of least privilege.”
* After integrating with third-party equipment, the third-party equipment will simplify the encryption function and provide a visual operation interface.
* Back up the encryption key. It is crucial to have a useful key backup function to prevent losing the encryption key.

A strong encryption management strategy makes it easier for enterprises to operate during the encryption process. Generally, security policy management needs to follow security and scalability, and encryption algorithms in the enterprise may be upgraded and updated over time. When accessing, the enterprise must ensure that the key is granted to the user appropriately and in compliance.

**2. Group Management Policy**

Through effective Group Policy management, the security department can make the essential changes necessary to properly configure the operating system, applications, and end-user settings. Acme will control various advanced settings of the work environment for users and computer accounts in Active Directory. By setting the correct group policy, the company can improve the computer's security and help defend against internal threats and external attacks.

Windows Group Policy Management

Acme company configured windows system computer as the standard working environment. Therefore, company security administrators use group policy management tools for centralized management. The organization will be set according to two types of Group Policy, including local GPO and non-local GPO. Local GPO only applies to internal company computers. The administrator will import the pre-configured local GPO into all the company's computers. Employees in different positions will use computers for the corresponding functions. The other type is a non-local GPO, which is a group policy stored in Active Directory. Administrators can easily control GPOs in different domains. Non-local GPOs can apply multiple group policies. The order in which Group Policy objects are placed determines their priority. When a conflict occurs, the system can predictably apply settings.

Group policy settings

The following are the critical group policy settings proposed by Acme Security Management:

* Adjust access to the control panel. Restricting employees' use of computer control panels can improve a safe working environment. The administrator will control employees' access rights by setting the "No access to the control panel" policy.
* Control access to the command prompt (cmd). Users can gain advanced access rights through the command prompt. The administrator can enable "Prevent access to a command prompt." When ordinary employees want to open the command prompt, the system should pop up a warning to prevent users from accessing it.
* The use of removable media drives, DVD, CD, and floppy disk drives are prohibited. Mobile drives usually contain viruses or malware, so the administrator should disable all drives by setting the "deny access to all removable storage" settings.
* Restrict software installation. If employees can install any software freely, this will increase the risk factor of the computer. Companies should manage employee permissions through group policies. The administrator will prohibit users from installing software. At the same time, employees need to apply to participate in the installation of special software.
* Account password setting. Employees need to set a complex password with a certain length. The administrator will improve the security of the computer by setting "minimum password length," "password character requirements," "password usage period," and other policies.

**3.Recovery and Restoration Policy-Zhijian He**

The purpose of this policy is to ensure that backup copies are created and tested at regular intervals. The main goals of this policy are to define backup and recovery standards. Prevent data loss in case of accidental deletion or damage of data. The list of services and controls that should apply this strategy includes confidential company data, intellectual property data, network equipment configuration files, key service configuration, etc. All departments must properly backup data and employees must accurately comply with the policy. Finally, the resilience of backup copies should be regularly tested. Should regularly verify the backups of all relevant departments and create reports on their ability to restore data. Every backup will be checked quarterly to monitor the duration of the backup and optimize backup performance. The IT team will solve the problems found to reduce the risk of backup failure. A random test restores every 6 months to verify the backup whether succeed. The IT department will keep records to prove the log inspection and test restoration. Relevant staff should report on their ability to recover data quarterly. The ability to recover data should be reported to the department through the quarterly director reporting process.

**4.Network Security Controls and Administrative policy**

Status update 11/22/2020 (Bhavana Honnappa)

ACME has very well worked on following network security,

* VPN Connection – VPN is a cost-effective solution to the requirement for a work environment.
* Centralized anti-virus and anti-spyware solution – A centrally managed anti-virus is deployed in the headquarter office. All the workstations located in other places and headquarters are configured and updated from this server. If there is any anti-virus found in the workstation it is reported back to the server. This eases down the burden on the network administrators.
* Ingress & egress filtering – This is used as the first level of determination of what is allowed in and what is out of the protected network from any other network that is connected. It is implemented both in Internet firewall and Internet router.
* Protection of a database server - This database server contains information about the members of this organization. This is certainly important to protect information from unauthorized access.
* Connection to Consolidated Industries – this is accomplished by a double-firewalled ethernet connection. The consolidated and ACME network both exist in the same physical facility, but still owned and controlled by different companies.

However, there is some weakness in the network security in order to minimize risk and to ensure confidentiality of data integrity of data and availability of resources. (mentioned below)

* Loose firewalls - there several rules which allow access that is not required for the business and sometimes might be completely inappropriate.
* Intrusion prevention/detection – Currently, there is no intrusion prevention or detection built into the network. the problem is that there is no knowledge of what is happening on the network
* Wireless Architecture – As wireless access points appear in the network architecture; it has become a regular and expected service. Secure wireless network access should be a priority for any organization.
* Network segmentation – The trading group is an important part of business operation. The direct internal connection is provided to the partners, which is not a good practice.

Proposed changes:

Security policy - The first change that must be done is the adoption and creation of an information security policy. The policy will be defined through meetings with the division and executive directors. The objective is to define what is acceptable and excepted. Also, the services that are not acceptable should be defined. Once the draft policies are defined, they are reviewed by the CEO for his/her agreement. Following the sign-off by the CEO, the policies will be circulated to the employees and will be used as the basis for network and computer configurations.

Segmentation - Segmentation of the network should be addressed. The VLAN’s are in preparation for the wireless architecture modification. This gives the immediate benefit of separating the trading network traffic from corporate traffic.

Intrusion Detection – Both host and network intrusion detection should be implemented. The network intrusion looks for the packets on the wire and a host intrusion watches the actual server for signs of compromise

Wireless – improvements must be made to wireless infrastructure in the organization. This will build upon the work that has to be performed in the segmentation portion of these recommendations. The infrastructure has to be re-designed to allow authenticated access to the internal networks and unauthenticated access to the internet.

**5.System Hardening and Securing Policy**

Background: Since Acme uses a variety of on-prem and cloud systems, the policy audit is going to leverage vendor-specific hardening guidance, appropriate guidance from the DISA STIG hardening guide, and CIS Benchmark Hardening guidance, per Acme’s Information Security Policy. Based on interviews that we have conducted with Acme and documentation received related to their asset inventory, we have determined that the following systems are in-scope related to the System Hardening and Security Policy audit:

* Azure – services related to cloud services authentication
* AWS – compute, storage, and other app-hosting services
* Windows – servers and employee workstations
* macOS – employee workstations
* Linux (RHEL) – various on-prem and cloud servers
* Perimeter Security Devices – Firewall, IDS/IPS, other SIEM type infrastructure

The audit itself will be utilizing an audit matrix based on applicable ISO/IEC 27001:2013, which contains the specific audit criteria and any findings related to the review. *See Appendix A for the detailed results related to the policy audit.* Observations Summary: While Acme had a defined security policy pertaining to system hardening and securing, we identified several findings related to the required procedures and the detailed system alignment audit:

* The macOS hardening and securing procedure was missing from the Information Technology Groups SharePoint site. Additionally, the team was unable to locate this procedure during an extensive search. Recommendation: Locate or develop a new MacOS hardening and securing standard based on the latest DISA STIG and CIS Benchmark.
* Per the Information Security Policy, the Information Technology group is required to retain a 3rd party to conduct an audit of compliance at least annually. However, an audit has not been conducted in over five years. Recommendation: While this audit meets the annual audit requirement, IT Management should develop a plan to conduct these audits annually per the Acme Information Security Policy.
* Based on detailed testing, we found that 33 of the 120 systems evaluated did not fully align with the hardening and securing procedures. The Information Technology Group was unable to produce any approved exceptions. Recommendation: IT Management should develop a project plan to complete a 100% compliance check for all production systems to ensure alignment with Acme’s policies and procedures.

**6.Backup Policy**

Backup and Recovery Policy 11/22/2020(Sreelekha)   
Backup for Acme systems is for protecting the organization's important businesses and operational systems.

The System backup is necessary for all the business, data systems, and infrastructures. In any significant disaster, such as loss of data center or system, business-critical systems can be

restored within a reasonable period if a backup is ensured.

Keeping in mind about the company, Acme requires all data to be saved in keeping with the subsequent policies, which includes:

1 Maintaining complete records on what data and systems are being backed up.

2 Schedules for all backup files must be recorded and maintained.

3 Backup media is clearly labeled with a specified identity.

4 library tapes must be barcoded, where tape media is placed or held within a data center.

5 Backups are not stored within the same building as the live data or system. Acme should strive to ensure geographically diverse locations between the first data/systems and their backup.

6 Frequent testing is done on Data and system recovery processes. the maximum period between tests should not exceed three months. Testing of recovery procedures must be undertaken to confirm that backup data are often used to re-instate data in an emergency or disaster situation. A record of backup testing must be maintained. Where a natural data or system recovery is required this will be used to contribute towards the testing process, provided details are recorded.

7 Maintain Recovery procedures for the restoration of data.

8 Records regarding points 1–6 above must be managed and retained for audit purposes.

9 All users must make sure that important organizational and confidential data is stored on a recognized Acme data server and not on personal computers or workstations as these do not seem to be secured (not backed up).

Backup frequency will be determined by the company that the backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

Expiration of Backup Media

backup medias like magnetic tapes have limited functional lifespan. The media can no longer be considered dependable after certain time. When backup media is kept into service, the date must be recorded on the media.

While determining the time required for backup retention, the company determines what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The company takes steps to determine and meet all requirements.

Full backups and Incremental Backups are frequently saved foe every 2 weeks.

Backup Storage is another significant issue. Backups contain critical, and often confidential, company data, precautions must be taken that are commensurate to the type of data being stored.

**7.Software Development Management Policy-Anil Erturk**

Software security consists of three parts.

- Programming

- Processing

- Access

To have a secure programming environment, the company needs to have proper physical and password protection for servers and mainframes. Physical access security can come in the form of electronic badges and badge readers, security guards, choke points, and security cameras. Physical security is important to ensure the CIA of the software and data against internal and external threats.

To make sure the processing environment is secure, procedures and monitoring of input of falsified or erroneous data, incomplete processing, duplicate transactions, and untimely processing are in place.

Cyber-attacks focus on getting unauthorized access which can be internal or external. It is important to change system access passwords regularly and be able to track access and changes so the company is able to identify who made what changes. All activities should be logged. Remote access should also be controlled. Setting up firewalls and password protection to on-line data changes will help protect us against unauthorized remote attacks.

Segregation of duties and principle of least privilege are important for ensuring the CIA. Ensuring that people who develop the programs are not the ones who are authorized to pull it into production is key to preventing unauthorized programs into the production environment where they can be used to perpetrate fraud.

**3.** **APPENDIX**

**APPENDIX – A**

**(System Hardening and Securing Policy Audit – Relevant Controls)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27001 Framework  Section** | **Subject** | **Control** | **Testing & Observations** |
| **A.5 Information security policies** | | | |
| A.5.1.1 | Policies for information security | A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties. | Inquired of John Doe, Director of IT, noting that a formal Acme IT Security Policy has been documented that identifies system and hardening and securing requirements for the organization. This policy is reviewed annually during an Enterprise Change Management Board (CAB) and must be approved by the Director of IT, Legal, and the CTO. Ad-hoc updates are made based on any outcomes related to security incidents.  Observations: None |
| A.5.1.2 | Review of the information security policy | The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. | Inspected the Acme IT Security Policy (*see A-XXXX Policy.doc*), noting that the policy was last reviewed and approved by the Director of IT, Legal and CTO, on 2/7/2020. Also noted that the security policy stated specific requirements related to system hardening and securing. Specifically, the policy states that the Information Technology group will create golden images and other systems/device hardening procedures based on the DISA STIG hardening guide and appropriate CIS benchmarks. These specific requirements are outlined in one or more procedures maintained by the Information Technology group. The policy also requires that adherence to these requirements be audited by a 3rd party, at least annually.  Observations: None |
| **A.12.1.1 Operational Procedures and Responsibilities** | | | |
| A.12.1.1 | Documented operating procedures | Operating procedures shall be documented and made available to all users who need them. | Inquired of John Doe, Director of IT, noting that all operating procedures related to system hardening and securing policies are stored on the Information Technology group’s SharePoint page. All employees within the organization have read access to these documents, and access to modify is restricted to the Director of IT and the owner of the specific process, platform, or system. This enables them to keep documentation updated based on changes to the environment or lessons learned. **Mr. Doe also advised that while there is an annual requirement to validate adherence to the security policy, this is the first audit in at least five years.**  Inspected the system hardening and securing procedures located on the Information Technology group’s SharePoint page (see A-XXXX.aspx, noting that hardening and securing procedures have been created for: Azure, AWS, Windows, Linux, and perimeter security devices. The procedures were also updated within the last year and appear to be relevant based on the asset and system inventory we received. **However, based on this review, it was noted that a procedure related to macOS was missing. Mr. Doe advised that he was unable to locate this procedure.** It was also noted that the procedures aligned with the most current STIG and CIS guidance.  **Based on detailed testing that consisted of randomly selecting 20 devices/platform types from the system inventory (120 total), it was noted that there were 33 failures, where one or more hardening requirements were not met (See A-XXXX.xlsx for details). Upon inquiry with Mr. Doe about exceptions, he advised that exceptions were not retained, and he did not have any further information.** |

**4.** **REFERENCES**

ISO/IEC 27001:2013. (2019, June 03). <https://www.iso.org/standard/54534.html>

National Institute of Standards and Technology (2014). Security and Privacy Controls for Federal Information Systems and Organizations (Department of Commerce, Washington, D.C) Special Publication 800-53. <https://www.nist.gov/publications/summary-nist-sp-800-53-revision-4-security-and-privacy-controls-federal-information>

National Institute of Standards and Technology (2001). Security Requirements for Cryptographic Modules. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS PUBS) 140-2. <https://doi.org/10.6028/nist.fips.140-2>

Resolver (2020). Resolver Corporate Back Up & Restore Policy. <https://www.resolver.com/trust/policies/a-12-3-resolver-corporate-backup-restore-policy/>

Thakkar, J. (2020, November 03). 12 Enterprise Encryption Key Management Best Practices. <https://www.thesslstore.com/blog/12-enterprise-encryption-key-management-best-> practices/

Wikipedia (2020). Information security audit. <https://en.wikipedia.org/wiki/Information_security_audit#Auditing_application_security>

Department Of IT, Govt. Of NCT Of Delhi. CDAC, Noida. (n.d.) IT Security & Audit Policy. <http://www.nsit.ac.in/static/documents/notices/itsa_policy.pdf>

Giac.org. 2020.https://www.giac.org/paper/gslc/61/acme-corpnetwork-security-design-study-recommendations/100197

Solomon, Michael G. (© 2014) Security strategies in windows platforms and applications, second edition. [Skillsoft version] Available from <https://login.proxy.cityu.edu/sso/skillport?context=69816>