**SK Co. IT Security Audit Proposal**

Sweta Kharel

Central Washington University

Information Technology and Administrative Management

**Table of Contents**

**Title Page****0**

**Table of Contents****1**

**Audit Proposal****2**

**Entity Level Control****3**

**Data Center Control****7**

**Database****9**

**Web Server 10**

**Network Devices** **11**

**Disaster Preparedness Plan****12**

[**References**](#_gjdgxs) **13**

Audit Proposal

February 1, 2024

Ellensburg, WA 98926

Dear Mr. Jose,

I appreciate you providing me with the opportunity to present a proposal to do an informal audit of important IT security controls and policies at SK Co. has recently made a few changes in the privacy policies and regulations, and a review of certain controls will help to prepare a formal audit verifying SK Co.’s compliance to General Data Protection Regulation (GDPR) in the organization. The audit is important to maintain quality operations in the organization which provides additional help in reducing potential risks to avoid a heavy loss to the organization in case of exposed vulnerability getting breached.

This will be an informal audit prepared to assess and analyze the security system of IT infrastructure in the organization. Auditors will be reviewing network systems, security controls and present recommendations to strengthen the system by reducing weak spots discovered in the process. SK Co. will further present the proposal to the company’s board to adjust present controls and strengthen network infrastructure. The Board will have complete control to make decisions to accept, mitigate, or transfer the audit’s recommended risks.

Thank you,

Sweta Kharel,

CISO

SK Co. IT Security Audit Proposal

Below is an outline that describes the audit proposal for the SK Co. IT audit. Audit includes entity-level controls, data center controls, cloud infrastructure controls, database controls, networking devices, web servers, and disaster preparedness plans. Data Center control assesses furthermore areas such as physical security, environmental controls, power and electricity, fire suppression, data center operations, and system resiliency. Entity-level control auditing helps increase the efficiency of organizational security by discovering and reducing risk.

**Entity Level Control**

Entity Level Control will be the first area that will be analyzed in the Audit. Entity-level control will address issues such as asset management software and hardware management, and system configuration. It will investigate the areas meeting industrial standards of policies, standards, and procedures.

Entity-level control is the high-level control including policies, rules, and procedures designed and executed by board members, management team, and employees to address the risks regarding the organization's financial statement. Entity-level control is generally pervasive, meaning that it is spread across every part of the organization and protects the whole organization by making everyone in the organization accountable for their behaviors and actions including stakeholders. Entity-level control provides governance of the company’s entire technological environment, so it's important to build strong entity-level control to form a solid IT environment foundation.

A good entity-level control displays IT management’s seriousness and dedication to risk management, internal controls, and governance. Upper management needs to communicate and set a persistent tone about the value and rewards of internal controls, governance, and risk management. Failure to do so will lead to inconsistencies in lower departments resulting in them focusing the behaviors such as: cutting costs, managing their budgets, and meeting schedules with minimal consideration of internal controls. This causes weak management of controls in the organization causing conflicts regarding the authority of decision-making and confusions of work and responsibilities. Poorly structured IT organization results in incompletion of duties, fraudulent activities, and lack of delivery of quality IT services that affect the company’s overall efficiency and performance along with open security vulnerabilities. (Davis, 213).

Auditing of entity-level controls involves several steps starting with reviewing the entire IT structure of the organization to deliver clear assignments of responsibilities and authority with proper segregation of work in the IT operations department. The company must review the organization’s charts to ensure it indicates clear reporting structures and specifics of work responsibilities vary depending upon the company (Davis, 215). However, every company must have segregated responsibilities for the indication, authorization, input, process, and checking of data so that the possibilities of fraudulent activities are limited. Following the process, will prevent an individual from subverting critical processes as a single person by themself will not have access to create, authorize, and hide evidence of fraudulent behavior.

It is also important that programmers responsible for running and maintaining support for systems must not have access to directly modify the production code. But programmers with responsibility for running and maintenance of systems must be distinct from the ones handling It operations support like networks, operating systems, and data centers (Davis, 513). Effective IT security will ensure a baseline of job expectations so information security will set policies and monitor compliance with them.

Strategic planning of IT organization and ensuring the plan aligns with the business strategy helps SK Co to achieve its long-term business goal with effective results. SK Co should regularly monitor the organization's progress through its strategic plan to keep the company aware of changes in the environment and market needs so that the company can plan and react to the upcoming needs of the business (Davis, 213). For the same reason, determining the existence of technological and application techniques, and roadmaps are crucial through evaluation of the process for long-term technical planning.

Similarly, SK Co should review performance measurements and indicators for IT, ensuring the stakeholders approve the metrics and processes. The performance measurement should be achieved on daily activities to track performance against budget, service level agreements, and other operational needs. This helps companies to determine the acceptable level of service by IT organizations (Davis, 425). It is also crucial that IT organizations review the process for approval and prioritization of new projects to determine the adequate developmental and system acquisition projects with proper approval. Management and stakeholders should ensure the review of project status and budget constantly throughout the project to meet the expected project goal.

If there aren't established and upheld standards, projects are likely to proceed without discipline, resulting in quality problems in both purchased and developed products, and causing unnecessary diversity within the IT environment. It is crucial to assess standards that govern the implementation of IT projects and ensure the quality of products created or procured by the IT department. Additionally, it is essential to determine the methods through which these standards are communicated and upheld (Davis, 422). In areas such as project management, software development, system configuration, hardware and software, and quality assurance standards.

IT infrastructure consists of several risks in physical and virtual network environments. Assessing risks involves examining various risk factors by monitoring internal controls within the IT environment, conducting internal audits and self-assessments, performing formal assessments of threats and risks concerning vital data centers and systems, reviewing strategic IT plans and technical roadmaps periodically to identify risks to their realization, and overseeing compliance with information security policies and other pertinent IT policies (Davis, 422).

Configuration change management guarantees that modifications to systems are regulated and monitored to minimize the likelihood of system failures. This process encompasses planning, scheduling, implementing, and monitoring changes to systems to mitigate potential risks to the environment. One aspect of entity-level control involves guaranteeing that the configuration management procedures encompass various processes, including requesting changes, determining the details of proposed changes, prioritizing and approving them, scheduling approved changes, testing and approving changes before implementation, communicating planned changes, executing changes, and reverting changes that fail to function as intended.

Likewise, organizational assets constitute a significant aspect of IT infrastructures, necessitating thorough review and assessment of policies and procedures governing procurement and movement. Asset management involves controlling, tracking, and reporting organizational assets to enable proper accounting for them. Effective asset management is crucial for preventing unnecessary expenses and minimizing the risk of hardware failure. It involves tracking and accounting for computer hardware assets such as desktops, laptops, and servers to avoid duplicate purchases and unnecessary lease expenses (Davis, 467). Proper asset management also helps identify end-of-life equipment conditions and reduces the likelihood of theft by ensuring all equipment is adequately tracked. Asset management includes examining and evaluating the policies as well as the procedures of the company to confirm they address different facets like acquiring assets, monitoring them, keeping an up-to-date inventory, and managing the process of moving and disposing of assets.

**Data Center Control**

A data center serves as a facility intended for hosting an organization's essential systems, encompassing computer hardware, operating systems, and applications. These applications play a role in facilitating various business operations like order processing, customer relationship management (CRM), and accounting. Given their foundational role, data center facilities require adequate controls to mitigate risks effectively (Davis, 337). The company will be housing 2 data centers that will be in Spokane, Washington. To ensure our data center is protected and implementing the highest security practices, our IT audit will be overseeing these major areas:

**Physical Security**

Data centers integrate various facility-based controls that require thorough evaluation. Our audit team will evaluate the efficiency of all installed physical obstacles, including access control protocols, doors, walls, authentication systems, along with security guard routines, and biometric readers. Additionally, we'll verify the adequacy of burglar alarms and surveillance systems in safeguarding the data center and ensuring access is appropriately limited (Davis, 340). Lastly, we'll review the placement of essential operational systems and equipment located in the data center.

**Environmental controls**

We will inspect the data center maintaining secure protocols to avoid environmental hazards such as flood, extreme heat, and humidity. Data centers should install alarm systems such as burglar alarms, water alarms, fire alarms, humidity alarms, and chemical or gas alarms to avoid environmental hazards.

**Power and electricity**

Fluctuations in power, such as spikes, surges, sags, brownouts, and blackouts, pose threats to computer hardware and can lead to system failures. To minimize these risks, data centers should implement power redundancy measures, including grounding, battery backup systems (UPSs), power conditioning, and generators (Davis, 338).

**Fire suppression**

Due to the extensive electrical infrastructure present, fire poses a significant risk to data centers. As a result, data centers should employ advanced fire suppression systems and ensure an adequate supply of fire extinguishers which commonly consist of two types: water-based and gas-based systems (Davis, 339).

**Data center operations**

While data centers are primarily automated with operating staff, they will require policies, plans, and procedures governing data center operations. In our Audit, we will assess that they encompass areas like physical access control, facility and equipment planning, system and facility monitoring, tracking, as well as backup in case of outages, alarm conditions, and emergencies (Davis, 337).

**System resiliency**

As computer systems within data centers are utilized for automating business processes, their availability is crucial during business operations. To ensure this availability, data centers should implement the best protective controls aimed at safeguarding power, the IT environment, and the networking system (Davis, 342).

**Data Backup and Restoration**

Backup procedures are essential for data protection, involving schedules, tape rotations, and offsite storage. The frequency of backups depends on the recovery point objective (RPO), ranging from real-time to monthly backups. Typically, backup schedules should span one week, with full backups on weekends and incremental backups during the week. Tape rotations typically last six to ten weeks, allowing retrieval of older file versions if necessary to address issues like file corruption. We will make sure every Data Center has a data backup and restoration system in case of accidents (Davis, 343).

**Database**

This SK Co. has 3 databases in Amazon Relational Database Service. Each database should be thoroughly audited and analyzed. The database organizes data records and their relationships in tables known as indexes. An audit should thoroughly examine different aspects such as the perimeter, operating system, and policies. It's important for the audit to acquire the database version and compare it against corporate policy requirements, confirm that the database is supported by the vendor, and verify proper access restrictions to the operating system and registry keys used by the database (Davis, 760).

Likewise, our team will examine the database to assess the procedures involved in creating user accounts, ensuring they are established solely for legitimate business purposes and with suitable authorization. This process aids in establishing efficient controls for granting and revoking access to the database, thereby restricting unnecessary access to its resources. We will make sure the database includes robust password strength and management capabilities to prevent passwords and the authentication system from becoming potential weak points in the system's security.

We will ensure that network encryption is correctly implemented for databases, securing data both during transmission and when stored (Davis, 769). Additionally, we will examine the utilization of database auditing activity monitoring, and capacity management, and assess performance monitoring to ensure it meets current and future business needs.

**Web Server**

SK Co. Will be using a cloud-based AWS web server, and the web server will be audited starting by testing the operating system of the host. We will confirm that the web server is operating on a dedicated logical system, separated from all other essential software and applications, and check that the server is completely patched and updated with the latest approved code. We will also check that services, APIs, and objects of less priority are disabled or removed. If they are still running, they must be operated at minimal privileges. We will also ensure that relevant port protocols will have the permit for web server access.

We will make sure that network protection such as Web Application Firewall, Reverse Proxy, Denial of Service prevention, and bot defenses are running in the server to avoid any disruptions in the smooth operation of the web server. We will verify that the web interface does not have information, such as version details and directory listings exposed by running some vulnerability assessment tests.

**Network Devices**

Networking serves as the primary means of transmitting information among companies, clients, and end-users. Ensuring that networking infrastructures, including network firewalls, switches, and routers, are optimized is crucial for safeguarding overall data involved in data transmission (Davis, 668). Switches, Routers, and firewalls work to facilitate data transfer securely between the networks, safeguarding both end-users and data. Wireless networks further expand these functionalities, catering to mobile users in locations where traditional infrastructure may be impractical or expensive. Networking consists of several networking and wireless devices, Internet protocols, GUIs, CLIs, networking layers, and several other components to make secure communication successful.

**Switches**

A network switch manages communications between devices by utilizing the MAC address of the destination host, operating at OSI layer 2, to transmit data directly to the intended recipient (Davis, 670). In our audit, we will ensure that administrators refrain from using VLAN, assess the implementation of trunk auto-negotiation, and confirm the activation of Spanning Tree Protocol attack mitigation measures.

**Routers**

Routers establish connections and direct data between networks by utilizing layer 3 network addresses, typically IP addresses. They manage the flow of data between different networks, forwarding packets either to other routers or to locally connected switches. We will audit the information (Davis, 674). We will utilize tools like encryption, authentication, firewalls, and intrusion detection systems to audit the security of routers. We will confirm that any inactive interfaces on the router are deactivated and verify that the router is set up to retain all core dumps. Additionally, we will ensure that all routing updates are authenticated.

**Firewalls**

Network firewalls are primarily intended to act as a barrier, setting up regulations to manage the movement of traffic. They create a secure network zone that can be accessed only by specific systems or through particular methods. Reviewing firewalls entails verifying that by default, all packets are rejected, except for those originating from and destined for addresses and ports explicitly defined (Davis, 674).. Our team will verify the filtering of unidentified internal and external IP addresses and assess firewall rule sets to ensure suitable protection. Additionally, we will review the implementation of intrusion detection systems or monitoring technologies for packet security and evaluate layer 7 application layer protection use.

**Disaster Preparedness Plan**

Regardless of the best security practices, there is still always the possibility of disaster, so every Data Center should have a disaster preparedness plan that includes data backup and restoration, and disaster recovery planning. We will confirm the existence of a Disaster Recovery Plan (DRP) for the data center, ensure that employees are knowledgeable about their responsibilities in executing it, and verify that the plan undergoes regular updates and testing.

# **References**

Davis, C., Schiller, M., & Wheeler, K. (2011). IT auditing: Using controls to protect  
 information assets (2nd ed.). New York, NY: McGraw-Hill

Thu. (2022, September 22). *Entity-level controls: The importance of setting the tone*. KnowledgeLeader. https://www.knowledgeleader.com/blog/entity-level-controls-importance-setting-tone#:~:text=Entity%2Dlevel%20controls%20are%20policies,rank%2Dand%2Dfile%20employees.

*What is a Firewall? types, history, methods & importance*. NordLayer. (n.d.). https://nordlayer.com/learn/firewall/what-is-firewall/?gad\_source=1&gclid=Cj0KCQjw-r-vBhC-ARIsAGgUO2A8ts\_lN-2x1Ppzd6xmAtelkAzULtXTveN4vDVJ-xjTGKL3tq5gybEaAi0zEALw\_wcB