INFO 6008 - S2023 Assignment 2

Gihan Shamike Liyanage

1142109

IT Auditing

09/06/2023

1. From the above article and from what you know of COBIT, NIST or other frameworks, how important are policies and procedures to a company? Why is Policy different from procedure?

Policies and procedures are important for organizations as they provide guidelines and instructions for employees to achieve objectives and maintain consistency. Policies set high-level goals, principles, and standards, guiding decision-making and defining the organization's approach. They ensure employees understand values and rules. Procedures, on the other hand, offer detailed step-by-step instructions for executing tasks, reducing errors and inefficiencies. Policies provide the "what" and "why," while procedures focus on the "how" and "when." Policies are broader and enduring, while procedures are more specific and can be revised frequently. COBIT and NIST frameworks emphasize the importance of policies and procedures in achieving compliance, operational efficiency, risk mitigation, and effective governance of information and technology assets. Well-defined policies and procedures align organizations with industry standards and regulatory requirements.

1. Do you believe the Central Bank of Bangladesh has a security framework like NIST or ISO 27001 etc. in place? Explain your answer.

Certain factors mentioned in the article indicate potential gaps in the bank's security practices. The absence of a firewall, the use of inexpensive switches, and the lack of proper segregation in the SWIFT room raise concerns about the bank's adherence to recognized security standards. These vulnerabilities indicate possible weaknesses in network security controls, secure infrastructure investment, and access controls. According to these factors I believe that the Central Bank of Bangladesh did not have any security framework in place when the incident occurred.

1. Do you believe there were unethical players at the Central Bank of Bangladesh? Explain your answer.

The article has highlighted security shortcomings at the bank, such as the absence of a firewall and the use of cheap switches, which could indicate negligence or lack of adherence to recognized security practices. These vulnerabilities suggest potential shortcomings in governance, risk management, and the implementation of appropriate controls, which could be seen as a failure of ethical responsibility. Based on these factors it is possible that there might have been unethical individuals within the Central Bank of Bangladesh at that particular time.

1. In your opinion, which Risk Treatment Plan did the Central Bank of Bangladesh apply? Explain your reasoning.

As mentioned in the article, the Central Bank of Bangladesh's security shortcomings include the lack of a firewall and the use of inexpensive switches. These issues indicate potential deficiencies in risk management and the implementation of adequate controls. The absence of a firewall indicates a failure to address unauthorized access and network attacks effectively. Furthermore, the decision to use cheap switches indicates a potential prioritization of cost savings over secure infrastructure. These observations indicate that the bank may have adopted a risk acceptance or risk avoidance approach, neglecting the implementation of robust risk treatment measures. This is only an assumption and a thorough analysis of the bank's internal risk management processes would be necessary to determine their specific risk treatment plan more accurately. However, the mentioned weaknesses in their approach highlight concerns regarding their information security controls and risk management practices. According to my perspective organizations especially those handling sensitive financial information, should prioritize the mitigation of known risks and allocate necessary resources to establish robust security frameworks.

1. As a freshly minted auditor, what would be your recommendation? Provide only one and explain why.

As a newly appointed auditor reviewing the security vulnerabilities highlighted in the article, I would recommend that the Central Bank of Bangladesh undertake a comprehensive risk assessment and implement a robust information security framework such as ISO 27001. This internationally recognized standard for information security management systems would provide a structured approach to identifying, assessing, and mitigating information security risks.

Implementing ISO 27001 would allow the bank to establish a systematic information security management system, encompassing policies, procedures, guidelines, and controls. Through this framework, the bank could ensure that security measures are properly documented, implemented, and monitored. ISO 27001 also emphasizes the importance of continuous improvement, enabling the bank to regularly review and update security measures based on evolving threats. By adhering to ISO 27001, the bank would demonstrate its commitment to safeguarding sensitive data and customer information. It would enhance stakeholder confidence, including customers, partners, and regulators, and facilitate compliance with relevant laws and regulations. Furthermore, the risk assessment process would help the bank identify and prioritize potential threats and vulnerabilities specific to its operations, enabling informed decision-making and allocation of resources. Implementing ISO 27001 and conducting a comprehensive risk assessment would significantly enhance the bank's information security posture, mitigate vulnerabilities, and improve the resilience of its systems against cyber threats.