Module Code & Module Title

CC5052NI Risk, Crisis & Security Management

Assessment Weightage & Type

50% Individual Coursework

Year and Semester

2021-22 Autumn

Student Name: Sarthak Bikram Rana

London Met ID: 20049228

College ID: NP01NT4S210129

Assignment Due Date: 3rd January 2022

Assignment Submission Date: 3rd January 2022

Word Count (Where Required): 1916

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

MARKING SCHEME

Items	***Marks Awarded***	***Feedback***
1) Technical content [Maximum 85 Marks]:		
Rationale and Objectives of the chosen topic [Maximum 20 Marks]:		
Abstract Content [Maximum 10 Marks]:		
Literature Review [Maximum 25 Marks]: ● Relevance of the resources (i.e. in terms of useful of the resources referred to within the context of the topic) (10) ● breadth and depth of the content reviewed, In-depth analysis **(15)**		
Identification of Issues (use of examples / case studies), Analysis and Reflection: [Maximum 30 Marks] ● Identify issues relating to the techniques being reviewed, compare and analyse **(15)** ● Reflection on what you have learnt about these techniques by undertaking this task. **(15)**		
2) Report Format [Maximum 15 Marks]: ● Overall structure – organization of material; quality of documentation; The report should have an abstract, introduction, main body, conclusions, references, face page, contents page and page number etc. **(8)**		

● citing the correct reference(s) in appropriate sections of the report using a chosen referencing style **(7)**		

Acknowledgement

This is the first coursework in the Risk, Crisis and Security Management module, in which we were given six different topics to choose from and then do the coursework on one of them. I chose the topic of information security audit for this coursework and conducted two case studies on it. I had to undertake research on the issue for my coursework by looking at a variety of related articles, journals, reports and websites.

Finally, I'd like to express my gratitude to Mr. Saroj Lamichhane, my respected module leader and Mr. Sandesh Gurung, my respected tutor for introducing me to the topic of information security audit, introducing me to the sci-hub, where I was able to access various journals and reports to gain a better understanding of the topic, and helping me by reviewing my coursework at various points.

Abstract

The Information Security audit is the focus of this coursework, and detailed study is conducted on the topic through various reports, journals, articles, and websites. The term Information Security audit, its history, current scenario and numerous audit phases are all detailed in the background part. Finally, two different case studies are conducted, each with an in-depth investigation and a significant role for information security audit.

Table of Contents

List of Figures

1. Introduction

In today's world, financial institutions such as banks and organizations play a critical role in a country's economic growth, stability, and long-term viability. As a result of its rapid growth, they are now exposed to a greater risk. To reduce these risks, the organization must conduct an information security audit to detect loopholes, flaws, and risk factors, which is the work and responsibility of the information system management.

An information security audit is a symmetric assessment of a company's information system's security by determining how well it complies with a set of predetermined standards. It is possible to secure the system's physical design and environment, software, information handling processes, and user habits by executing the audit (Tierney, 2020).

This audit strategy includes the monitoring of an organization's transactions, database management system, plans and policies, as well as human resources. In practice, software/application audits, public key infrastructure (PKI) audits, database audits, and policy audits are some of the most common types of IS audits (Bajracharya, 2021).

Surprisingly, the concept of information security auditing was first introduced in the mid-1960s. Its technicalities have progressed gradually, in full agreement with the growth of modern technology. Since 2019, the government of numerous countries including Nepal has made the IS audit mandatory for certain types of businesses (Bajracharya, 2021).

1.1 Aims and Objectives

The main aim of this report is to understand what an Information System Audit is, why it is important and how it can help information system managers efficiently fulfill their tasks and responsibilities in order to achieve the organization's goals while also improving proper decision-making and data and information security.

To fulfill this aim the following objectives are required:

- To conduct research on the topic of Information Security Audit.
- To gain the fundamental knowledge about it through using a variety of related news, journals, papers and websites.
- To consult with teachers, field related experts and friends about the topic.
- To figure out several issues that may arise in Information Security audit through real world case analysis.
- To give solution to the real world case about how Information Security audit can minimize it.

2. Background

2.1 History

The concept of Information Security audit was introduced during the mid-1960s. As the use of computers in businesses grew, so did the need for auditors to become familiar with business EDP ideas. With the rise of computer use comes the emergence of a variety of accounting systems. The Electronic Data Processing Auditors Association was founded about this period by EDP auditors (EDPAA) and then the EDPAA was renamed the Information Systems Audit and Control Association (ISACA) in 1994 (Karl de Leeuw, 2007).

2.2 Current Scenario

An information system audit is a way to keep track of how information is managed, what they do with it, and what system they use, whether it's in a large or small company. This audit strategy includes the monitoring of an organization's transactions, database management system, plans and policies, as well as human resources. Its technicalities have progressed gradually, in lockstep with the growth of modern technology (Umar, 2003).

Since 2019, the government of numerous nations including Nepal has made the IS audit mandatory for certain types of businesses. The Nepal Rastra Bank's IT policy and IT Guidelines guide IS audit regulations (2012). According to the guidelines, an organization must take the necessary steps to make its employees, contractors and consultants aware of the company's IS policy and to ensure that they follow it, which can be accomplished through proper employment information, employee agreements, policy awareness, and acknowledgment (Bajracharya, 2021).

Certified listed companies such as Eminence Ways Pvt Ltd and Biz Serve IT Pvt Ltd are two government-approved Nepali cybersecurity companies that are permitted to conduct external IS audits (Bajracharya, 2021).

2.3 Introduction to Information Security Audit

An Information Technology (IT) audit is the process of testing and analyzing an organization's information technology infrastructure, policies, procedures, applications, data use, and management before moving on to Information Security Audit (Harvaard University, 2021).

When it comes to Information Security (IS) Audits, they are a special type of audit that entails meticulous planning, designing audit programs, and documenting them in order to assess an organization's Information Security policies and standards in order to ensure quality.

The certified IS auditor conducts the information security (IS) audit by following the four procedure described below,

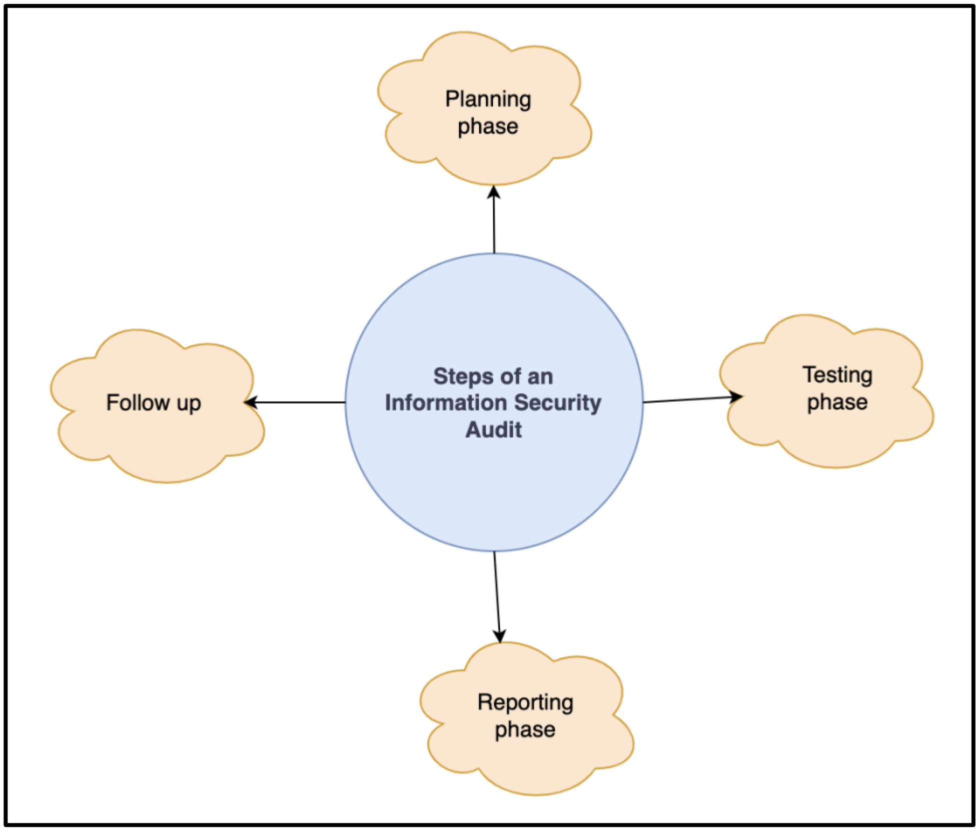

Figure 1: Steps of an Information Security audit.

2.3.1 Planning Phase

The auditor must get a thorough understanding of the organization's terms and policies during the planning phase of an Information Security (IS) audit. The auditor should meet with IT management to discover potential areas of concern, assess the organization's policies, processes, and disaster recovery plan, and evaluate all IT budget and systems planning documentation throughout audit planning and preparation (Wiki Educator, 2016).

The following phase is to define the audit objectives and gather the data needed for the audit, which involves conducting a review of a cooperating data centre after the auditor has defined the data centre audit objectives. Multiple aspects relating to data centre operations and activities are taken into account by auditors in order to identify audit risks in the operating environment and assess the controls in place to minimize such risks. Finally, the planning phase includes the creation of an audit checklist (Wiki Educator, 2016).

2.3.2 Testing Phase

The testing phase is when the auditor gathers evidence to prove that the data centre audit objectives have been met. During this process, the auditor visits the data centre and watches the processes and operations that are carried out there. Meeting with the site managers and questioning them is also part of the procedure (Wiki Educator, 2016).

During the testing phase, the auditor collects a variety of data based on the audit's objectives, as well as reviewing the organization's physical security, interviewing employees, and doing vulnerability and access control assessments (Wiki Educator, 2016).

2.3.3 Reporting Phase

The third step of the Information Security (IS) Auditing is the reporting phase, in which the certified auditor creates two reports, one is a short report in which the auditor identifies immediate issues, lists some questions for the site manager and presents preliminary findings. However, this brief report does not provide in-depth information about the audit (Wiki Educator, 2016).

The auditor also creates/presents a final report on the audit that includes an introduction section that explains the audit's goals and objectives, a detailed analysis of how data was obtained, any unexpected outcomes, a detailed description of the problem and an analysis of the problem (Wiki Educator, 2016).

2.3.4 Follow up

The Information Security (IS) audit's final stage is the follow-up process, which is carried out after the audit is done. The auditor performs a follow-up process based on the organization's Management Action Plan and the entire progress is tracked during this process. They go through all of the re-testing procedures whenever a certain case arises and then the visitor's board is updated (Wiki Educator, 2016).

3. Literature Review

3.1 Case Study

The case study explains and illustrates the importance of conducting an Information Security (IS) audit, as well as the real-life issues that some organizations have experienced as a result of failing to do an Information Security (IS) audit.

3.1.1 ATM hackers exposes vulnerability of Nepali banks:

Findings:

One of the Nepal's major banks software hacking incidence occurred on August 31st 2019, Saturday night where a member of the Chinese national hackers organization named "Zhu Lianang" was caught at a Nabil Bank ATM booth in Durbar Marg while attempting to withdraw cash using cloned debit cards. Following the interrogation, the police seized Rs 12.6 lakhs and $10,000, as well as 132 fake visa debit cards and 17 genuine visa debit cards. They also came to know that the group has already stolen more than Rs 34 lakhs and INR 10.5 lakhs (Shuvam Dhungana, 2019).

The ATM cash-out attack, in which the hackers breach a bank or payment processor's system developed by Nepal Rastra Bank that is known as Nepal Electronic Payment Systems (NEPS). This is an interface that allows the transaction of all the money deposited in the bank using cards issued by other members of the banks was carried out by the hackers using both fake and genuine cards in order to withdraw huge amount of money in a short amount of time (Shuvam Dhungana, 2019).

The event was mostly caused by the Nepal Rastra Bank's refusal to enhance their digital security measures and follow its 2015-2016 Monetary Policy, which required all Nepali banks to switch to microchip-equipped ATM cards since they are safer than those with magnetic strips. Following the investigation, Nepal Rastra Bank spokesperson "Laxmi Parpanna Niroula" revealed that the incident arose due to a lack of care in their digital security procedures (Shuvam Dhungana, 2019).

Analysis:

Before any issue occurred, the Nepal Rastra Bank should have conducted an Information Security audit to detect loopholes and weaknesses in its information system, identify likely sources of threats, assess information misuse and identify high-risk factors.

During the planning phase of the Information Security audit, the auditor would have been presented to the bank's 2015-2016 Monetary Policy, which had already directed all Nepali banks to replace their magnetic strip cards with microchip-equipped cards. The auditor would have known from the testing phase that the Nepal Electronic Payment Systems (NEPS) is out of date, posing a significant risk to other banks security measures and due to which the ATM incident occurred.

The auditor would have listed all of NEPS flaws and vulnerabilities in the final assessment report from the reporting phase of the audit, from which the governor of the Nepal Rastra Bank would have gotten the idea to upgrade their digital security measures and NEPS system, which is part of the follow-up phase.

3.1.2 Foodmandu 50K user details dump:

Findings:

Foodmandu is an online food delivery application which supply food across the Kathmandu Valley in Nepal. It faced a major data breach on March 8th 2020 by the hacker named "Mr. Mugger" which caused them the loss of 50 thousand user's data including their name, phone number, email address and more (Rizal, 2020).

The hacker tweeted that the company neglected their database security vulnerabilities which consisted their 150 thousand customers personals details. He was successful in hacking because the company had loop hole in their web application and they took the vulnerability too lightly which made it easier for the hacker to hack the system and leak the data (Rizal, 2020).

Later the foodmandu officially confirmed the data breach has occurred and they have begun working with the government's cybercrime bureau to track down the hacker. They assumed the hacker had access to the user's bank account (Rizal, 2020).

Analysis:

The data breach at Foodmandu occurred because the company had a loophole in its web application and they ignored the vulnerability, making it easy for the hacker to gain access to the system. The company should have conducted an Information Security audit in a timely manner, allowing the auditor to identify the loophole in their web application.

It would also assist the company in upgrading their digital security measures by implementing firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS), as well as strengthening their policies. If the company had already carried out the Information Security audit in past the situation would have never occurred.

We can see from the above two case studies that the incident occurred as a result of the banks and companies failure to upgrade and apply their digital security measures. If the bank and company had properly undertaken an Information Security (IS) audit, they would have been able to detect flaws and vulnerabilities in their security measures through which the hackers attacked the system, leading them to upgrade their system and policies.

4. Conclusion

Finally, the coursework has given us the opportunity to learn more about information security auditing and to define aims and objectives for this report. The term Information Security audit, as well as the four separate steps of the audit, are defined in detail in the background section to meet those aims and objectives. Aside from that, the case study shows the various issues that the bank and company encountered when the Information Security audit was not completed effectively.

References

Tierney, M., 2020. *IT Security Audits: The Key to Success.* [Online]
Available at: https://blog.netwrix.com/2020/04/09/it-security-audit/
[Accessed 23 December 2021].

Bajracharya, N., 2021. *Information system audit in Nepal: Everything you should know about - OnlineKhabar English News.* [Online]
Available at: https://english.onlinekhabar.com/information-system-audit-in-nepal-explained.html
[Accessed 24 December 2021].

Harvaard University, 2021. *What is an Information Technology (IT) audit?* | *Risk Management & Audit Services.* [Online]
Available at: https://rmas.fad.harvard.edu/faq/what-does-information-systems-audit-entail
[Accessed 27 Decemebr 2021].

Shuvam Dhungana, R. K., 2019. *Millions stolen by ATM hackers exposes vulnerability of Nepali banks.* [Online]
Available at: https://kathmandupost.com/money/2019/09/01/millions-stolen-by-atm-hackers-exposes-vulnerability-of-nepali-banks
[Accessed 30 December 2021].

Rizal, C., 2020. *Foodmandu Hacked – Foodmandu hacked.* [Online]
Available at: https://gadgettrait.com/foodmandu-hacked/
[Accessed 30 December 2021].

Wiki Educator, 2016. *Information Systems Audit Methodology - WikiEducator.* [Online]
Available at: https://wikieducator.org/Information_Systems_Audit_Methodology
[Accessed 30 December 2021].

Umar, A., 2003. Security Issues unique to the digital age. In: *Information Security and Auditing in the Digital Age.* s.l.:NGE solutions, pp. 1-8.

Karl de Leeuw, J. B., 2007. *The History of Information Security.* 1st Edition ed. s.l.:Elsevier Science B.V..

Bibliography

Bayuk, J., 2009. *Information systems audit: The basics* | *CSO Online.* [Online]
Available at: https://www.csoonline.com/article/2124025/information-systems-audit-the-basics.html
[Accessed 28 December 2021].

Edward C. Lo, M. M., 2004. *Security Audit: A Case Study,* Abbotsford: University College of the Fraser Valley.

Ana-Maria SUDUC, M. B. F. G. F., 2010. Audit for Information Systems Security. *Informatica Economica,* 14(1), pp. 43-47.

Yogesh Ghorpade, R. M., 2015. *Information Security and Audit ,* s.l.: Self Publications.

Ian Cooke, C. C. C. C. C. 5. A. a. I. C. C. C. C. F. C. D. I. F. S. S. G. B., 2020. The Components of the IT Audit Report. *ISACA journal,* 1(20), pp. 6-9.