LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5052NI Risk, Crisis & Security Management

Assessment Weightage & Type

50% Individual Coursework

Report Title - Information Security Audit

Year and Semester

2021-22 Autumn / 2021-22 Autumn

Student Name: Sujen Shrestha

London Met ID: 20049250

College ID: NP01NT4S210105

Assignment Due Date: January 3, 2022

Assignment Submission Date: December 30, 2021

Word Count: 1984

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 marks of zero will be awarded.

Abstract

There are various threats that can hamper the information system of an organization. These threats can compromise the confidentiality, integrity and availability of data and information assets of the company. As a result, the organization suffers financial crisis, legal issues, loss of reputation, loss of customers and the overall loss in business. In order to avoid such situations, an organization creates various policies, procedures, security measures and follows the internationally accepted standards. However, the various factors in the organization like change of staffs, adaptation of new technology, environmental inconsistencies and many such variables may introduce different kinds of risk in the company. Therefore, to make sure that all the policies, procedures and standards are implemented correctly so that the information of an organization are secured, the company uses a process to check the entire actions carried out by the organization. This process of evaluation and examination of all the activities performed by the organization to make sure that there are no inconsistencies in policies, technologies and the actions performed by the employees is known as Information Security Audit. The various aspects of Information Security Audit are elaborated in detail in this report.

Table of Contents

Abstract i

Table of Contents ii

Table of Figures iii

1. Introduction to Information Security Audit 1

1.1 Importance of Information Security Audit 1

1.2 Aims and Objectives 3

2. Background 4

2.1 Information Security Audit Process 4

2.1.1 Planning 4

2.1.2 Fieldwork and Documentation 5

2.1.3 Reporting and Follow-up 6

3. Literature Review 7

3.1 Case Study 7

3.1.1 Findings 8

3.1.2 Analysis 9

4. Conclusion 10

5. References 11

6. Bibliography 12

Table of Figures

Figure 1: Components of an organization: 2
Figure 2: Components of Information Security Audit 3
Figure 3: IT Audit Process 4
Figure 4: Information Security Audit Phases 6
Figure 5: Case Study of Equifax Inc 7
Figure 6: Statistics of data breach 8

1. Introduction to Information Security Audit

Information can be defined as the processed collection of data which gives detailed knowledge about any particular subject. It can be represented in the form of charts, tables, reports, etc. It is one of the most valuable assets in an organization as it allows a company to analyse its current situation and derive ways to improve their profitability. Since this asset is so important to the company, it needs to be safeguarded from any threats and vulnerabilities which may damage or destroy it. The methods and techniques created and deployed to secure critical company information against modification, disruption, destruction and observation are referred to as information security or InfoSec. In order to verify the implementation and effectiveness of these security measures, a company makes use of a process known as audit. An audit is the systematic examination which evaluates the policies and standards of an organization and whether they are strictly following it or not. The examination and evaluation of an organization's information technology infrastructure, policies, and operations is known as an Information Security Audit.

1.1 Importance of Information Security Audit

An organization possess various sensitive information about their clients and employees. This includes various personal details like address, phone number, etc. When an organization acquires such critical information, it is their responsibility to make sure that the information is secure from the people or parties which do not require them. Any organization must provide Confidentiality, Integrity and Availability (CIA) in order to provide information security. These three factors are important because these elements help a company to build trust with their clients. If the authentic information of a customer is accessible to that particular customer at any moment in which they require, the company gains a competitive advantage because of the convenience that is received by the customers. However, these elements can be compromised because of problems with the equipment like equipment failure, use of obsolete technology, etc. Also, human errors like staff not following the proper office procedure, employee not well-trained for their role,

etc. can compromise the security of information in an organization (Whitman & Mattord, 2018).

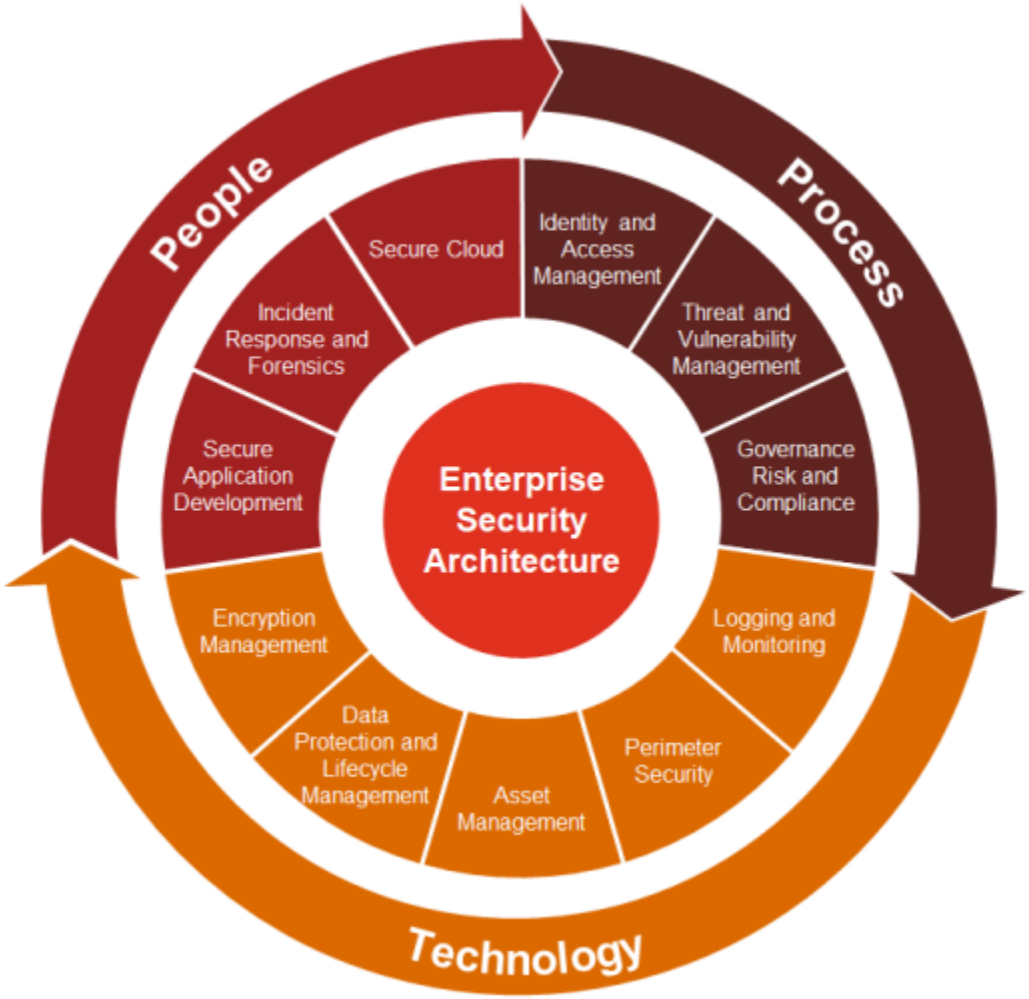

Figure 1: Components of an organization:

(Department Of Information Technology, 2019)

The information security audit helps to find out the short-comings and threats lurking in the organization and provides a detailed report after inspecting the organizations policies and procedures. It provides ways to improve the policy or procedure if any threats or vulnerabilities are obtained after the examination. This is why the Information Security Audit must be performed at certain intervals in order to find out the irregularities, vulnerabilities and risks present in an organization and solve them effectively in order to prevent the organization from potential loss in the future (ISACA, 2016).

1.2 Aims and Objectives

The various aims of information security audit are to make sure of the following:

- A management control framework exists.
- An effective security program is in place.
- Security education and training is adequate.
- Information/communications is appropriately classified and protected.
- Security breaches are effectively dealt with.
- An effective personnel screening program is enforced.
- Physical safeguards are in place for the protection of personnel and assets.
- Contingency management has been developed.
- Security requirements are met in contract management.
- Threat and risk assessments are conducted on a regular basis and prior to major system, application and telecommunication changes.
  (Department Of Information Technology, 2019)

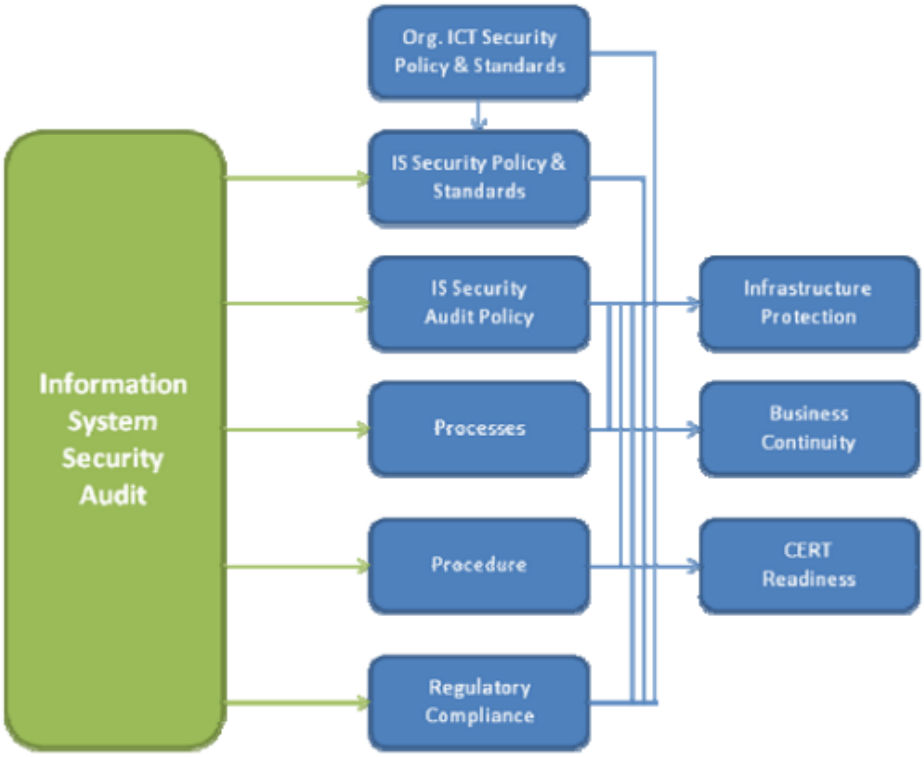

Figure 2: Components of Information Security Audit

(Gupta & Shakya, 2015)

2. Background

2.1 Information Security Audit Process

There are three major phases in the IT auditing process according to ISACA (Information Systems Audit and Control Association). They are categorized as planning, fieldwork and reporting.

Figure 3: IT Audit Process

(Cooke, 2018)

2.1.1 Planning

Each organization has a unique structure. They have their own set of procedures, equipments and number of staffs. Therefore, to conduct the audit for a particular organization, various steps must be devised for all the actions to be performed according to the circumstances of the organization. Planning is the phase which involves developing strategies and establishing the step-by-step procedures to be conducted in an organization during the audit. The first step is to create an audit programme. An audit program is a collection of documents that define the auditing objectives of the auditing process, the expected audit outcomes, the risk management process, and risk assessment. This includes preparing for the steps such as:

- Written and verbal questioning for interviews and questionnaires
- Visual inspection of the systems, locations, spaces, rooms and objects
- Technical examination for testing alarm systems, access control systems, applications, etc.
- Analysis of files and data like electronic data, log files, database evaluations, etc. (Ghorpade & More, 2015)

The audit program's goal is to provide the organization's CEO and Board of Directors with an audit report that includes the audit's findings, facts, recommendations, and

conclusions. The audit team will be set up for success if the planning is carried out properly (ISACA, 2016).

2.1.2 Fieldwork and Documentation

After developing a detailed plan, all the required audit activities are conducted by the audit team. This includes various activities such as:

- Reviewing the location of the tools and technologies and find out if the data center has adequate physical security controls in order to prevent unauthorized access.
- Reviewing the company's IT policies and procedures to evaluate the responsibilities of the personnel and check it they are following the correct procedures.
- Reviewing the job descriptions of all the data center employees and finding out if the employees are sufficiently skilled and whether they require additional training for their jobs.
- Reviewing the data center's disaster recovery plan and find out if the adequate environmental controls are in place to ensure equipment safety in case of natural disasters.
- Inspecting all operating systems, software applications and equipments operating within the data center to check if the all the equipments are working properly and effectively and whether the maintenance is performed timely.
- Evaluating the company's IT budget and systems planning documentation to know if proper equipments are used and appropriate backup procedures are in place so as to minimize downtime and prevent loss of important data.
  (Ghorpade & More, 2015)

The information about the state of the organization is gathered by performing these activities which helps the auditors to analyze the risks present in the organization. After the completion of fieldwork, all the audit observations, evidences, logs and results should be systematically organized and documented. The documentation is necessary for the approval of the current audit procedure by the organization and, if required, by regulatory authorities. The records will also be utilized to rectify the nonconformity goals and as a reference for the future. The documents should be stored in an AMS or in an electronic format (Audit Management System) (ISACA, 2016).

2.1.3 Reporting and Follow-up

Reporting is the final phase of the audit. In this step, all the problems and inconsistencies discovered are tested to verify the accuracy of the results generated. After that, the auditor prepares a report that includes the auditor's views, recommendations, and suggestions for reducing potential risks, as well as findings. The report is the "product" of the audit process, in which the audit team communicates its findings to the organization's management. The report's core is a list of concerns and activities that must be addressed as part of the audit follow-up to correct, avoid, or enhance the audited area's weakness. It's important to realize that the purpose of the audit is to strengthen environmental controls, not to produce an audit report that proves the auditor's work. As a result, the audit team will achieve their aim if the IT teams correct issues during the audit. It's important to note that there are a variety of audit frameworks and procedures to choose from while conducting an audit. However, it is important to make sure that the auditors, both internal and external, have a thorough grasp of the company they are auditing and are familiar with the organization's information systems before the start of each audit. The auditors' job is to create an audit program, carry it out, and publish a report that accurately reflects the state of the IT systems being audited (ISACA, 2016).

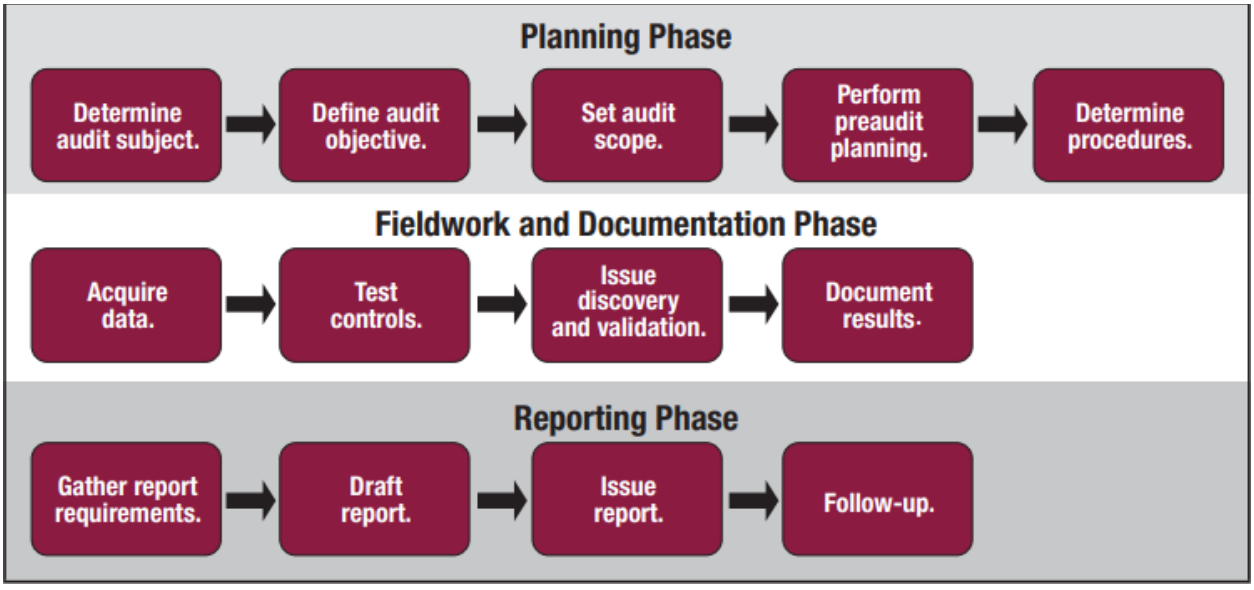

Figure 4: Information Security Audit Phases

(ISACA, 2016)

3. Literature Review

3.1 Case Study

In September 2017, Equifax, one of the three main consumer credit reporting agencies in the United States, disclosed that its systems had been breached, compromising the sensitive personal information of 148 million Americans. Names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers were among the information stolen. A total of 209,000 people's credit card numbers were also compromised.

Figure 5: Case Study of Equifax Inc.

(Leonhardt, 2019)

In terms of size and intensity, the data breach of Equifax is unparalleled. Various companies before the Equifax have faced greater attacks regarding information security, however the confidential client information possessed by Equifax, along with magnitude of probable problems, makes the Equifax breach exceptional (EPIC, 2019).

3.1.1 Findings

The attack was triggered by the vulnerability Apache Struts CVE-2017-5638. Apache Struts is managed by the Apache Software Foundation, a well-known platform for creating Java Web apps. The foundation issued a statement on March 7, 2017, highlighting the threat and provided a fix.

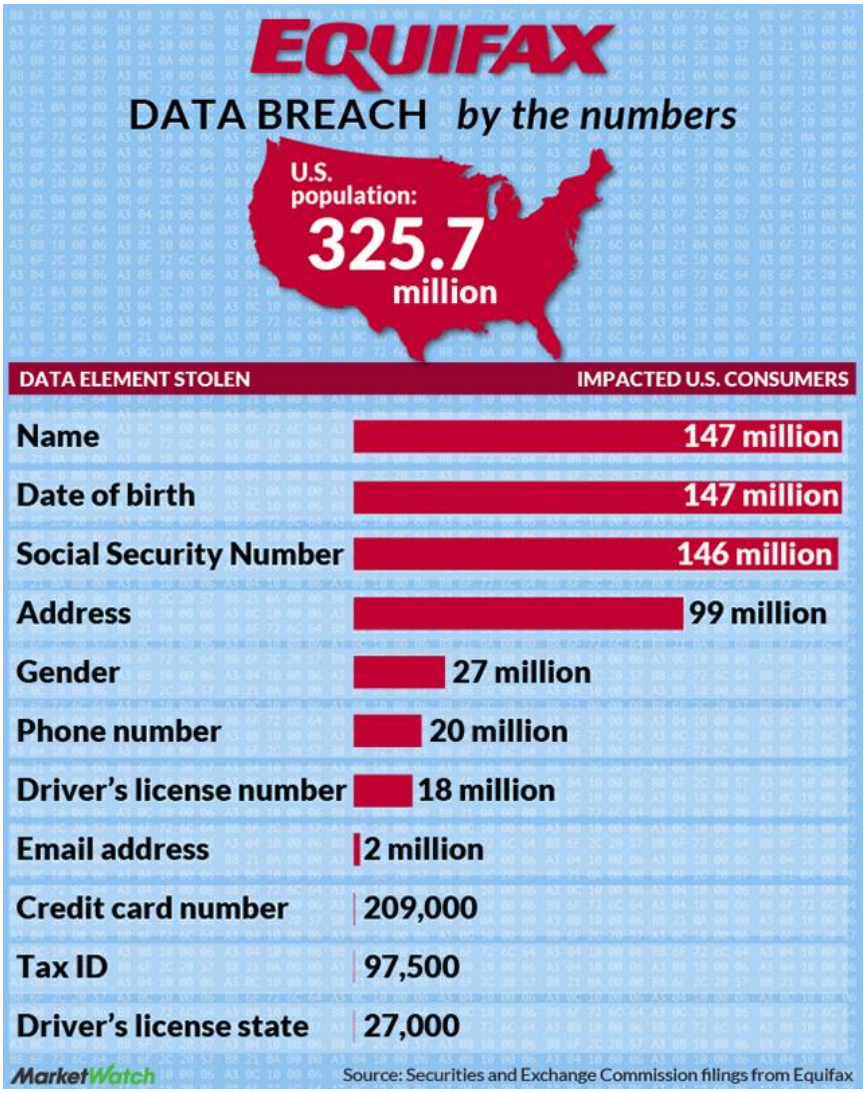

Figure 6: Statistics of data breach

(Owens, 2018)

On March 9, 2017, Equifax administrators received an internal email message advising them to deploy the Apache patch. On March 15, 2017, the information security team of Equifax performed scans to check systems that were vulnerable to the Apache Struts vulnerability, however the scans failed to detect the vulnerability (EPIC, 2019).

3.1.2 Analysis

A suspicious network traffic was noticed on its online dispute portal by the information security department on July 29, 2017 and until that point, the vulnerability was not addressed. After finding such unusual behaviour they implemented the Apache patch. Equifax discovered more suspicious behaviour on July 30, 2017, and shut the web application down. Later, Equifax contacted Mandiant, a cybersecurity organization, after three days, to run a forensic investigation into the breach (EPIC, 2019).

Equifax should have contacted the system administrators in a different way than the alert update notification. The appropriate authorities should have responded quickly in order to update the security updates. The digital signature for the traffic inspection system should have been refreshed on a regular basis. The database should have been kept in a separate way over many secure network connections with redundant pathways. Encrypted Data Base System should have been used to store sensitive user credential information. Equifax's Information Security Policy, particularly the Authentication Policy, should have been extensively amended and adhered to. Instead of "Apache Strut," they should have utilized other technologies like Tapestry, Vaadin, Blade, Dropwizard, and so forth.

4. Conclusion

An information security audit is a manual or automated technical analysis of an organization's people, processes, and technology. Interviewing employees, running security vulnerability scans, examining application and operating system access controls, and evaluating physical access to the systems are all part of manual assessments. System produced audit reports or employing software to monitor and report changes to files and settings on a system are examples of automated assessments, or CAATs. Personal computers, servers, mainframes, network routers, and switches are examples of systems. Web Services, Microsoft Project Central, and Oracle Database are examples of applications. Regular security audits also save the auditors from having to return week after week to solve the same problems. Because companies are constantly changing – such as upgrading network setups, adding/removing personnel, or building a new branch - quarterly audits are encouraged. All of these events have the potential to introduce a new security threat vector, and thus need to be addressed accordingly in order to comply with the organization’s legal responsibility (obligations). Therefore, complete security audits should be performed at least once a year. Also, quarterly audits are highly recommended, especially if the organization has a legal obligation to conform to certain security standards.

5. References

Cooke, I., 2018. IS Audit Basics: Innovation in the It Audit Process. *ISACA JOURNAL,* Volume 2, p. 6.

Department Of Information Technology, 2019. *Nepal GEA 2.0 Security Architecture,* Kathmandu: Ministry of Communication and Information Technology.

EPIC, 2019. *Equifax Data Breach.* [Online]
Available at: https://archive.epic.org/privacy/data-breach/equifax/
[Accessed 27 December 2021].

Ghorpade, Y. & More, R., 2015. *Inforamtion Security and Audit.* 1st ed. s.l.:Self Publication.

Gupta, A. & Shakya, S., 2015. Information System Audit: A study for security and challenges in Nepal. *International Journal of Computer Science and Information Security (IJCSIS),* 13(11), p. 4.

ISACA, 2016. Information Systems Auditing: Tools and Techniques - Creating Audit Programs. *ISACA White Paper,* Volume 1, p. 16.

Leonhardt, M., 2019. *What you need to know about the Equifax data breach $700 million settlement.* [Online]
Available at: https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html
[Accessed 26 December 2021].

Owens, J. C., 2018. *The Equifax data breach, in one chart.* [Online]
Available at: https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07
[Accessed 26 December 2021].

Whitman, M. E. & Mattord, H. J., 2018. *Management of Information Security.* 6th ed. Boston: Cenage Learning.

6. Bibliography

Cooke, I., 2018. IS Audit Basics: Innovation in the It Audit Process. *ISACA JOURNAL,* Volume 2, p. 6.

Department Of Information Technology, 2019. *Nepal GEA 2.0 Security Architecture,* Kathmandu: Ministry of Communication and Information Technology.

EPIC, 2019. *Equifax Data Breach.* [Online]
Available at: https://archive.epic.org/privacy/data-breach/equifax/
[Accessed 27 December 2021].

Ghorpade, Y. & More, R., 2015. *Inforamtion Security and Audit.* 1st ed. s.l.:Self Publication.

Gupta, A. & Shakya, S., 2015. Information System Audit: A study for security and challenges in Nepal. *International Journal of Computer Science and Information Security (IJCSIS),* 13(11), p. 4.

ISACA, 2016. Information Systems Auditing: Tools and Techniques - Creating Audit Programs. *ISACA White Paper,* Volume 1, p. 16.

Leonhardt, M., 2019. *What you need to know about the Equifax data breach $700 million settlement.* [Online]
Available at: https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html
[Accessed 26 December 2021].

Owens, J. C., 2018. *The Equifax data breach, in one chart.* [Online]
Available at: https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07
[Accessed 26 December 2021].

Whitman, M. E. & Mattord, H. J., 2018. *Management of Information Security.* 6th ed. Boston: Cenage Learning.