islington college
(इस्लिङ्टन कलेज)

LONDON METROPOLITAN UNIVERSITY

Module Code & Module Title

CC5052NI Risk, Crisis and Security Management

Assessment Weightage & Type

50% Individual Coursework

On

Information Security Audit

Year and Semester

2024 -25 Autumn Semester

Student Name: Bachan Timalsina

London Met ID: 23047401

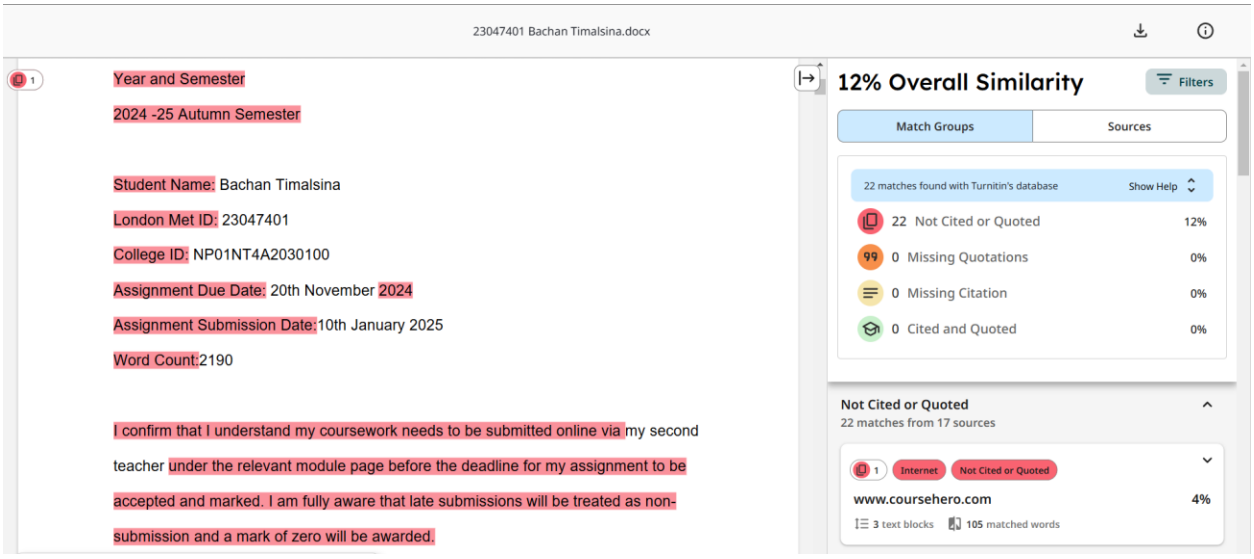
College ID: NP01NT4A2030100

Assignment Due Date: 20th November 2024

Assignment Submission Date:10th January 2025

Word Count:2190

I confirm that I understand my coursework needs to be submitted online via my second teacher under the relevant module page before the deadline 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.


23047401 Bachan Timalsina.docx
Year and Semester
2024 -25 Autumn Semester
Student Name: Bachan Timalsina
London Met ID: 23047401
College ID: NP01NT4A2030100
Assignment Due Date: 20th November 2024
Assignment Submission Date:10th January 2025
Word Count:2190
I confirm that I understand my coursework needs to be submitted online via my second teacher under the relevant module page before the deadline 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.
12% Overall Similarity
Filters
Match Groups
Sources
22 matches found with Turnitin's database
Show Help
22 Not Cited or Quoted 12%
0 Missing Quotations 0%
0 Missing Citation 0%
0 Cited and Quoted 0%
Not Cited or Quoted
22 matches from 17 sources
Internet
Not Cited or Quoted
www.coursehero.com 4%
3 text blocks
105 matched words

Acknowledgement

I would like to express my heartfelt gratitude to everyone who supported me in completing this report on "Information Security Audit." I am thankful to my tutor Mr. Akash Ojha for providing valuable guidance and clear instructions throughout this project. I also extend my appreciation to my peers for their encouragement and constructive feedback. Special thanks to the library and online resources that helped me gather relevant information for my research. Finally, I am deeply grateful to my tutors and lecturers for their constant support and motivation, which enabled me to complete this work successfully.

Abstract

This report investigates the role of information security audits in preventing data breaches, with a comprehensive focus on their methodologies, effectiveness, and challenges. Information security audits are vital tools for identifying vulnerabilities, assessing compliance with regulatory frameworks, and ensuring the robustness of an organization's cybersecurity posture. The study examines key auditing techniques, including vulnerability assessments, penetration testing, compliance reviews, and configuration audits, to determine their contributions to breach prevention.

The report explores the theoretical foundation of audits, their practical application, and the challenges organizations encounter, such as resource limitations, rapidly evolving threats, and inadequate follow-up actions. It includes a detailed review of relevant literature to establish the importance of effective audits, alongside an analysis of real-world challenges in implementing these practices. Additionally, through case study analysis, the report highlights lessons learned from significant data breaches and identifies how stronger audits could have mitigated or prevented these incidents.

The findings aim to provide actionable recommendations to enhance the efficiency of information security audits, ensuring that organizations can adapt to emerging threats and improve their overall resilience against data breaches. This work also reflects on the broader implications of audit practices for risk management and regulatory compliance, contributing valuable insights to the field of cybersecurity.

Table of Contents:

1. Introduction:

In today's connected world, businesses depend on digital technology to handle and protect sensitive information. While these tools make work faster and more efficient, they also open the door to risks like data breaches, hacking, and unauthorized access. To keep sensitive information safe, businesses need to regularly check how secure their systems are that's where Information Security Audits come in.

Data breaches remain one of the most significant threats to organizations, with incidents becoming increasingly frequent and severe. According to research by Verizon's 2023 Data Breach Investigations Report, 74% of all data breaches were financially motivated, while 52% involved hacking. These statistics underscore the need for proactive measures to safeguard sensitive data.

Information Security Audits have emerged as a critical line of defense, enabling organizations to identify vulnerabilities, ensure compliance with data protection regulations, and implement controls to prevent breaches. By systematically evaluating an organization's security infrastructure, these audits provide insights into potential weaknesses, whether technical (e.g., unpatched software) or procedural (e.g., lack of access control).

An Information Security Audit is like a check-up for a company's digital systems, policies, and practices. It helps find weak spots, ensures the company follows the rules, and checks how ready it is to handle security problems. These audits give a clear picture of how secure the company's systems are and help them fix issues before they become big problems. By doing this, businesses can stay ahead of risks and make sure their security measures meet industry standards. Ultimately, they are crucial for a strong and sustained information Security position. (Sahoo, 2024)

Key points about information security audits:

- **Purpose:**

  To assess the effectiveness of an organization's security controls and identify areas for improvement in protecting sensitive data from unauthorized access, use, disclosure, disruption, modification, or destruction.

- **Scope:**

  Covers various aspects of information security including network security, application security, access controls, data encryption, incident response procedures, physical security, and compliance with relevant regulations.

1.1 Aims and objectives:

Aims:

As put forward in this discussion, it is therefore appropriate to stress the significance of carrying out formal security check-ups habitually. It will describe different methods used in the identification of risks that is during these audits and the general assessment of how compliance is achieved.

Objectives:

1.Provide a clear understanding of what these audits entail and their purpose in safeguarding data.

2.Examine key methodologies used in audits, such as vulnerability assessments and penetration testing, and their relevance to breach prevention.

3.Explore how security audits prevent breaches by identifying gaps in security controls and recommending mitigation strategies.

2. Literature review:

The effectiveness of information security audits in preventing data breaches lies in their ability to systematically evaluate an organization's cybersecurity posture. By identifying vulnerabilities, ensuring compliance with regulations, and assessing security policies and controls, audits help mitigate risks before they can be exploited by attackers.

The ultimate measure of an audit's success lies in its ability to prevent data breaches. According to the Verizon Data Breach Investigations Report (2023), organizations conducting regular audits reported 37% fewer breaches compared to those without audit processes. This underscores the role of audits in identifying misconfigurations, weak access controls, and outdated software, which are often exploited in breaches.

Further, Weiss and Solomon (2020) note that audits contribute to better incident response by exposing gaps in an organization's preparedness. For example, during the Equifax breach in 2017, auditors highlighted unpatched vulnerabilities that were later exploited. Had these audit findings been acted upon, the breach could have been mitigated.

2.1 Key ways for effective audit include:

Identifying Weaknesses: Detecting vulnerabilities in systems, networks, and configurations.

Ensuring Compliance: Validating adherence to regulatory standards like GDPR or ISO 27001 to avoid penalties and enhance data security.

Improving Security Policies: Evaluating and refining policies such as access control and incident response plans.

Enhancing Resilience: Preparing organizations to detect, respond to, and recover from potential threats.

2.2 Types of security audit:

Assurance of information systems' availability, confidentiality, and integrity is evidently provided through information security audits. The several kinds of information security audits are listed below, along with their brief overview:

1. Vulnerability Assessment:

Vulnerability Assessment, which is in fact a prevention method, is a way of detecting the risks within an information system actively, with the use of the automated tools. It identifies risks and categorizes them, and suggest ways to avoid or manage them. It allows organizations to stop issues and attacks from happening and take charge of security in their own organization.

2. Penetration Test:

A pen test, or Penetration Test, is an authorized attempt to demonstrate to an organization how an unauthorized person might be able to infiltrate the IT structure of company. This is beneficial in probing the system so that?' Points are discovered that might compromise the computer system or otherwise leads to illicit intrusions or other improper actions. This approach will help organizations measure levels of security and as well feel more secure to prevent an attack from occurring.

3. Application Audit:

An application audit evaluates the risk involving software applications. This includes, code review, configuration review and vulnerability assessment. This audit inscribes an assurance that applications are best developed and distributed with immense security prowess to keep attackers away from precious data.

2.3 Importance of security audit:

An Information Security Audit checks an organization's IT systems to find security weaknesses and risks. These risks can harm not just IT systems but also overall business operations. Information Security isn't just about protecting technology; it's also about keeping data safe. Here's why regular security audits are crucial for every business:

1.A security audit shows how strong your current defenses are. It helps organizations see if they're well-protected against threats. The audit provides a detailed report that highlights weak points and suggests ways to fix them. This helps businesses improve their security policies, procedures, and systems.

2.The audit identifies gaps and weak spots in your security setup. It also checks how effective your current policies and standards are. The findings will suggest whether your existing measures are

enough or need to be updated. Businesses can use these suggestions to adjust their policies and improve security.

3.An audit checks for vulnerabilities in your IT systems and networks. It looks for flaws or entry points that hackers could exploit. This regular assessment ensures that your security measures are working and keeps your data and systems safe.

2.4 Challenges of data security audits implementation:

1.Defining the target: This is important to avoid generalize the security audit and grant a specific focus to the areas of the environment of the organization. As a part of this critical process, one needs to define which networks, databases, apps, etc. require auditing This, however, is one of the key questions faced during the definition of the audit target: depending on the options chosen, one has to choose the properly balanced approach between completeness of coverage and feasibility.

2.Adapting to an evolving cyber landscape: Managing the difficulties of security audits while operating in an environment where the threats are constantly changing means working in a constantly changing environment. It is the same as protecting a city in the future in which you need to defend a skyline of towers that can shift forms, roads that may pop out of nowhere, and villains who invent new strategies all the time. There are constant new technologies, new software and new gadgets in the world.

3.**Human-factor challenges**: The current accuracy of the security audit can be compromised em by instance through the human elements involved. Some of the examples of potential security risks include the issues of communication, the threat from insiders in an organization, wrong interpretation of the findings made in analyses as well as the overlooking of security measures to be followed. (Firewall.cx., 2024).

2.5 Tools for effective Audit:

Using Firewall Analyzer for Security Audit is a powerful tool that helps to minimize the difficulties of the security audit process. It offers a wide range of features to facilitate security audits, such as:

1. **Log analysis**: Firewall Analyzer by ManageEngine offers the features related to log analysis and integration of firewalls, routers, IDSs, and IPSs. They provide meaningful information about networks activities, user's behavior, and security threats and breaches. Said logs play a significant role helping detect potential vulnerabilities or incidents as soon as possible.

2. **Compliance auditing**: For the mentioned compliance standards like GDPR, SOX, HIPAA, among others, the tool delivers ready-made compliance reports. These reports provide additional information on how an organisation complies with general and or specific security standards for the industry it belongs to.

3.**Real-time alerts**: Firewall Analyzer conveys alerts the moment there is violation of the policy or occurrence of a security event. This allows organisations to have preventive measures against the probable threats. These alert notifications can be personalized, meaning that the appropriate action has to be taken before the threat level goes up.. (Firewall.cx., 2024)

3 Analysis:

3.1 Basics and procedure of analysis

The paper also analyses how information security audits have been efficient in avoiding data loss incidents. The following basis and procedure were adopted:

1. Mainly oriented towards vulnerability detection, examination of audit follow-up activities and the function of real-time monitoring in security enhancement.

2. Reports from the IBM, Verizon and academic journals, as well as the case study related to the Equifax data breach occurred in 2017.

3. Linked audits with breach prevention via majored parameters such as response times and resolution rates.

4.Equifax’s case shows what may happen when there are serious lapses in auditing.

3.2 Case study background and impacts:

In 2017, Equifax, one of the largest credit reporting agencies in the world, experienced a catastrophic data breach. This incident exposed the sensitive personal and financial information of 147 million individuals, including Social Security numbers, birthdates, and credit card information. The root cause was traced to an unpatched vulnerability in the widely used Apache Struts web application framework (CVE-2017-5638). Despite prior warnings and internal scans identifying the issue, the patch was not applied, leaving the system vulnerable.

The breach lasted from mid-May to July 2017, during which attackers exploited this vulnerability to gain unauthorized access. The extended period of undetected intrusion highlighted significant flaws in Equifax’s security practices, including its information security audit processes. (breachsense, 2024)

3.3 Reasons for breach

The Equifax breach was a culmination of technical, procedural, and organizational failures:

Technical: Unpatched vulnerabilities, poor encryption, and lack of monitoring.

Procedural: Ineffective audits, delayed patch application, and inadequate incident response.

Organizational: A weak security culture and insufficient accountability.

3.4 Audit-Related Failures

1.Failure to Act on Audit Findings:

The internal scans done by Equifax regarding Apache Struts had identified the vulnerability prior to the breach but due to poor accountability and management none of the issues were prioritized and remain unaddressed.

2.Inadequate Audit Scope:

Critical areas like the patch management processes and third-party software assessments are areas that working or did not receive a mention. Such was the case with Salford PCA where these critical vulnerabilities never budged even with the lack of a comprehensive audit scope.

3.Lack of Continuous Monitoring:

Here the company was more into periodic audits which are quite ineffective when it comes to finding real-time threats. Therefore, the attackers were able to remain undetected on the system for at least 76 days.

3.4 Potential Improvements:

1.Timely Patching:

Implementing stringent patch management policies and adhering to audit recommendations would have significantly reduced the risk of exploitation.

2.Comprehensive Scope:

Expanding the scope of audits to include third-party software evaluations and vendor risk assessments would have provided a more holistic view of vulnerabilities.

3.Real-Time Monitoring:

Adopting continuous auditing tools, such as Security Information and Event Management (SIEM) systems, could have identified unauthorized access and mitigated the breach's impact.

4.Enhanced Accountability:

Establishing clear accountability structures for implementing audit findings and tracking progress would ensure timely remediation of vulnerabilities.

4. Conclusion:

This report stressed the enormity of Information security audit in checking incidences of data violation as demonstrated from the Equifax case. It is found out that bad audit practices that include delayed patching and short audit coverage contributed to the breach and caused it to protract. It also showed what measures, ranging from embracing continuous auditing practices to proactive vulnerability management and holistic audit approaches, could minimize similar risks.

The outcomes show that effectiveness of security audits is higher if such check switches from the focus on compliance to proactive assessment. The observations of Equifax case draw attention of the fact that timely actions with the audit findings are essential and how information technologies, like SIEM systems, should be integrated to track and respond for threats immediately.

Based on the analysis, it is recommended that organizations:

1. Enrich the current audit opportunities by enlarging the project's scope to address third-party and vendors' risks.

2. It means that one should incorporate continuous audits so that any openings revealed along the way may be closed immediately.

3. Install sound lines of responsibility to ensure that responsibilities follow audits are promptly addressed.

4. Patch management should be updated and checked more often to reduce exploitation consequences.

These measures help organizations improve the efficiency of their audits, strengthen protection of vital information and better tackle new threats in the sphere of cyber security.

References:

breachsense, 2024. *breachsense.* [Online] Available at: https://www.breachsense.com/blog/equifax-data-breach/ [Accessed 26 december 2024].

Firewall.cx., 2024. *Firewall.cx..* [Online] Available at: https://www.firewall.cx/tools-tips-reviews/manageengine/firewall-analyzer/dealing-with-security-audit-challenges.html [Accessed 2 12 2024].

Intuit, 2024. *Intuit.* [Online] Available at: https://mailchimp.com/resources/security-audit/ [Accessed 2 12 2024].

Sahoo, C., 2024. *Qualysec.* [Online] Available at: https://qualysec.com/what-is-information-security-audits/#:~:text=Information%20security%20audits%20are%20necessary,before%20threats%20can%20leverage%20them. [Accessed 29 November 2024].