



slington college
(इस्लिङ्टन कलेज)

CC5052NI & Risk, Crisis and Security Management

50 % Individual Coursework

on

**Evaluating Nepal's Information Security Audit Practices with Global
Standards**

Semester 3

2024-25 Autumn

Student Name: Navraj Rajak

London Met ID: 23047346

College ID: NP01NT4A230040

Assignment Due Date: Friday, January 10, 2025

Assignment Submission Date: Thursday, January 9, 2025

Submitted To: Apil Chand

Word Count: 2869

I confirm that I understand my coursework needs to be submitted online via MST 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.

A Coursework Submitted
on
Evaluating Nepal's Information Security Audit Practices with Global Standards

Semester 3
2024-25 Autumn

Student Name: Navraj Rajak

London Met ID: 23047346

College ID: NP01NT4A230040

Assignment Due Date: Friday, January 10, 2025

Assignment Submission Date: Thursday, January 9, 2025





Submitted To: Apil Chand

Word Count: 2869




5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **11 Not Cited or Quoted 5%**
Matches with neither in-text citation nor quotation marks
-  **0 Missing Quotations 0%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 3%  Internet sources
- 2%  Publications
- 4%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

***Note:** This similarity test is conducted from Introduction to Conclusion section only, i.e. Chapter 1 to Chapter 4.*

Abstract

The evaluation of Nepal's information security audits practices with global standards gives insights into the alignment and gaps in current policies. Globally recognized frameworks, ISO 27001:2022, COBIT 5, and NIST 800-53 Revision 5, are some of the world's best known. These provide guidelines for information security management, risk mitigation, IT governance and so on. These proves to be of very significance while evaluating these against national practices.

Nepal's national regulatory frameworks such as the NTA Cybersecurity Byelaws (2020), Nepal Rastra Bank IT Guidelines, and Nepal Beema IT Guidelines have played a vital role in creating and maintaining resilient cyber security posture of the nation's infrastructure. However, a comparative analysis shows some level of gaps between Nepal's current practices and these global standards. These have provided the awareness to areas where improvements are necessary. By identifying these gaps, the research provides recommendations for enhancing the country's information security audit practices with an aim to align them more closely with global best practices in order to create resilient cybersecurity posture.

Table of Contents

Abstract	ii
Table of figures	v
List of Abbreviations.....	vi
Chapter 1: Introduction	1
1.1. Background	1
1.2. Problem Statement	2
1.3. Objectives	2
1.4. Rationale	2
Chapter 2: Literature Review.....	3
2.1. Global Standards in Information Security	3
2.1.1. ISO 27001:2022	3
2.1.2. COBIT 5.....	3
2.1.3. NIST 800-53 Rev. 5	3
2.2. Nepal's Regulatory Framework	4
2.2.1. Cybersecurity Byelaws (2020).....	4
2.2.2. Nepal Rastra Bank Cyber Resilience Guidelines.....	4
2.2.3. Nepal Beema IT Guidelines.....	4
Chapter 3: Analysis	6
3.1. Basis for Compatibility	6
3.2. Procedure for the Analysis	7
3.3. General Practices in Nepal.....	7
3.4. Case Study: Comparison of NRB Cyber Resilience Guidelines with Global Standards	8
3.4.1. Governance	8
3.4.2. Risk Management	8

3.4.3.	Security and Privacy Controls	8
3.4.4.	Incident Response and Recovery	9
3.4.5.	Contingency Planning.....	9
3.4.6.	Continuous Improvement.....	9
3.4.7.	Other Areas	9
3.5.	SWOT Analysis	10
Chapter 4: Conclusion.....		11
4.1.	Results.....	11
4.2.	Discussion.....	11
4.3.	Recommendations.....	12
References.....		13

Table of figures

Figure 1: SWOT Analysis	10
-------------------------------	----

List of abbreviations

NRB	Nepal Rastra Bank
IS	Information Security
DRP	Disaster Recovery Plan
BCP	Business Continuity Plan
RMF	Risk Management Framework
NTA	Nepal Telecommunications Authority
CERT	Computer Emergency Response Team
ISMS	Information Security Management System
ISO	International Organization for Standardization
ICT	Information and Communications Technology
NIST	National Institute of Standards and Technology
SWOT	Strengths, Weaknesses, Opportunities, and Threats
COBIT	Control Objectives for Information and Related Technologies

Chapter 1: Introduction

1.1. Background

Digital technology has globally revolutionized the daily operations of organizations and government. Nepal being no exception has been experiencing significant growth in digitalization in many sectors. Those sectors are telecommunications, financial institutions, governance, administrations, service delivery etc. The number of users for internet and mobile banking has increased from 1,754,566 (July 2016) to 21,363,989 (July 2023), an increase of **1117.62%** [1]. The Telecommunication Indicator of September 2014 and July 2024 shows that the broadband internet subscription has climbed from **8,782,936** to **34,028,583**, a *fourfold* increase in a decade [2] [3]. Many other official processes such as data management, logging and recording have adopted cloud-based systems.

In one way, these have been enabler for transparency efficiency and improving governance. However, it has also increased the risks of cyber breaches and data theft by introducing new vulnerabilities. To enjoy full merits of these digitalization around us, the security of these platforms must be secure and safely used. The digital assets must be made secure. This is achieved by implementing robust information security framework, regular information security audits, following the best practices globally recognized.

Global standards such as ISO 27001:2022, COBIT 5, and NIST 800-53 are some of the best frameworks available for strengthening cyber security of any institution [4] [5] [6]. These provide guidelines for ensuring IT governance, risk management and compliance in information security. These standards outline the best internationally recognized practices for managing security controls, identifying vulnerabilities and mitigation risks. Nepal has also adopted security measures outlines in these. However, its audit practices are not fully complaint with these frameworks.

This raises concerns about Nepal's IT governance and risk management strategies in addressing the growing challenges. A proper evaluation of Nepal's Information Security Audit practices in compliance with global standards would prove to be very vital to learn about Nepal's posture and strength to the country's digital ecosystem.

1.2. Problem Statement

Nepal's security practices partially comply with international standards. This partial alignment creates vulnerabilities and potential risks in the country's digital ecosystem.

1.3. Objectives

- To evaluate Nepal's information security audit practices compliance with global standards
- To analyze the gaps in information security audit practices.

1.4. Rationale

The centralization of digital platforms for financial transaction, official recording keeping, user/customer information, service delivery, data management, data processing and so on has enhanced operational efficiency, transparency and accessibility. This has brought many advantages to the people and the nation as a whole. These could pose significant risk leading to cyber-crimes, data theft, data breaches and so on in case of inefficiency. This can be mitigated by staying update to on-going cyber intelligence, identifying current security posture, assessing and testing assets and then providing proper recommendations to further enhance the security's posture. This in turn is achieved by periodic internal or external information security audit.

Nepal's information security audit practices partial alignment with those set by global standards such as ISO 27001:2022, COBIT 5, and NIST 800-53 rev 5 could create potential gaps in governance, security controls, risk management and compliance. This research evaluates the compliance with the global standards to identify the gaps, and emphasize to addressing those in order for country's resilience to cyber threats.

Chapter 2: Literature Review

2.1. Global Standards in Information Security

2.1.1. ISO 27001:2022

It is a framework for information security management systems (ISMS). It set outs requirements for information security management systems. Its main focus is to manage sensitive information to ensure its confidentiality, integrity and availability. ISO claims it to be the world's best world's best-known standard for information security management systems. The organization certified under this standard have shown to experience relatively fewer data breaches and security incidents. This is due to its robust security controls that it mandates. [4]

2.1.2. COBIT 5

Its full form is Control Objective for Information and Related Technologies. It provides framework emphasizing for IT governance and management. It outlines a set of practices to manage IT risks and ensure that the IT investments align with the organizational goal. It is built on 5 principles: meeting stakeholder needs by delivering values by balancing risk and resources; covering the enterprise end-to-end in order to integrate IT governance across all areas of an institution; applying a single, integrate framework in a way that it can combine with other standard or companies own policies to create a unified approach in order to meet organizational needs and goals; enabling a holistic approach to promote independencies among organizational elements; and separating governance from management by clearly defining their roles. [6]

2.1.3. NIST 800-53 Rev. 5

It is a special publication by developed by National Institute of Standards and Technology. It is a framework for security and privacy controls for information systems and organizations. Its main focus is to improve security and privacy posture through its guideline's implementation. It has introduced privacy controls, security controls in order to protect personally identifiable information (PII). It has also focused on supply chain risk management to mitigate any threats from third-party vendors. This framework is organized into 20 control families, covering areas such as access control, incident response, risk

assessment, and system & communication protection. This enables organizations to customize controls as per their specific needs. [5]

2.2. Nepal's Regulatory Framework

2.2.1. Cybersecurity Byelaws (2020)

It was created by Nepal Telecommunication Authority (NTA) under the Telecommunication Act 2053. It establishes cybersecurity framework to protect ICT infrastructure of Nepal's telecommunication industry. Any institution approved by NTA is enforced to maintain robust security practices. This includes implementing board-approved ICT policies, DDoS preventive mechanisms, secure coding practice, strong authentication mechanisms, use of encryption, periodic internal (every six month) and external audits (once a year). It has emphasized cloud security, Computer Emergency Response Team (CERT)/incident response capabilities. It has also focused on SOC for real-time monitoring, and cyber security awareness programs. Its key provisions are focused on safeguarding data privacy, periodic vulnerability assessment and penetration testing, ensuring application security. These aim to improve Nepal's telecommunication industry cyber resilience and align them with global security standards. [7]

2.2.2. Nepal Rastra Bank Cyber Resilience Guidelines

The Cyber Resilience Guidelines has been published by Nepal Rastra Bank pursuant to its monetary policy of fiscal year 2022/23, policy number 128, states "*Cyber and Information Security Guideline will be issued for the institutions licensed to carry out payment-related transactions*" [8]. This guideline has emphasized risk management across governance, identification, protection, detection, and response/recovery. It has also addressed testing, situational awareness, and continuous improvements. Licensed Institutions must adopt risk-based approach, ensure system recovery within two hours of disruptions, and must manage interconnection risks. The key provision under this guideline is periodic information security audit, vulnerability assessment, penetration testing, strong data protection mechanisms, automated anomalies detection and board-level oversight. [8]

2.2.3. Nepal Beema IT Guidelines

This guideline is issued by the Insurance Board of Nepal under the Insurance Act 2049. It emphasizes implementation of robust IT system, security and compliance for any

institution operating under authorization of Nepal Insurance Authority (नेपाल बीमा प्राधिकरण). It has enforced insurers to use IT system in all offices, establish well developed data-centers with backup capabilities, and maintain user-friendly websites with necessary business information. The insurers must adopt IT security measures, including cyber insurance, to protect against malware, network vulnerabilities, physical threats, annual audits by licensed professionals to assess system security, access control, and disaster recovery. Also, the insurers have to develop internal IT policies, use genuine software, regularly update system. In addition to this, they also must have dedicated IT teams. Also, they must submit all these detailed in annual reports to the Board. [9]

These highlight both global and national frameworks aimed at strengthening information security. International standards like **ISO 27001:2022**, **COBIT 5**, and **NIST 800-53 Rev. 5** provide structured approaches to risk management, IT governance, and data protection. These frameworks emphasize the need for continuous monitoring, risk assessment, and customized security controls. In Nepal, regulations such as the **Cybersecurity Byelaws (2020)**, **Nepal Rastra Bank IT Guidelines**, and **Nepal Beema IT Guidelines** focus on enhancing cybersecurity resilience across key sectors by enforcing practices like regular audits, penetration testing, and strong data protection mechanisms, aligning with global standards to safeguard against cyber threats.

Chapter 3: Analysis

3.1. Basis for Compatibility

A framework to be considered compatible with NIST 800-53 Rev. 5, ISO 27001:2022, and COBIT 5, it must meet the following criteria.

- i. **Governance and Leadership:** There should be provision for clearly defined roles and responsibilities, established with accountability at each leadership level, and must have integrated cybersecurity into their overall organizational strategies. ^{[4] [6]}
- ii. **Risk Management:** The framework adopted must have included policies that defines a clear structure for identifying, assessing, mitigating and continuously monitoring risks. This could include addressing risks from supply chain, and other interdependencies such as third parties. ^{[4] [5] [6]}
- iii. **Incident Response and Management:** There must be a clearly set structures for procedures to be applied in the process of detection, responding and recovering from any cyber incidents. These could include pre-defined simulation and response playbook, periodic testing to check the effectiveness of those plans. ^{[4] [5] [6]}
- iv. **Contingency Planning:** There should be provision for clearly set contingency plans that could address fallback mechanisms for critical system and services at the time of disruption. These include plans such as mitigating the impact of natural disaster, cyber-attacks, or system failures. ^{[4] [5] [6]}
- v. **Business Continuity Plan and Disaster Recovery:** It should include a robust business continuity plans for critical system and services to ensure uninterrupted operations during crises. These should account for data backup, redundancy, and recovery timeframe. ^{[4] [5] [6]}
- vi. **Security and Privacy Controls:** There should be defined instructions for advanced technical and operation controls, including encryption, multi-factor authentication, secure access protocol, and data masking techniques. The privacy controls should ensure keeping sensitive data protected at all stages of its lifecycle. ^{[4] [5] [6]}
- vii. **Employee and Stakeholder Awareness:** There should be well structured periodic training program for employees and stakeholders for increasing awareness about cybersecurity risk, compliance policies, and incident handling procedures for

minimizing the impact of cybersecurity incident. NIST's and ISO's have considered human factor as an important for the cybersecurity resilience. [4] [5] [6]

- viii. **Education and Capacity Building:** There ought to be inclusion of initiatives to educate teams and enhance technical capacity, focusing on evolving threats, standards and best practices, as specified by COBIT and ISO's. [4] [5] [6]
- ix. **Continuous Monitoring and Improvement:** It should include clear and firm inclusion for real-time monitoring systems, threat intelligence sharing, and iterative improvement of cybersecurity strategies. [4] [5] [6]
- x. **Performance Metrics and Accountability:** There should be clear definition of metrics to evaluate the effectiveness of cybersecurity measures, that includes response time, audit compliance rates, recovery time, and so on. Accountability mechanism must ensure that individuals and teams are held responsible for meeting cybersecurity guidelines and any other action. [4] [5] [6]

3.2. Procedure for the Analysis

Nepal's information security audit practices, as in the NTA Cybersecurity Byelaws 2020, Beema IT Guidelines 2019, and NRB Cyber Resilience Guidelines 2023 were evaluated with global standards such as NIST 800-53 Rev.5, ISO 27001:2022, and COBIT 5. A systematic approach was adopted to highlights the alignment, the gaps, the strengths and room for improvement. The approach is structured below.

- i. **Review of Nepalese and Globoal Frameworks:** NTA Cybersecurity Byelaws 2020, Beema IT Guidelines 2019, and NRB Cyber Resilience Guidelines 2023 are analyzed to evaluated them with global standards.
- ii. **Comparison:** The Nepalese Information security frameworks are compared with global standards, NIST 800-53 Rev.5, ISO 27001:2022, and COBIT 5.
- iii. **Evaluation:** Each Nepal's framework is mapped with the guidelines of all the three global frameworks to identifying the alignment, gaps and strengths.

3.3. General Practices in Nepal

Nepal's cybersecurity policies emphasize foundational measures like operational controls, risk assessments, and incident response. Governance is primarily at the board level, ensuring leadership accountability, but integration at lower organizational levels is limited.

While periodic risk assessments are mandated, frameworks lack provisions for managing supply chain and interdependencies. Privacy measures are weak, with limited emphasis on encryption and data protection. Disaster recovery mechanisms are present but lack comprehensive business continuity planning. Continuous improvement practices are evident in some sectors but inconsistent across frameworks. Overall, Nepalese policies provide a foundational base but require significant enhancements to align with global standards comprehensively. [7] [8] [9]

3.4. Case Study: Comparison of NRB Cyber Resilience Guidelines with Global Standards

A comprehensive comparison between NRB Cyber Resilience Guidelines and global standard is done for the demonstration of strengths and gaps.

3.4.1. Governance

It defines provision that requires board-level oversight and promoting IT governance structure within an organization. It closely aligns with ISO's ISMS frameworks, emphasizing governance integration at all levels. It meets governance principles set COBIT by clearly defining roles and ensuring strategic alignment with organizational objective. [4] [6] [8]

3.4.2. Risk Management

It addresses interconnection risk management and mandates regular risk assessment. It closely aligns with NIST's principle of risk management, however, lacks specific provision for supply chain risk management. The risk assessment is defined in the NRB guidelines, meeting ISO requirements, but lack integration into a broader ISMS framework. [4] [5] [6] [8]

3.4.3. Security and Privacy Controls

There is a provision that firmly focus on layered security and operational controls but there are limited privacy measures like data masking. It meets many NIST security control requirements. However, it does not clearly address privacy frameworks. It aligns with ISO's operational control requirements but lacks advanced privacy measures. [4] [5] [6] [8]

3.4.4. Incident Response and Recovery

It includes provision for collaborative response strategies and recovery plans, aligning well with NIST and ISO. It is partially aligned with COBIT, emphasized resources optimization for incident recovery, which is not defined in NRB's guideline. [4] [5] [6] [8]

3.4.5. Contingency Planning

The guidelines include provision for implementation of contingency measures but does not include any mechanisms for diverse crisis scenarios. This contrasts with NIST's operational resilience and COBIT's contingency planning with enterprise risk strategies. [4] [5] [6] [8]

3.4.6. Continuous Improvement

It strongly emphasis for regular update and testing, aligning with ISO's ISMS principles and NIST's adaptive controls. [4] [5] [6] [8]

3.4.7. Other Areas

It lacks comprehensive Business Continuity Plans (BCPs), and performance metrics like recovery times or incident response rates. Also, training programs are mandatory, however, there is no detailed implementation, and thus partially aligning with global standards. [4] [5] [6] [8]

3.5. SWOT Analysis



Figure 1: SWOT Analysis

Chapter 4: Conclusion

4.1. Results

The analysis of Nepal's cybersecurity frameworks, particularly the NRB Cyber Resilience Guidelines 2023, its alignment along with the gaps while comparing it with global standards, *ISO 27001:2022*, *NIST 800-53 Rev. 5*, and *COBIT 5*.

There is provision to include governance, board-level oversight to promote leadership accountability. It also emphasizes continuous improvements in the information security posture through regular updates and iterative refinement. Also, there is inclusion of operational measures like firewalls, incident response mechanism and vulnerability assessments.

However, the provision for risk management focuses only at interconnection risks with limited to no provision for supply chain and third-party risk management. The privacy control measures are limited with insufficient provision for encryption and data masking. Also, business continuity planning along with disaster recovery provision is not integrated into compressive strategies.

There is absence of measurable performance metrics to assess the overall cybersecurity effectiveness. Also, there is weak governance integration and lack of structured training programs and capacity building initiatives.

4.2. Discussion

Nepal's cybersecurity frameworks have a foundational structure for information security posture. However, it does not meet compliance with global standards' holistic requirements. Those frameworks emphasize for comprehensive integration across governance, risk management, privacy, and performance tracking.

The NRB Cyber Resilience Guidelines 2023 has provisions that's effective in governance and operational measures. However, it lacks advanced risk management and privacy control measures. There is absence of performance metrics and structured programs for employee and stakeholder training. These should be addressed to enhance the Nepal's information security posture for effective and safer digital realm.

4.3. Recommendations

The following recommendations are proposed to address the identified gaps in order to enhance Nepal's overall information security posture.

- i. **Governance:** The governance structured must be strengthen to ensure integration across all organizational levels. The IT strategies should comply with the organization's goal, aligning with COBIT principles for improving accountability and strategic alignment.
- ii. **Risk Management:** There should be proper introduction of provision for supply chain and third-party risk management. Implementation of comprehensive Risk Management Framework (RMF) should be done to address interdependencies and evolving threats comprehensively.
- iii. **Privacy Controls:** There should be comprehensive provision for advanced privacy measures such as proper encryption, data masking, and anonymization for improving and enhancing data security. These methods should align with international standards for privacy.
- iv. **Business Continuity:** There must be development and implementation of robust Business Continuity Plans (BCPs) integrated with disaster recovery mechanism is required. These should be periodically tested to ensure the operational capabilities.
- v. **Performance Metrics:** A proper measurable performance metrics like incident response times, recovery rates, and compliance outcomes must be defined. These metrics should be used to evaluate the information security effectiveness.
- vi. **Education:** A proper and structured cybersecurity programs should be developed for training employees and stakeholders. There must be investment in capacity building initiatives to develop technical expertise and raise awareness of emerging threats.
- vii. **Global Standards:** The policies and framework should be regularly updated to align with the latest international standards for information security. These frameworks should be used to address the existing gaps and improve alignment with global best practices.

References

- [1] Nepal Rastra Bank, "Payment Systems Oversight Report FY2022/23," Nepal Rastra Bank, Kathmandu, 2023.
- [2] Nepal Telecommunication Authority, "Management Information System," Nepal Telecommunication Authority, Kathmandu, 2014.
- [3] Nepal Telecommunication Authority, "Telecommunication Indicator Ashadh, 2081," Nepal Telecommunication Authority, Kathmandu, 2024.
- [4] International Organization for Standardization , "ISO/IEC 27001," International Organization for Standardization , 2022.
- [5] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," in *NIST Special Publication 800-53 Revision 5*, National Institute of Standards and Technology, 2020.
- [6] Information Systems Audit and Control Association (ISACA), "COBIT 5," in *COBIT 5: A Framework for the Governance and Management of Enterprise IT*, ISACA, 2012, pp. 1-10.
- [7] Nepal Telecommunication Authority, "Cyber Security Byelaw, 2077 (2020)," Nepal Telecommunication Authority, 2020.
- [8] Nepal Rastra Bank, "Cyber Resilience Guidelines," Nepal Rastra Bank, 2023, pp. 1-47.
- [9] Nepal Beema Samiti, "Nepal Beema IT Guidelines, 2076," Nepal Beema Samiti, 2076, pp. 1-7.