An Analysis of Isrm-Bcp Practices in Nepali Bfis

Prabin Mainali[1], Dr Pramod Parajuli[2]
[1]PG Scholar, Lord Buddha Education Foundation, Kathmandu, Nepal
[2]PGD Manager, Lord Buddha Education Foundation, Kathmandu, Nepal

Abstract

This thesis titled "An Analysis of Isrm-Bcp Practices in Nepali Bfis" examines Information Security Risk Management (ISRM) and Business Continuity Planning (BCP) within Nepali Banking and Financial Institutions (BFIs). Amid increasing cyber threats and regulatory complexities, this study explores the adoption and effectiveness of ISRM and BCP strategies, utilizing the Technology-Organization-Environment (TOE) framework. Through a mixed-methods approach, combining surveys and interviews, it identifies key drivers and barriers, including regulatory compliance and technological infrastructure. The findings highlight variability in practice maturity across BFIs and offer strategic recommendations for enhancing resilience against security risks and disruptions. This research contributes valuable insights to both academia and industry, aiming to fortify the stability and sustainability of Nepal's financial sector.

Keywords: *Information Security Risk Management (ISRM), Business Continuity Planning (BCP), Cyber threats*

1. Introduction

The banking sector in Nepal has experienced rapid digitalization, which, while enhancing accessibility and efficiency, has also introduced significant information security risks. This transformation demands robust Information Security Risk Management (ISRM) and Business Continuity Planning (BCP) strategies to protect sensitive financial data against cyber threats and ensure continuous business operations during disruptions. The chapter discusses how the integration of advanced digital technologies into banking operations has exposed financial institutions to increased risks of cyber-attacks, data breaches, and system failures.(Pokharel, 2021) It emphasizes the critical need for well-structured ISRM and BCP frameworks to mitigate these risks and ensure the stability and reliability of banking services.

2. Objectives

This research aims to provide a comprehensive analysis of the current ISRM and BCP frameworks in Nepali Banking and Financial Institutions (BFIs). The specific objectives are outlined as follows:

1. Evaluation of Existing Frameworks: To examine the current ISRM and BCP practices within BFIs to understand their scope, integration, and effectiveness in mitigating information security risks and ensuring business continuity.
2. Readiness and Resilience: To assess the preparedness of BFIs to handle security threats and disruptions, evaluating their resilience in maintaining critical operations under adverse conditions.
3. External Influences: To explore the impact of external factors such as regulatory changes, technological advancements, and emerging cyber threats on the adoption and effectiveness of ISRM and BCP practices.
4. Best Practices Identification: To identify and recommend best practices and innovative approaches from global and local contexts that could enhance the ISRM and BCP frameworks in Nepali BFIs.

3. LITERATURE REVIEW

The literature review begins with an overview of ISRM and BCP as critical components in safeguarding information assets and ensuring operational continuity in the financial sector worldwide. It discusses various models and frameworks commonly adopted, such as ISO 27001 for security management and the Institute's Good Practice Guidelines for BCP.(Joshi & Singh, 2017)
The review further explores case studies from international banks that have successfully integrated these practices, highlighting the benefits of robust ISRM and BCP frameworks in mitigating risks from cyber threats, natural disasters, and other disruptions.
The review then narrows down to the context of Nepal, where the banking sector is still developing its digital infrastructure amidst growing cybersecurity threats and a challenging regulatory environment. It discusses the impact of Nepal's geographic and socio-economic conditions on its banking sector, including high susceptibility to natural disasters which exacerbates the need for effective BCP measures.(Khadka, n.d.)
Specific challenges related to the adoption of ISRM and BCP practices in Nepali BFIs are detailed, such as limited technological resources, lack of skilled IT personnel, and regulatory complexities. These challenges hinder the effective implementation of comprehensive security and continuity strategies.(Gupta & Pokharel, n.d.)
One of the most significant gaps identified in the literature is the scarcity of empirical data concerning the actual adherence of Nepali BFIs to ISRM and BCP standards. Most existing studies provide theoretical models or anecdotal evidence without robust empirical support. The literature also reveals a gap in comprehensive, integrated frameworks that align ISRM and BCP with organizational strategies specifically tailored for the Nepali context. There is a need for research that bridges these gaps by providing data-driven insights and locally adaptable frameworks that can be implemented effectively in Nepal's unique banking environment.

2. Methodology

This chapter outlines the methodological framework employed in the study to investigate Information Security Risk Management (ISRM) and Business Continuity Planning (BCP) practices in Nepali Banking and Financial Institutions (BFIs). It describes the integrated use of quantitative and qualitative research methods to provide a comprehensive understanding of the phenomena under study.
Surveys were designed to collect quantitative data from a large sample of respondents across various BFIs in Nepal. This method enables the gathering of extensive data on the prevalence and effectiveness of ISRM and BCP practices. The surveys include closed-ended questions, which facilitate statistical analysis and ensure that data collection is standardized and replicable. This approach allows for a broad assessment of practices across the sector, highlighting trends and commonalities in ISRM and BCP implementation.
The survey targets IT managers, risk officers, and other relevant personnel involved in ISRM and BCP at their respective institutions. The structured nature of the surveys ensures that data collected are objective and quantifiable, making it suitable for statistical analysis to test hypotheses about the factors influencing ISRM and BCP effectiveness (Creswell & Creswell, 2018).

Qualitative Interviews

In-depth, semi-structured interviews are conducted to complement the quantitative data with qualitative insights. These interviews allow participants to discuss their experiences and perspectives

on ISRM and BCP practices in greater detail. This method is particularly useful for understanding the contextual nuances that influence the adoption and success of these practices in Nepali BFIs (Yin, 2014). The interviewees include senior managers and decision-makers who provide strategic insights into the challenges and drivers of ISRM and BCP practices. The qualitative data gleaned from these interviews help to interpret the quantitative findings and provide a richer, more detailed understanding of the underlying issues.

Framework

The TOE framework is utilized to analyze the factors influencing the adoption of ISRM and BCP practices. This framework posits that technology-related factors, organizational characteristics, and the environmental context significantly affect the adoption and success of technological innovations within organizations (Tornatzky et al., 1990). In this study, the TOE framework helps in identifying how technological capabilities (such as advanced cybersecurity tools), organizational attributes (including leadership support and cultural attitudes towards risk), and environmental factors (like regulatory requirements and competitive pressures) influence the implementation and effectiveness of ISRM and BCP in BFIs (Baker & Sinkula, 2005).

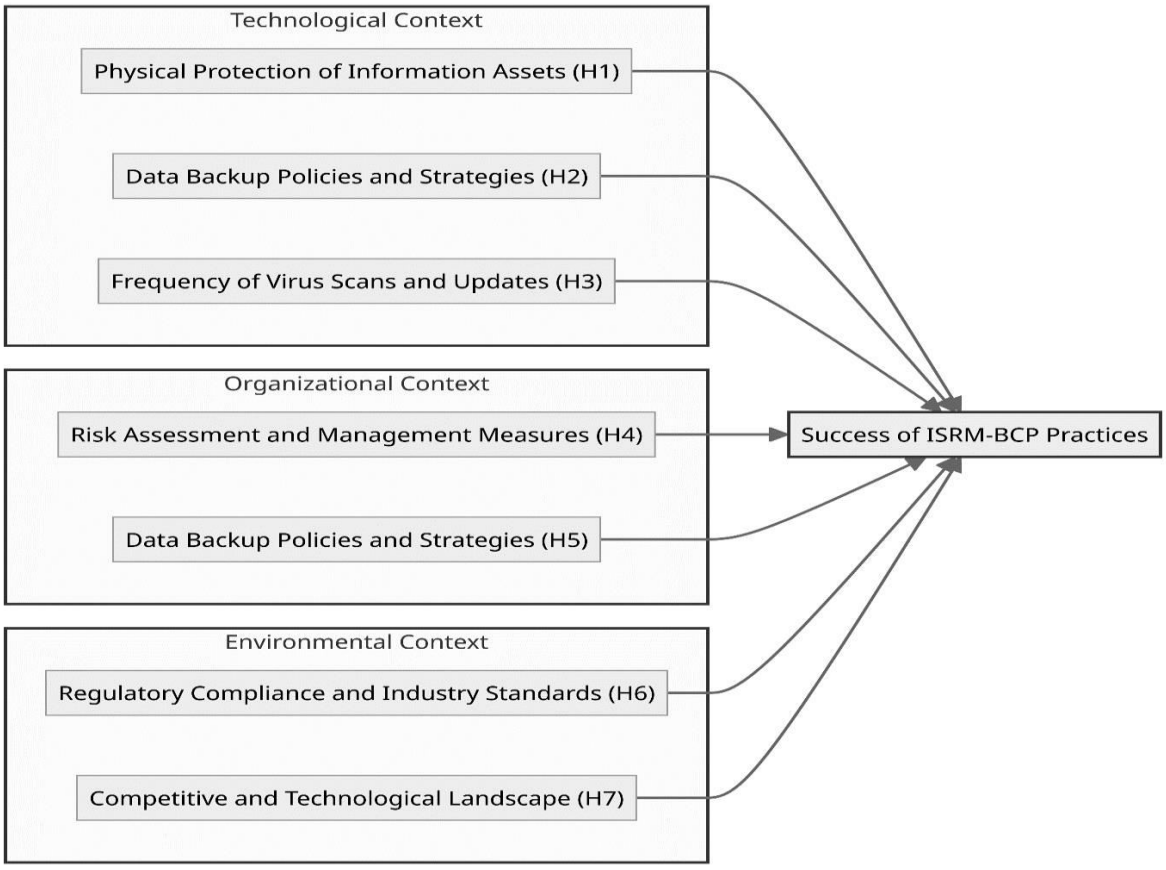

Figure 1:TOE Framework

The combination of quantitative and qualitative methods, supported by the TOE framework, provides a robust approach to investigating ISRM and BCP practices. This methodological triangulation not only enhances the validity of the findings by corroborating evidence from different sources but also enriches the study's insights into the complex dynamics of information security and business continuity planning in the Nepali banking sector.

3. Data Analysis

Reliability testing was performed using Cronbach's Alpha, confirming the consistency of the survey instruments across different segments. High reliability scores indicate that the survey instruments were well-suited for this research.

Table 1:Table of Reliability Statistics

Section	Cronbach's Alpha	Number of Items
Overall Survey	0.946	18
Technology Context	0.859	6
Organization Context	0.857	6
Environmental Context	0.846	6

The frequency analysis of this study examines the distribution of responses to a series of questions that explore the impact of technological, organizational, and environmental contexts on Information Security Risk Management (ISRM) and Business Continuity Planning (BCP) within Nepali Banking and Financial Institutions (BFIs). This analysis is crucial for identifying prevailing attitudes and uncovering how these contexts influence ISRM and BCP practices.

The frequency analysis of this study examines the distribution of responses to a series of questions that explore the impact of technological, organizational, and environmental contexts on Information Security Risk Management (ISRM) and Business Continuity Planning (BCP) within Nepali Banking and Financial Institutions (BFIs). This analysis is crucial for identifying prevailing attitudes and uncovering how these contexts influence ISRM and BCP practices.

Table 2: Combined Frequency Analysis Tables

Context	Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Technology	T1	10.4%	26.2%	33.7%	20.6%	9.2%
	T2	10.7%	23.7%	30.8%	23.7%	11.1%
	T3	12.1%	22.0%	35.1%	21.8%	9.0%
	T4	10.2%	23.0%	33.2%	22.8%	10.9%
	T5	10.7%	22.3%	29.1%	27.1%	10.9%
	T6	11.4%	22.8%	32.2%	24.2%	9.4%
Organization	O1	12.1%	24.5%	31.0%	20.6%	11.9%
	O2	9.7%	24.2%	32.4%	21.3%	12.3%
	O3	10.7%	22.5%	33.9%	20.8%	12.1%
	O4	9.7%	22.5%	36.1%	21.8%	9.9%
	O5	7.7%	25.2%	33.9%	20.6%	12.6%
	O6	10.9%	19.6%	35.4%	23.5%	10.7%

Environment	E1	9.9%	20.8%	36.3%	22.3%	10.7%
	E2	12.6%	20.6%	34.4%	22.3%	10.2%
	E3	10.2%	25.9%	30.8%	23.0%	10.2%
	E4	8.0%	25.9%	33.7%	22.0%	10.4%
	E5	10.2%	22.3%	34.1%	23.5%	9.9%
	E6	10.7%	20.6%	34.1%	24.0%	10.7%

Technology Context: Responses highlight a general ambivalence toward technology's role in ISRM and BCP, with a significant portion of participants opting for neutral positions. This suggests a cautious approach to technological implementations, with variations indicating context-dependent acceptance or skepticism.

Organizational Context: There is notable uncertainty among respondents regarding organizational practices, shown by the prevalence of neutral responses. This indicates potential areas for improvement in internal policies and practices to better support ISRM and BCP.

Environmental Context: Responses show a mixed perception of external environmental factors impacting ISRM and BCP. While there is recognition of their importance, the high rate of neutrality suggests a lack of clarity or agreement on how to effectively integrate these factors into existing frameworks.

This frequency analysis provides a comprehensive view of the attitudes and perceptions across technological, organizational, and environmental contexts within Nepali BFIs. It underscores the complex dynamics of acceptance and skepticism and highlights the importance of targeted strategies and policy interventions to enhance ISRM and BCP practices effectively.

Table 3:Descriptive Statistics of the response variables

Context	Mean	Median	Mode	Standard Deviation
Technology	2.9843	3.0000	3.50	0.87614
Organization	3.0238	3.0000	2.17	0.89394
Environment	2.9931	3.0000	3.17	0.87571

In the exploration of statistical relationships and predictive modeling, regression analysis is a foundational methodology. This section of the study employs regression coefficients to quantify the influence of independent variables (Technological Context [TC], Organizational Context [OC], and Environmental Context [EC]) on the dependent variable, Information Security Risk Management (ISRM). These coefficients measure the expected change in ISRM for a unit change in each independent variable, with other variables held constant.

The table 3 details the regression coefficients, providing insight into the magnitude and direction of each context's influence on ISRM:

Table 4: Regression Coefficients

Model	Unstandardized Coefficients (B)	Standardized Coefficients (Beta)	t-value	Significance (p-value)
Constant	0.198	N/A	2.672	0.008

TC	0.360	0.360	7.380	<0.001
OC	0.308	0.314	7.185	<0.001
EC	0.271	0.271	6.092	<0.001

Dependent Variable: ISRM-BCP

Analysis of Coefficients:

Intercept (Constant): The intercept, significant at p = 0.008, suggests a baseline effectiveness of ISRM practices, which can be enhanced through strategic initiatives within the examined contexts.

Technological Context (TC): With a coefficient of 0.360, this context shows a strong positive influence on ISRM success. This supports hypotheses H1-H3, suggesting that robust information protection, strategic data backups, and diligent updates and virus scans are crucial for strengthening ISRM and BCP practices.

Organizational Context (OC): The coefficient of 0.308 for OC underscores the importance of internal risk assessments and data backup strategies, supporting hypotheses H4 and H5. This highlights the critical role of organizational governance in aligning risk management with business continuity goals.

Environmental Context (EC): The coefficient of 0.271 for EC affirms the significant impact of regulatory compliance, industry standards, and the competitive and technological landscape on ISRM, backing hypotheses H6 and H7. This suggests that external factors are essential components of comprehensive risk management.

The significance of these coefficients across all contexts illustrates the multifaceted nature of ISRM-BCP. It highlights the synergistic effect of technological, organizational, and environmental practices on the robustness of ISRM initiatives. The findings validate the study's hypotheses and encourage the integration of these contexts into ISRM-BCP frameworks.

Using correlation and regression analyses, significant relationships were identified between the effectiveness of ISRM and the variables of Technology, Organization, and Environment, illustrating their combined impact on ISRM success.

The findings emphasize that technological resources, organizational policies, and environmental conditions significantly influence the efficacy of ISRM and BCP frameworks across BFIs in Nepal.

4. CONCLUSIONS

By merging theoretical frameworks with empirical evidence, the study bridged the gaps in existing literature, offering a detailed analysis of how these institutions manage security risks and maintain operational continuity amidst evolving threats and regulatory demands.

1. Variability in Framework Effectiveness: There is significant variability in the effectiveness of ISRM and BCP frameworks across BFIs, indicating a need for strategic improvements to enhance robustness and ensure resilience.
2. Diverse Levels of Preparedness and Resilience: Institutions show varied levels of preparedness and capacity to manage disruptions, emphasizing the need for targeted improvements to stabilize the sector.
3. Influence of External Factors: External factors such as regulatory demands and the changing landscape of cyber threats significantly impact ISRM and BCP practices, necessitating adaptive strategies within these contexts.
4. Discovery of Best Practices: Comparative analysis with global standards reveals successful strategies and innovative approaches that Nepali BFIs could adopt or adapt, setting benchmarks for framework enhancement.
5. Strategic Recommendations: Based on these insights, the study offers actionable recommendations to address challenges and leverage opportunities to strengthen ISRM and BCP frameworks within the sector.

These conclusions not only aim to fill the identified knowledge gap but also provide a comprehensive, empirically grounded examination of ISRM and BCP practices tailored to Nepal's

banking sector. The study's comprehensive analysis provides conclusive insights that confirm the proposed hypotheses, delineating the impact of various factors on the effectiveness of ISRM-BCP practices:

H1: Physical protection of information assets positively affects ISRM-BCP success, emphasizing the importance of robust security measures.

H2: Effective data backup policies within the technological context are crucial for the success of ISRM-BCP practices.

H3: Regular virus scans and timely updates are vital for maintaining a secure information environment.

H4: Organizational risk management measures are integral to effective ISRM-BCP practices.

H5: Organizational commitment to data backup strategies enhances ISRM-BCP outcomes.

H6: Regulatory compliance and industry standards significantly influence ISRM-BCP effectiveness.

H7: The competitive and technological landscape drives BFIs to adapt their ISRM-BCP practices continually.

These findings validate the study's objectives and hypotheses, providing a roadmap for strategic improvements and reinforcing the sector's resilience and security in an increasingly digital and interconnected environment.

This research makes significant contributions to both academic and practical fields, offering insights into the multifaceted nature of ISRM and BCP within the context of Nepali BFIs. It not only enhances the academic understanding of these practices but also offers practical recommendations for businesses to enhance their security and continuity strategies.

1. Academic Implications: The study enriches the theoretical landscape of ISRM and BCP by introducing empirical data from a less-explored geographical context, encouraging further research into the unique challenges and opportunities in emerging economies.
2. Practical Implications: For practitioners, this research highlights the importance of comprehensive risk management and the adoption of best practices. It provides evidence-based recommendations for enhancing ISRM and BCP frameworks, ultimately aiding institutions in mitigating risks and enhancing operational resilience.

In conclusion, through its detailed analysis and strategic insights, the study highlights the pivotal roles of technological innovation, organizational commitment, and environmental awareness in shaping effective ISRM and BCP practices.

References

Acharya, S., & Dahal, S. (2021). Security threats and legalities with digitalization in Nepal. *Research Nepal Journal of Development Studies, 4*(2), 1–15. https://doi.org/10.3126/rnjds.v4i2.42666

Baker, J. (2012). The technology–organization–environment framework (pp. 231–245). https://doi.org/10.1007/978-1-4419-6108-2_12

Bhat, S., & IAEME. (2023). Exploring the impact of digital transformation on the banking sector: Opportunities and challenges. *Open Science Framework.* https://doi.org/10.17605/OSF.IO/BU8EP

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage Publications.

Drazin, R. (1991). The processes of technological innovation. *The Journal of Technology Transfer, 16*(1), 45–46. https://doi.org/10.1007/BF02371446

Hollweck, T. (2015). Robert K. Yin. (2014). *Case study research design and methods* (5th ed.). *Canadian Journal of Program Evaluation, 30*(1), 108–110. https://doi.org/10.3138/cjpe.30.1.108

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35,* 128–137. https://doi.org/10.1016/j.jisa.2017.06.006

Pokharel, J. (2021). Banking sector development and economic growth in Nepal: Test of cointegration. *Management Dynamics, 24*(1), 27–42. https://doi.org/10.3126/md.v24i1.47540