INFOKUM
Volume 13, Number 03, 2025, DOI 10.58471/infokum.v13i03
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Cyber Security Incident Handling Model In Small Bank

I Wayan Wiasta Guna[1*], Eugene Ario Suradilaga[2]
[1*,2]Master of Information Technology, Swiss German University, Alam Sutera, Indonesia

Article Info
Keywords:
Cyber-Attacks, Risk Management, Incident Response

ABSTRACT
Bank digitalization is a breakthrough in this era. Almost all banks in Indonesia are competing to implement bank digitalization. However, this presents a new challenge in the form of a security gap called Cyber Security Risk. Ransomware and all the cyber-attacks that have recently occurred in several Banking and Finance areas in Indonesia have forced companies to rethink cybersecurity governance, bringing together all the essential things. Elements of practical cyber defense and risk management. This research aims to ensure that their security strategies and policies are implemented consistently and measurably by developing a Design Cyber Security Incident Response Model Based on DMAB SEOJK 03 2023 on Small Private Japan Bank in Indonesia.

Corresponding Author:
I Wayan Wiasta Guna
Master of Information Technology, Swiss German University, Alam Sutera, Indonesia
wayanayung@gmail.com

INTRODUCTION

Improving customer experience and increasing operational efficiency to reduce costs have been transforming Digital Technology. With the help of digital technology, banks can now process transactions faster, reduce costs, and offer personalized services to customers. Furthermore, digital technology has enabled banks to enhance security measures and prevent fraud through biometric authentication and real-time monitoring. Digital technology will continue to shape the future of the banking industry.

A January report from the Identity Theft Resource Center (ITRC) concluded a 78% increase in data compromises year-to-year, from 1,801 2022 to 3,205 in 2023. This indicates that 2023 was the worst year for data breaches in the United States and worldwide. Even as the global community fights against hackers, criminals constantly find new ways to access and exploit readable personal data, particularly when stored in the cloud. The numbers are staggering: The 3,205 compromising incidents in 2023 include 3,122 breaches of data, 25 data exposures, two data leaks, and 56 compromises of an unknown nature, according to the ITRC's report[2]. Further, this paper will discuss: 1. Introduction; 2. Definition and related work explain the differences between standards and frameworks, best practices and guidelines, and cybersecurity standards and frameworks; 3. Methodology; 4. Analysis and Discussion, 5. Conclusions.

Under the new regulations, the BUKU classification was replaced by the Bank Grouping based on Core Capital (KBMI) classification. This new classification system is as follows: a) KBMI 1: Banks with a core capital of up to IDR 6 trillion. b) KBMI 2: Banks with a core capital

INFOKUM
Volume 13, Number 03, 2025, DOI 10.58471/infokum.v13i03
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

between IDR 6 trillion to IDR 14 trillion. c) KBMI 3: Banks with a core capital between IDR 14 trillion and IDR 70 trillion. d) KBMI 4: Banks with a core capital of more than IDR 70 trillion.

This new classification system allows a more nuanced understanding of a bank's financial standing based on its core capital. Under Regulation 12, a BUKU 1 or BUKU 2 bank can be reclassified as a KBMI 1 bank, a BUKU 3 bank can be reclassified as a KBMI 2 or KBMI 3 bank, and a BUKU 4 bank can be reclassified as a KBMI 3 or KBMI 4 bank. This shift in classification methodology represents a significant step forward in the Indonesian banking industry's regulatory landscape, providing banks with greater operational flexibility and paving the way for more robust competition and innovation in the sector. Gorton (Gorton, 2014), in his work Using Incident Response Trees as a Tool for Risk Management of Online Financial Services, deploys defensive measures against cybercrime before a new attack. To sum up, the domain of cybercrime against online financial services has: 1) Relevant data: A limited number of online channels to attack (as seen from the financial institution). 2). A limited problem of underreporting. 3)The potential to allocate defensive measures that affect all avenues of attack. 4) A limited external visibility of internal countermeasures in advance (if we exclude insiders).

Yohannes, Lessa, and Negash, in their work "Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis" (Yohannes et al., 2019), Found that Bank X does not have a predefined and separate information security incident management plan that they follow strictly. Nevertheless, to some extent, they comply with international standards and guidelines, such as ITIL and ISO. Some procedures, such as incident classifications and escalation of incidents, are well performed. In their study titled "A new approach to analyzing business impact in business continuity management," Torabi, Soufi, & Navid introduce a method that involves creating an RWBS matrix to identify all functions necessary for producing essential products. Subsequently, these functions are ranked based on relevant criteria using a fuzzy DEMATE-NP method to pinpoint critical functions. Finally, a novel algorithm is employed to determine continuity parameters, such as MTPD and MBCO measures, for key products and their critical functions. Initially, the researchers use the RWBS matrix to list all functions essential for generating key products. Then, they use a method similar to fuzzy DEMATE-NP to prioritize these functions based on specific criteria, identifying the critical ones. Following this, a unique algorithm is applied to establish continuity parameters like MTPD and MBCO for key products and their critical functions.This approach defines the MTPD and MBCO for key products by considering the organization's risk tolerance level. Then, it determines the MTPD for critical functions using a straightforward algorithm.

METHODS

Cyber Security Maturity

These frameworks offer structured approaches to managing cybersecurity risks, which is particularly beneficial for smaller banks like Bank ABC, which may require additional cybersecurity resources. One such framework is the International Standard Organization (ISO) 27001:2013, which establishes global standards for managing information security (Herera et al., 2021). This framework emphasizes establishing a systematic process for identifying and evaluating organizational risks. Organizations can implement appropriate

INFOKUM
Volume 13, Number 03, 2025, DOI 10.58471/infokum.v13i03
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

controls and measures to mitigate these risks through this process. A vital aspect of this approach is conducting a thorough risk assessment, which helps organizations identify their sensitive information and assets and assess the potential impact of cyber-attacks or data breaches (Von Solm & Niekerk., 2013).

By prioritizing the protection of their most critical assets and information based on the assessment, organizations can ensure they have adequate measures to safeguard them. For small banks like Bank ABC, adopting these frameworks provides a structured way to manage cybersecurity risks and enhance the resilience of their computer systems (Drivas et al., 2017).

Business Impact Analysis

Several key steps are necessary to establish a comprehensive research framework for conducting a Business Impact Analysis (BIA) at a small bank like Bank ABC. The initial step involves collecting data, which is crucial in the BIA process and can be achieved through surveys and interviews with relevant organizational stakeholders. Surveys are beneficial for obtaining quantitative data on vital business functions, dependencies, and potential impacts of disruptions.

During the assessment of the BIA, information is gathered regarding the Business Unit Overview, starting with basic details such as the unit's name, manager's name, and staff count. We also delve into the operational processes of the business unit, including the average number of daily transactions or processes. Additionally, we identify critical periods, such as peak processing times like end-of-month salary processing and explore the interdependencies between different business processes and their potential impacts. This includes understanding processes that rely on others or could affect other business operations and identifying the systems and applications supporting these processes.

Moving forward, we assess the business process criticality level, which involves understanding the maximum tolerated outage and the maximum acceptable period during which a business process can be unusable during a disaster. We also inquire about the Recovery Time Objective and Recovery Point Objective to comprehend the continuity strategy without system support. Moreover, we discuss aspects like manual process execution, necessary personnel and equipment, and the time required for a complete manual process. We seek insights into testing business processes without system support and their success rate and investigating how long a business process can be sustained before significant issues arise.

The assessment then proceeds with quantitative and qualitative analyses, gathering data on average monthly and yearly revenue generated by the business unit. We also explore the link between business processes, government policies, regulations, and customer relationships

Disaster Recovery Exercise

One of the main goals of a disaster recovery test is to determine if a DR plan can work and meet an organization's predetermined RPO/RTO requirements. It also provides feedback to enterprises so they can amend their DR plan should any unexpected issues arise. IT systems rarely remain static, so new and upgraded products need to be tested again. Storage systems and servers may have been added or upgraded, new applications deployed, and older applications updated since an organization developed its disaster recovery plan.

INFOKUM
Volume 13, Number 03, 2025, DOI 10.58471/infokum.v13i03
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Alternatively, the private, public, or hybrid cloud may be more significant in an organization's IT infrastructure.

A disaster recovery test helps maintain a DR plan in a constantly changing IT world. IT systems rarely remain static, so new and upgraded products need to be tested again. Storage systems and servers may have been added or upgraded, new applications deployed, and older applications updated since an organization developed its disaster recovery plan. Alternatively, the private, public, or hybrid cloud may be more significant in an organization's IT infrastructure. A disaster recovery test helps maintain a DR plan in a constantly changing IT world.

Legowo and Juhartoyo (Legowo and Juhartoyo., 2022) concluded that the current maturity level had reached 75%, according to information gathered using a checklist based on Annex A of ISO standard 27001:2005. Business continuity management, which has reached a maturity level of 55%, requires a revision or improvement of business continuity management on their work "Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001."

Proposed Model

After analyzing the risk assessment of disaster recovery in small banks, the authors maintain the previous framework while expanding its scope to make it more applicable and relevant to a broader range of businesses. The NIST SP 800-30 Guide for Conducting Risk Assessments is widely used and adaptable. Similarly, ISO/IEC 27001 is globally accepted and thorough, while the Center for Internet Security (CIS) Controls are pragmatic and budget-friendly. Choosing a specific framework for risk assessment will depend on the organization's unique requirements, characteristics, and available resources and expertise.

As illustrated in the previous paper, a new risk assessment framework can be developed by considering the strengths and weaknesses of the NIST Cybersecurity Framework and the ISO 27001 Framework. By integrating these essential components, the new framework can overcome the limitations of existing ones and offer organizations a more efficient and practical approach to managing risks related to their information technology systems.

RESULTS AND DISCUSSION

Result

The framework result validation received positive feedback from the experts, indicating that the identified risks align well with the concerns in banking operations and the information technology domain. The experts acknowledged the significance of risks related to unauthorized changes to records, unintentional data changes, social engineering attacks, compromising confidential information, and the potential impact of these risks on regulatory compliance and reputational damage. However, some experts have emphasized the importance of addressing risks associated with poor culture and human error, which may require more attention in risk assessment. Additionally, the increasing sophistication of social engineering tactics and the rise of zero-day exploits were highlighted as factors that could elevate the probability of certain risks, such as social engineering attacks and malicious code.

INFOKUM
Volume 13, Number 03, 2025, DOI 10.58471/infokum.v13i03
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Discussion

Writers recommend that the bank exercise Cyber Incident BCP/DR using this model. The result will show how ready they are the employee to face cyber incidents, how aware all stakeholders are of the system risk, and how all of the Cyber Security Incident Response Team (CSIRT) and Departmental Security Incident Response Teams (DSIRT) follow the incident handling playbook guidelines

Figure 1. Result of Framework Control Mapping

Document Policies	Propose	Gap Analysis	Recommended Uplift
Asset Management Policy	Need to be Updated	Does not explain related to Implementation, User/Ownership, Technology Assets, exceptions, Inventory Systems of Record, Hardware Asset Inventory, Software Asset Inventory, Data Asset Inventory, Identity Asset Inventory, Audit and Physical Inventory, Acceptable Use of Assets, Implementation Plan, Maintenance, Consequences for Noncompliance,	The asset management policy should include Users/Ownership, Technology Assets, Exceptions, Inventory Recording System, Hardware Asset Inventory, Software Asset Inventory, Data Asset Inventory, Identity Asset Inventory, Physical Audit and Inventory, Acceptable Use of Assets, Implementation Plan, Maintenance, Consequences of Non-compliance,
Security Incident Management Policy	New Creation	Bank ABC does not yet have a policy document	Will formulate policies: 1. Incident handling 2. Incident monitoring 3. Incident reporting
Cyber Incident Response Plan Standard	New Creation	Bank ABC does not yet have a Standard document	Explaining related to Standards and Frameworks High-Level Incident Response General Security Incident and Response Communication: Internal Communications External Communication Incident Notification and Reporting. Incident Response Process: Detection, Investigation, Analysis, and Activation Containment, Evidence Collection, and Remediation Evidence Collection and Retention Remediation Action Plan Recovery Lessons Learned.
Information Protection Procedure	Need to be Updated	Bank ABC already has an SOP Information Leakage Prevention Rev. 2-01 document: a. Classification of general and specific customer data types per the PDP Law has yet to be created. b. Reporting if there is a leak/disclosure of personal data per the PDP Law does not yet exist	a. Classification of general and specific types of customer data, per the PDP Law, needs to be added b. Reporting in the event of leakage/disclosure of personal data per the PDP Law needs to be added
Disaster Recovery Plan Procedure	Fulfilled	No Gap, Bank ABC already has DRP documents: Core Banking, Internet Banking, SKN BI, RTGS, Internet & email	
Incident Handling Playbook	New Creation	Bank ABC does not yet have Incident Handling Playbook	Will formulate on : Incident Response definition, incident response team, incident response sub team, incident response team role and responsibilities, incident response tools, 15 most cyber attacks
Cyber Security Incident Response Team	New Creation	Bank ABC does not yet have Cyber Security Incident Response Team	Will formulate on : Incident Response member day-to-day job description, incident response call tree, departmental incident response team (DSIRT)

CONCLUSION

This paper also continues the previous work (Eugene and Mohammad., 2023) that give NIST Framework to cover Gap and weakness in Disaster Recovery process. While the Small Bank Cyber Security Incident Handling Model has demonstrated some effectiveness, aligning these plans with the NIST Framework guidelines can strengthen their effectiveness in addressing cyber security incidents, given Bank resource constraints through cost-effective and prioritized measures. These measures include investing in employee training and awareness programs, establishing regular testing and updating recovery plans, and implementing more comprehensive monitoring and incident response capabilities. In future work, the researcher suggests creating a new standard for Bank Compliance to comply with several standards, regulations, and business culture. This study also proposes that future research should seek a Maturity Assessment Model Based on digital forensic readiness and consider developing a combination maturity assessment model.

ACKNOWLEDGEMENT

We sincerely appreciate my esteemed colleagues at Adira Finance - Mr. Rizky, Mr. Budianto, Mr. Arifyanto, and Mr. Tomy. Your dedication, collaboration, and insightful perspectives have greatly enriched this research. We would also like to extend my heartfelt thanks to our

colleagues from Resona Perdania Bank - Mr. Stevie, Mr. Novi, Mr. Faizal, and Ms. Susanti. Your expertise, guidance, and partnership have been instrumental in shaping this thesis.

REFERENCE

Berger, A.N., Bouwman, C.H. and Kim, D., 2017. Small bank comparative advantages in alleviating financial constraints and providing liquidity insurance over time. The Review of Financial Studies, 30(10), pp.3416-3454 https://doi.org/10.1093/rfs/hhx038

Eugene, Suradilaga. and Mohammad, A., 2023. Enhancing Cybersecurity Posture: A Comprehensive Analysis of Risk Assessment of Disaster Recovery in Small Bank

G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook, and H. Janicke, "A NIS Directive compliant Cybersecurity Maturity Assessment Framework." arXiv, Apr. 22, 2020. Accessed: Apr. 28, 2023. [Online]. https://doi.org/10.1109/COMPSAC48688.2020.00-20

Gorton, D., 2014. Using incident response trees as a tool for risk management of online financial services. Risk analysis, 34(9), pp.1763-1774. https://dx.doi.org/10.1111/risa.12195

Legowo, N. and Juhartoyo, Y., 2022. Risk management; risk assessment of information technology security system at bank using ISO 27001. Journal of System and Management Sciences, 12(3), pp.181-199.Approach with another plan, such as comment, etc & 11.
https://doi.org/10.33168/JSMS.2022.0310

O. A. Fonseca-Herrera, A. E. Rojas, and H. Florez, "A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard," vol. 48, no. 2, 2021. IAENG International Journal of Computer Science, 48:2, IJCS_48_2_01

R. Von Solms and J. Van Niekerk, "From information security to cyber security," Comput. Secur., vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/. https://dx.doi.org/10.1016/j.cose.2013.04.004

Torabi, S.A., Soufi, H.R. and Sahebjamnia, N., 2014. A new framework for business impact analysis in business continuity management (with a case study). Safety Science, 68, pp.309-323. https:// doi.org/10.1016/j.ssci.2014.04.017

Yohannes, T., Lessa, L. and Negash, S., 2019. Information security incident response management in an Ethiopian bank: A gap analysis. Twenty-fifth Americas Conference on Information Systems, Cancun, 2019