JOURNAL LA MULTIAPP

VOL. 05, ISSUE 04 (361-379), 2024
DOI: 10.37899/journallamultiapp.v5i4.1399

Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework

Kamil Ryanto[1], Vitri Tundjungsari[1]

[1]*Faculty of Computer Science, Esa Unggul University,Jl.Arjuna Utara 9, Jakarta*

**Corresponding Author: Kamil Ryanto*
E-mail: kamilryanto26@esaunggul.ac.id

Article Info

Article history:
Received 24 June 2024
Received in revised form 12 July 2024
Accepted 29 July 2024

Keywords:
Standardization
Bank
ISO 27001:2022
Cyber Security
Evaluation

Abstract

This research discusses evaluations related to cyber security standardization in the banking sector at Bank Victoria International Tbk using qualitative methods and data collection techniques, interviews and focus group discussions. The focus of this research is evaluation related to Data Leaks, Threats of Attacks from outside, and Policies for preventing cybercrime in banking using the ISO 27001:2022 Framework. The location of this research was carried out at Bank Victoria International Tbk. The location for this research was chosen because Bank Victoria is one of the banks that is currently carrying out a preventive implementation process in preventing cybercrime by implementing ISO 27001:2022 related to Cyber Security. The problems that will be explained in this thesis research are First, how does PT. Bank Victoria is taking precautions regarding data leaks using the ISO 27001:2022 framework (1). Second, how does PT Bank Victoria carry out monitoring and monitoring related to external threats or attacks that could harm the bank using the ISO 27001:2022 framework (2). Third, how to comply with procedures, policies or regulators related to process flow and security controls for the use of information technology at PT. Bank Victoria uses the ISO 27001:2022 Framework (3). The conclusion of this research is that Bank Victoria International Tbk is still in the stage of improvement in terms of cyber security, although currently PT Bank Victoria is showing good preventive measures by forming a special organizational structure to handle legality issues and implementing cybercrime prevention applications, but this has not been stated in the Policy.

Introduction

The very rapid development of technology today means that companies and business people must be able to adapt quickly, the need for information and data connections to update information knows no time and place (Pereira & Romero, 2017; Mazzone et al., 2022). Information is one of the company's most important assets (Sims, 2022). With the rapid development of information technology, the possibility of information security disturbances is increasing (Tundis et al., 2019). For this reason, companies must implement appropriate policies to protect the information assets they own (Mohamed & Weber, 2020). Security issues are one important aspect of an information system (Seddigh et al., 2017). Often security issues come last on the list of things that are considered important (Colwill, 2009). If it disrupts system performance, security is often reduced or even eliminated (Zhang & Huang, 2017). Information in this era has become a very important commodity (Bosch et al., 2017).

PT. Bank Victoria International 'Tbk is a company that operates in the banking services sector and has high quality IT governance, therefore security management for Core Banking and

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Bank Operational Systems is very necessary in ensuring the security of information systems (Huang & Pearlson, 2019; Müller & Berg, 2019). An Information Security Management System (ISMS) or Information Security Management System (ISMS) is a set of policies and procedures for managing an organization's sensitive data systematically (Ramachandran et al., 2017). Therefore, information security indirectly guarantees the company's business continuity (Shaikh et al., 2019). It is important to implement an information security management system so that information circulating in the company can be managed correctly so that the company can make decisions based on existing information correctly in order to provide the best service to customers (Sun et al., 2019). This ISMS has three key components in providing guaranteed information security services, including Confidentiality, namely ensuring that information can be accessed only by those authorized to have access, Integrity, namely protecting the completeness and accuracy of information and processing methods, and Availability, namely ensuring that authorized users have access to it. information and connect with assets when needed (Integra technology solutions, 2023).

Companies need a framework for deciding what to do in information security management (Brotby et al., 2020). This framework was formed using the PDCA concept to ensure the company makes continuous improvements and uses mapping results from the ISO 27001 Standard to ensure threats and risks that may occur will not affect the company's main business (Aginsa et al., 2016; Watson, 2020). There are various information security standards currently in effect, the most widely applied is the standardization related to information management systems published by ISO 27001 (Humphreys, 2008). ISO 27001 is a special structured method for information security that is internationally recognized (Sims, 2022). ISO 27001 is an information security management system standard document, which provides a general description of what a company must do in their efforts to evaluate, implement and maintain information security in the company based on 'best practice' in information security (Seddigh et al., 2017).

In managing the security of surrounding applications and core banking systems owned by PT. Bank Victoria International 'Tbk, it is considered that the company still does not have IT governance capabilities that are in line with the expected competencies, and there is still a lack of supervision and assessment of system security, so there is a need for IT governance to ensure the security of surrounding application information and the core banking system (Ali et al., 2019; Ahmad et al., 2020). Therefore, in maintaining data and information security, it is necessary to carry out an IT Governance Audit to ensure adequate information security for surrounding system and core banking system applications in order to be able to plan and recommend improvements to weaknesses found, related to information system security using the ISO 27001 security standard (Cherdantseva & Hilton, 2013). ISO 27001 is needed because it has a fairly good inspection framework and is the most complete guide to best practices for information technology security management (Brotby & Hildebrandt, 2021).

Therefore, it is necessary to design an information technology model in managing information security for Core Banking and Bank Operational Systems, which can provide guidance in the form of improvement strategies and reducing security system weaknesses that must be followed up in improving the security quality of the core banking system, as well as recommendations for policy (Hwang et al., 2021). It is hoped that the recommendations provided can become a basis for directing information technology improvements in information security (Soomro et al., 2016). For this reason, the author has carried out research at PT. Bank Victoria International 'Tbk regarding the implementation of IT Audits with the security standardization of the ISO 27001:2022 Framework (Mace et al., 2022).

The ISO 27001:2022 framework is a standardization for information technology system security to meet the needs for Cyber Security, resources (Hard Skills and Soft Skills), and fulfill SOP or Regulatory policies that apply to PT. Bank Victoria International 'Tbk (Rehman

ISSN: 2716-3865 (Print), 2721-1290 (Online)

et al., 2020). With the 11 newest clauses in ISO 27001:2022, the 11 additional clauses focus on Cyber Security. Research concentrates on Data Leak Prevention, Security Intelligence, and Policies related to SOPs at PT. Victoria Bank (Ravindran & Sinha, 2022).

Methods

The chosen research method is case study, appropriate to offer a detailed examination of modern topic in a context of a real-life situation. Subsequently, this design facilitates an assessment of Bank Victoria International Tbk's cyber security programme as it moves towards implementing the ISO 27001:2022. As a research strategy, the value of case study is that it makes it possible for the researcher to obtain data that can be analyzed in detail in light of the immediate environment of the bank; this makes it possible for the researcher to develop findings that are grounded and useful in both theory and practice of information security management.

The study employed purposive sampling technique whereby participants in this study are involved directly with the banks IT and cybersecurity procedures. It also makes sure that only relevant information to the objectives of the study is collected and this makes the collected data to be of high quality. The sample contained ten respondents, one Divizion Head, four respondents Section Heads and five section staff of PT Bank Victoria IT Divizion. Such people were selected because they are directly involved in the execution and governance of the ISO 27001:2022 framework which makes them well-placed to give relevant information on the affairs of the bank's information security. This decision falls inline with the qualitative research methods which do not select large sample sizes but rather small specialized scrapes of population samples. The sample size was calculated basing on Isaac and Michael's calculation which estimated a sample size of 10 for a population of 10 so that all the stakeholders involved in the process were included.

The participants were interviewed using a semi structured questionnaire with questions primarily based on the 14 clauses of the iso 27001:2022 regulation. The questionnaire was developed to enable the respondents to express their views towards several aspects of the banks IMS, such as Data Leak Prevention, System Security, and Monitoring. The questions were framed in such a way that they invited both yes or no answer which suits quantitative analytical method and probing questions which are likely to elicit qualitative analysis. The questionnaire was first pre-tested in a small sample of the target population in order to ensure the questions were properly understood and answered and that the questions addressed the issues under investigation in the study. Those of the pilot test were used to tweak the questions with a view of ensuring that the right data was being captured in the best way possible.

This research was carried out for two months whereby the respondents got Qnaire information through completing it. Due to the fact that the area of inquiry was quite technical and required rather detailed answers, further GROUP interviews were conducted in order to discuss the answers and gather supplementary information where needed. These interviews were semi-structured, so that the interviewer could freely explore any themes or topics which were not originally planned for the research but which emerged during the first data collecting phase. Both authors conducted the interviews using digital audio recorders after obtaining participants' informed consent; all interviews were transcribed, and the transcriptions were scrutinised for analysis. While interviews together with questionnaires offered broader datasets, it was much easier to get deeper insights into the concerns of the bank in terms of cybersecurity.

The aggregation, synthesis and interpretation of data involved both the qualitative and the quantitative procedures. To analyze the quantitative data, which came from the socio-demographic questionnaire, descriptive statistics were employed: frequencies and percentages of variables. This approach entailed process of themes and pattern coding with

ISSN: 2716-3865 (Print), 2721-1290 (Online)

regards to implementation of the ISO 27001:2022 framework by the bank. The thematic analysis was done manually since the researcher needed to immerse himself in the data by closely focusing on a set of emerging themes made of challenges, accomplishment, and opportunities that the bank could consider for its ability to manage cybersecurity threats. The closed-ended questionnaire responses were quantified and analysed using descriptive statistics this gave an insight of the respondents' perception of the effectiveness of the bank's IMS on information security. The quantitative data were used together with the qualitative data in order to gain a more holistic picture on the actual state of the bank's cybersecurity.

Results and Discussion

Prevention of Data Leaks at PT. Victoria Bank

Information Security

Information security is an action to protect information from various threats that may occur, with the aim of ensuring business continuity, reducing business risks, and optimizing investment returns and business opportunities. [4] Aspects of information security include three things, namely CIA, including Confidentiality (secrecy), Integrity (integrity), and Availability (availability). These aspects can be seen as follows [3]: (1) Confidentiality Information confidentiality means protecting information from being accessed by unauthorized parties; (2) Integrity: Information integrity indicates that information must be intact and not subject to unauthorized or unwanted changes; (3) Availability Availability means ensuring that services, system functions and information are available to users when needed

Information Technology Risks

In the use of information technology, there are six categories of risks that need to be considered: (1) Security: The risk of changes or use of information by unauthorized parties; (2) Availability: The risk of data not being accessible after a system failure, caused by human error, agency configuration, or lack of use of appropriate architecture ; (3) Recovery: The risk of being unable to recover required information following failures in software, hardware, external threats, or natural disasters; (4) Performance: Risk of information not being available when needed, due to distributed architecture, high demand, and variations in information technology topography; (5) Scalability: Risks arising from business growth, regulatory constraints, and architectures that are unable to handle many new applications cost-efficiently; (6) Compliance: Risks related to the management or use of information that violates regulatory requirements, including government regulations, agency guidelines, and internal policies.

Factors Causing Customer Data Leaks in Financial Services

Based on the results of a review of several papers that I found, here are a number of factors that cause customer data leaks in financial services that have already been researched.

Aksenta et al. (2023) regarding protecting the confidentiality of investor data to prevent investor data leaks at the digital financial innovation company Goolive. One of the factors causing investor data leaks is hacking which often occurs in the SSL (Secure Socket Layer) security feature on the web. The same thing was also found by Ahmed (2020) regarding the use of personal data and customer identity in banking crimes, finding that data leaks were caused by breaking into customer data or accounts and duplicating consumer identities by financial services, Martin et al. (2017) found the factor of consumer data leakage due to parties breaking into customer data or accounts and duplicating consumer identities, Barona & Anita (2017) found customer data leakage due to a breach in the Internet Banking application used by customers.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Widyastuti & Sugianto (2020) in the paper Legal Protection of Debtor Data in Information Technology-Based Money Lending and Borrowing found that financial services use debtor personal data without the owner's consent to commit an unlawful act. Setyawan et al. (2024) financial services will leak consumer data to third parties if consumers cannot pay their bills or loans, Acquisti (2010) found a data leak factor because financial services provide personal information of service users and disseminate it to third parties to carry out unlawful actions, Aprilia (2021) found that financial services provide consumer data to third parties. The Desk Collector will access the debtor's data if the debtor is overdue for payment and disseminate the debtor's data via social media so that if the consumer is late in paying, ha This is also found in the results of Widadatul Rahmatullah research (2024) which found that financial services provided data to third parties by terrorizing consumers due to being late in paying bills.

Setiyawan et al. (2020) found that consumer big data had been leaked by irresponsible parties and misused Location-Based Messages to consumers by offering online loan offers. Soemitra (2022) who found that consumer data leaks were caused by negligence by financial services business actors, in this case Bank BNI, who handed over consumer data to a second party (insurance) without prior notification or confirmation to consumers verbally or in writing. This data is used to add or offer products for other financial institutions in collaboration with BNI. Dharani et al. (2024) found consumer data leaks caused by theft through phishing and misuse of one-time passwords or OTP. Alharbi (2020) that consumer data leaks are caused by hackers and malware via the internet system.

Table 1. Factors causing data leaks

No	Financial services sell customer data
1	Financial services provide data to third parties
2	The financial services party leaked customer data
3	Data theft via lending applications
4	Customers deliberately provide their personal data to financial services to carrying out loans
5	The customer opens the link in the email on the gadget sent by the person, when it is accessed open personal data.
6	Customers make purchases of goods online by stating three digit numbers back of credit and debit cards
7	Using the public internet so that personal data can be accessed by hackers
8	Malware viruses enter computer devices and absorb customer personal data and sending it to other people without the owner's consent

Data Leak Prevention Using the ISO 27001:2022 Framework at PT. Victoria Bank

PT Bank Victoria is a private bank that is currently developing into the digitalization area, where the products and services provided are PT Bank Victoria's superior products, such as: Deposits and the use of Mobile Banking and Internet Banking. To attract customers, PT Bank Victoria really thinks about service quality so that customers can feel comfortable using the products and services provided. Service quality is an attitude or assessment of the services that customers want with the services they receive. The concept of service quality includes efforts to meet customer needs and preferences as well as compatibility in service methods to match customer expectations so as to create a sense of satisfaction for them. Good service quality can take the form of providing adequate facilities and infrastructure, when customers carry out transactions they never experience problems or obstacles, and fulfilling customer expectations regarding the services provided by the bank will further increase customer loyalty.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Banks have an obligation to provide services to customers because banks must maintain a good image in the eyes of customers to maintain and build trust. Sitorus & Yustisia (2018) also stated that service quality has a positive and significant influence on customers, which means that the level of customer trust is influenced by the level of service quality. One of the important points to retain customers is to provide good service. Of course, customers will move elsewhere if the service provided is not optimal. This research is confirmed by Saulina & Syah (2018) who explains that good service quality will create trust or loyalty. If the quality of service provided by the company is in line with expectations and performance, consumers will be happy because the expectations and performance of the service are good and customer trust will directly arise in the company.

The introduction of Data Leak Prevention (DLP) controls in ISO 27001:2022 is important for organizations because it emphasizes the importance of protecting sensitive information and helps organizations identify, assess and prevent unauthorized disclosure of sensitive information. Implementing DLP controls is critical for organizations that handle sensitive information such as personal data, financial information, intellectual property and other confidential information. Whether government-owned or private, family-owned or multinational, an organization's intellectual property is often a key component of its competitive advantage, in terms of how it provides value that its competitors cannot provide. DLP controls help organizations identify and classify sensitive data, implement controls to prevent data exfiltration, and monitor suspicious activity. This can help organizations detect and respond to data breaches quickly, reducing the risk of financial loss, reputational damage and regulatory fines.

Financial loss, reputational damage, legal/regulatory liability, and criminal prosecution of perpetrators are just some of the potential impacts of a data leak incident. To address these issues, ISO Standard 27001:2022 has been updated to include clear guidance on what organizations need to consider, to ensure appropriate controls are in place, and managed through the organization's Information Security Management System (ISMS). Researchers created a framework of thinking related to preventing data leaks carried out by PT Bank Victoria, which was outlined in a questionnaire distributed to several work units such as IT, Digital and Products. The following framework of thinking consists of:

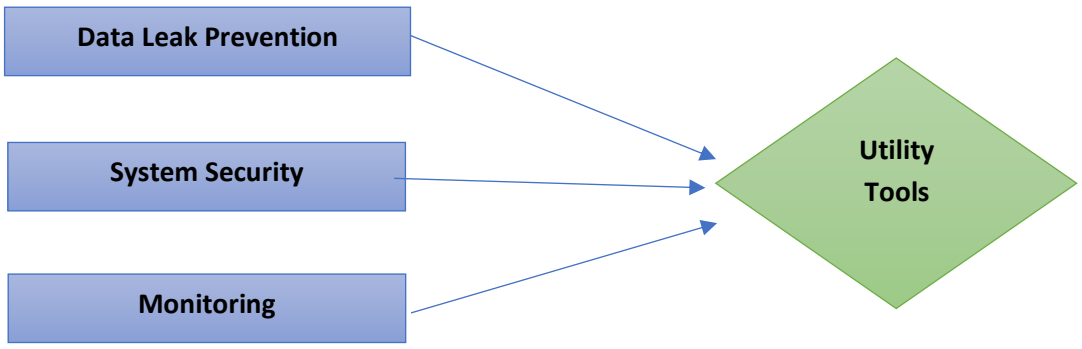


Figure 1. Thinking Framework

Figure 1 below presents the “Thinking Framework” used in the research done in PT Bank Victoria specifically on Data Leak Prevention (DLP), System Security, Monitoring under the ISO 27001:2022 framework. It is crucial to note that in its scale, this framework places specific priority on the integration of all of these key factors in the construction of schema for sound cybersecurity practices. Data Leak Prevention serves the purpose to prevent the leakage and breach of confidential data whereas System Security helps to protect the IT structure and vital operations of the bank. The third one is monitoring and it involves constant surveillance of the security environment as well as identification of threats in real-time for the purposes of

ISSN: 2716-3865 (Print), 2721-1290 (Online)

determining whether the counter measures that have been put in place are still effective and whether they are in compliance with the standards that have been set. In combination they form a balanced risk management strategy to assert the cybersecurity threats, which focuses on information resources protect in the bank.

Table 2. Percentage

No	Statement	Percentage
A. Data Leak Prevention		
1	I feel worried that there will be misuse of my personal data and funds at PT Bank Victoria if there is a Customer Data Leak	10%
2	Experiencing access problems or errors with the PT Bank Victoria Mobile Banking service	20%
3	The possibility of spreading negative information related to PT. Bank Victoria consequences if there is a customer data leak	20%
4	Ease of Procedure	80%
B. System Security		
1	The system at PT Bank Victoria has not yet been standardized	40%
2	Ease of use of systems such as: Mobile Banking, Internet Banking, and Website	90%
3	Security System Capabilities of PT. Victoria Bank	90%
4	Data and information security guarantee at PT Bank Victoria is in accordance with ISO 27001 standardization	90%
C. Monitoring		
1	The availability of monitoring tools related to security is reliable	90%
2	Ease of searching for information on system problems easily	90%
3	Speed of handling problems according to SLA	99%
4	The accuracy/precision of the monitoring system used is very accurate	95%

The survey data presented in the table above shows that in regard to the ease of procedures related to data leak prevention, 80 percent of the respondents are satisfied, but there are still 10 percent, who are worried about misuse of personal data and funds if the data were leaked. At the same time, 20% said that they faced the problem of limited access to the bank's Mobile Banking service, and the same percentage of respondents are concerned with the dissemination of undesired information if cyber-attacks take place. As far as system security is concerned, 90% of the respondents agree that data and information security provisions are satisfactory in compliance with ISO 27001 standard, security system capability and ease of use. However 40% gave a concern that the overall system has not been fully standardized. Monitoring is highly appreciated where 95% of respondents agree with the accuracy and precision of the monitoring systems; 99% of respondents satisfied with the speed of problem resolution according to SLA and 90% of the respondent found the availability of monitoring tools satisfactory and easy to search for the system issues.

The result of respondents' perception concerning the effectiveness of data leak prevention measures of PT Bank Victoria is captured in figure 2. Respondents' view shows that stakeholders are worried, as confirmed by 10% of the participants who said that they would get worried if their personal data and funds are misused in case of a customer data leak. This figure highlights perceived risks under the current information security situation in the context of the bank with an emphasis on the protection of customers' information.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

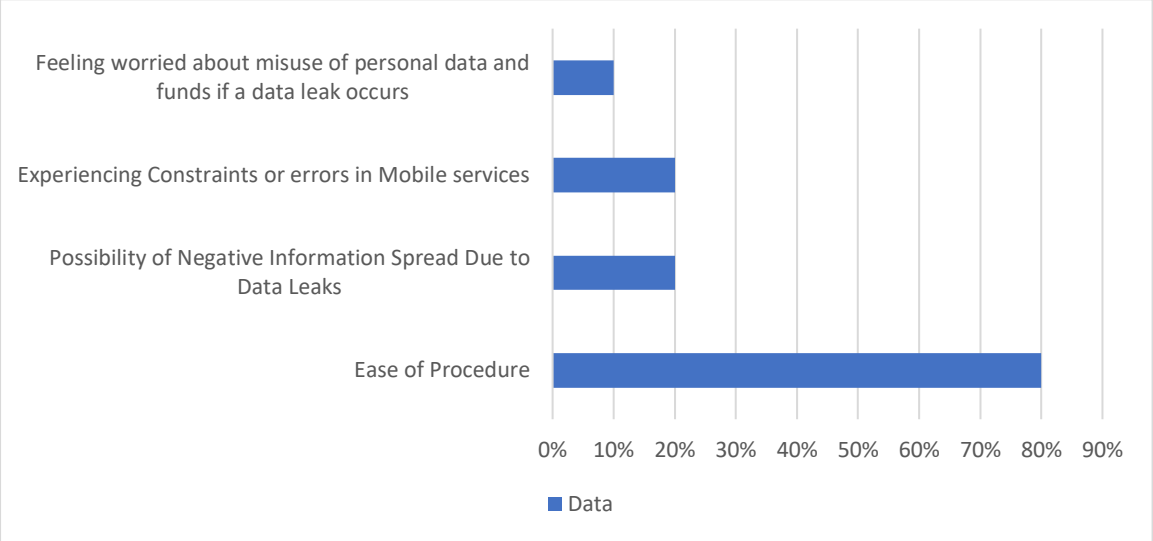
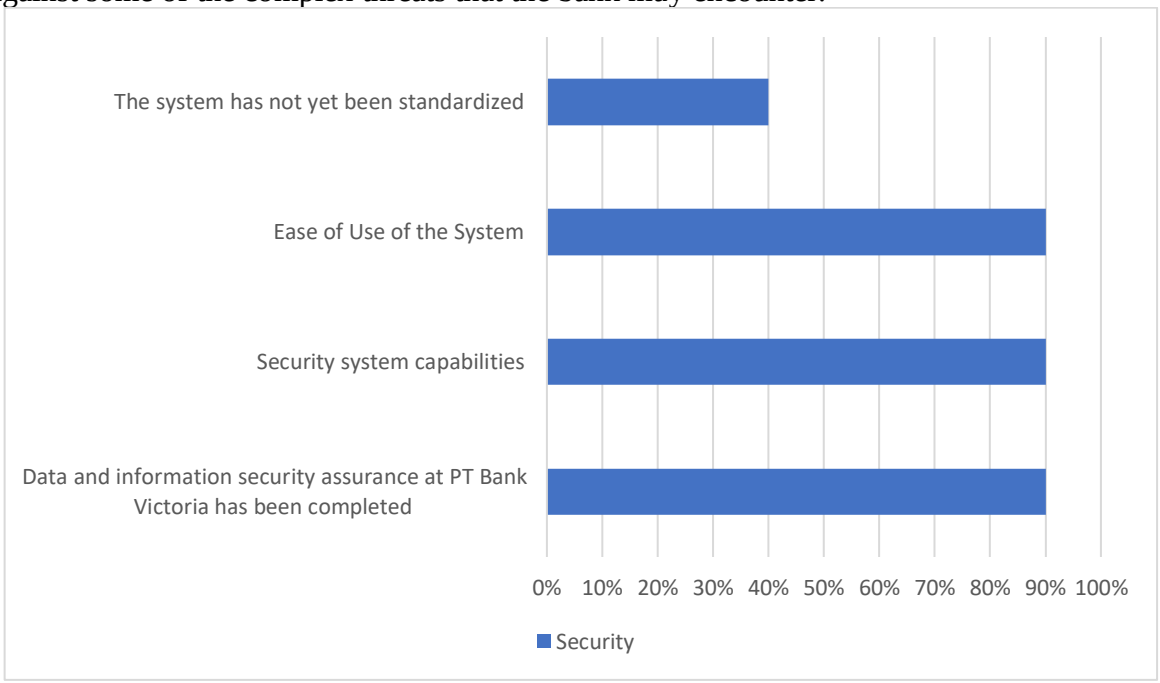


Figure 2. Data Leak Prevention

The data also suggests that 20% of the respondents complained about access problems or errors with the bank's Mobile Banking services this may mean that the bank has some technological problems that may lead to potential data breach. Further, 20 percent of the respondents raised the issue of publicity in the case of data breach; this is likely to expose organizations negative information. Notably, 80% of respondents feel that ease of procedures implemented for data leak prevention is satisfactory implying that although the process implementations that have been done might be easy, they might not offer sufficient protection against some of the complex threats that the bank may encounter.



The findings on the respondents' ideas regarding the security systems at PT Bank Victoria are presented in the Figure 3 as well. figure also reveal that 90% of the respondents agree with statement that the bank has standardized data and information security in accordance with ISO 27001, but still there is concern in standardizing the overall system, as 40% of the respondents argued that the system is not yet fully standardized.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

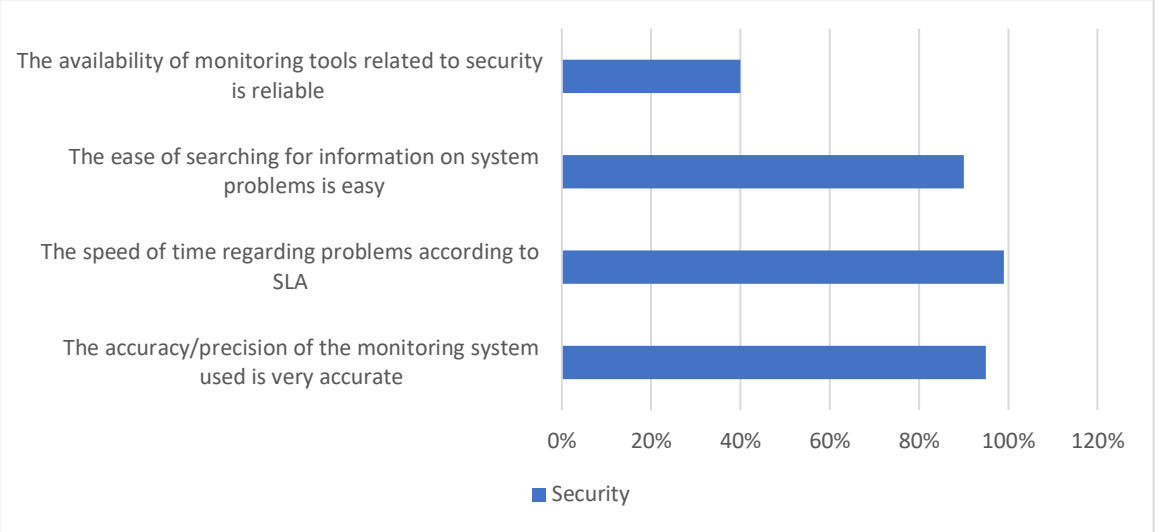


Figure 3. Security

With regards to the last two statements which are 'To what extent do you agree with the following statement – 'The current security system has enough capabilities?' 90% and 'How easy or difficult is it to manage the security system of this bank? 90% ' it has been established that the existing bank security is highly rating by the respondents. Though a little over one-half of the respondents expressed the opinion that, the system has not yet been standardised, the 40% result probably indicates that the level of security implementation might still be inconsistent or below standard across the organisation. This finding also elicits questions regarding the equilibrium of the bank's security practices where some areas maybe less compliant to ISO 27001 than others.

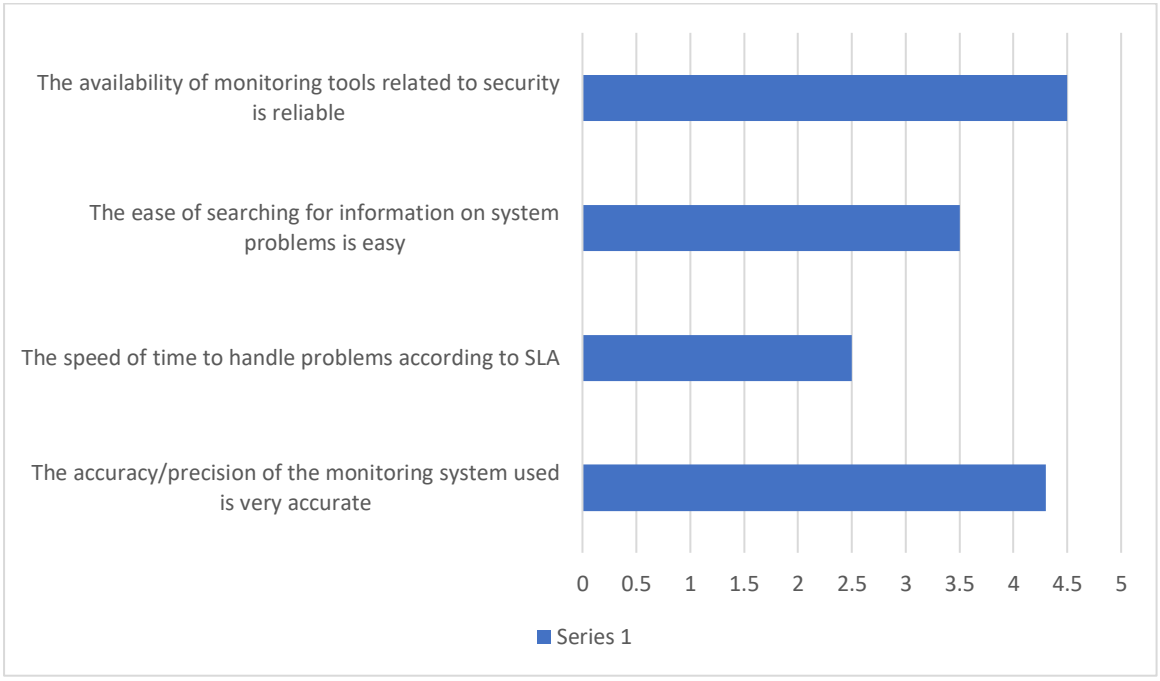


Figure 4. Monitoring

From the results of the distribution of questionnaires carried out by the researchers, there were 10 people. The results of the questionnaire consisting of Data Leak Prevention, Security and Monitoring obtained the results as described above. From the table above we can see that there is still concern about data leaks of 10% and the spread of information if there is a data

ISSN: 2716-3865 (Print), 2721-1290 (Online)

leak to parties outside the Bank carried out by parties involved. irresponsible by 20%. Apart from that, regarding system security, it still does not meet the standard of 40%.

It is difficult to eradicate data leaks completely. However, to reduce risks that occur in Bank operations, based on ISO 27001:2022 compliance guidelines Appendix A 8.12 Institutions must: (1) Organize data in accordance with institutional standards (PII, commercial data, product information) to determine different risk levels; Carefully examine data outlets that are (2) frequently used and susceptible to leaks (e.g. email, incoming and outgoing file transfers, USB gadgets); (3) Be proactive in protecting data from exposure. Implement strong file restrictions and set up appropriate authorization methods; (4) Limit users' capacity to copy and paste data (if applicable) only to and from certain platforms and systems; (5) Before large-scale exports occur, require authorization from the data holder ; (6) Think about regulating or stopping users from taking screenshots or taking monitor images that show protected data types; (7) Encrypt all backups that have sensitive data. Ensure all confidential information is safeguarded; (8) Establish gateway security and leak prevention measures to protect against external influences, including (but not limited to) industrial espionage, sabotage, commercial interference and intellectual property theft; (9) Data leak prevention is closely related to other ISO security guidelines aimed at protecting information and data across corporate networks, including access control.

Based on these compliance guidelines, currently at PT Bank Victoria the tools for data prevention are still not optimal, the following are the parameters at PT Bank Victoria related to preventing data leaks based on the ISO 27001:2022 compliance guideline Appendix A 8:12:

Table 3. ISO 27001:2022 Compliance Guide at PT Bank Victoria

ISO 27001:2022	PT Bank Victoria
Data management is in accordance with institutional standards	Regarding data management, it is in accordance with institutional standards
Device restrictions such as (email, incoming and outgoing file transfers, USB gadgets)	Regarding device device restrictions, it is still not optimal because users can still transfer files in and out and can still use USB gadgets to copy and paste data from cellphone to computer and vice versa.
Enforce file restrictions	Regarding file restrictions, it is still limited to sending emails, but regarding the use of the data file limitation process, it has not yet been realized
prepare strong authorization regarding data security	lack of authorization regarding data security
limiting user capacity to copy and paste data only to and from certain platforms and systems	There is no procedure for limiting user capacity to copy and paste from certain platforms and systems
prior to large-scale export, requires authorization from the data holder	related to this process, not all large-scale export systems use authorization from data holders. Only core banking uses authorization
Restrictions on the use of taking screen captures or images using screen capture	there are no restrictions or precautions regarding screen or image capture
Excrypt all backups that have sensitive data	In general, not all data has been extracted

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Establish gateway security and leak prevention measures to protect against external influences	Regarding gateway security, it is currently still in the process of being refined, and is still in the implementation process regarding several tools for the information security system.
Data leak prevention is closely related to other ISO security guidelines aimed at protecting information and data across corporate networks, including access control.	Currently PT Bank Victoria is in the ISO 27001:2022 certification process

Based on the results of research related to the compliance guidelines in ISO 27001:2022 Appendix A 8:12 at PT Bank Victoria, seen from the table above there are still procedural discrepancies where the implementation of preventing data leaks at PT Bank Victoria is still not in accordance with the ISO 27001:2022 Compliance Guidelines Appendix A 8 :12.

In addition to the compliance guide, in Appendix A 8:12 there is a data leak tool guide based on ISO 27001:2022. Institutions should consider using dedicated data leak tools and utility programs that: (1) Collaborate with the organization's data classification system and identify potential data leaks in high-risk categories. (2) Be proactive in detecting and alerting on data transfer/disclosure, especially on unapproved systems, file sharing sites, or applications. (3) Be aware of the risks associated with certain data transfer techniques, for example transferring financial data from a database to a spreadsheet. (4) Data leak prevention tools are inherently intrusive and must be used and managed in accordance with applicable regulations or laws regarding user privacy.

Based on the information above regarding the data leak tool guide, currently PT Bank Victoria has not yet implemented special devices/software/utilities to prevent data leaks or DLP related to securing sensitive data. PT Bank Victoria is currently preventing data leaks by restricting folder sharing, installing antivirus on every computer device and security from the network side related to firewalls. The following are several utility / software solutions that researchers know about, which could be a solution for implementing DLP at PT Bank Victoria.

Its primary purpose as a data security solution, to stop end users from sending sensitive or critical data outside an organization's network using a variety of techniques, tools and methods, monitoring, detecting and blocking sensitive data while it is in use, in motion by monitoring, identifying and prevent potential data breaches and data exfiltration attempts. CybelAngel detects data leaks using a combination of machine learning and cyber analysis, performs data breach prevention and CybelAngel finds, identifies and eliminates data leaks with machine learning. Complete data leak prevention and detection through dedicated data leak detection techniques and continuous attack surface monitoring. *UpGuard BreachSight* Continuous attack surface monitoring, Finds leaked employee credentials exposed to the public Internet Identifies software vulnerabilities that can facilitate data leaks. *UpGuards VendorRisk* Continuous third-party attack surface monitoring, Identifying software vulnerabilities that could facilitate third-party data leaks.

Tabel 4 Summary Threat Januari 2024

No	Description	Januari
1	Traffic Threat	642,649,430
2	Virus Threat	71
3	Application Threat	1,866,990
4	IPS (Intrusions Prevention System) Threat	1,342
5	Email Threat	190
6	Spam Email	32,747

ISSN: 2716-3865 (Print), 2721-1290 (Online)

7	Antivirus Report (Remove-Quarantine)	741

The table highlights several areas where the bank's practices fall short of full compliance. While data management aligns with institutional standards, there are significant gaps in device restrictions, file restrictions, and authorization procedures, indicating that users can still transfer files and use USB gadgets without adequate controls. Additionally, there are no procedures in place for limiting the capacity to copy and paste data across platforms, and the large-scale export of data often occurs without proper authorization. Other issues include the lack of restrictions on screen captures, incomplete encryption of sensitive data backups, and the ongoing refinement of gateway security and leak prevention measures. This assessment suggests that PT Bank Victoria is in the process of implementing these security measures but has not yet achieved full compliance, highlighting the need for further improvements to meet the ISO 27001:2022 standards fully.

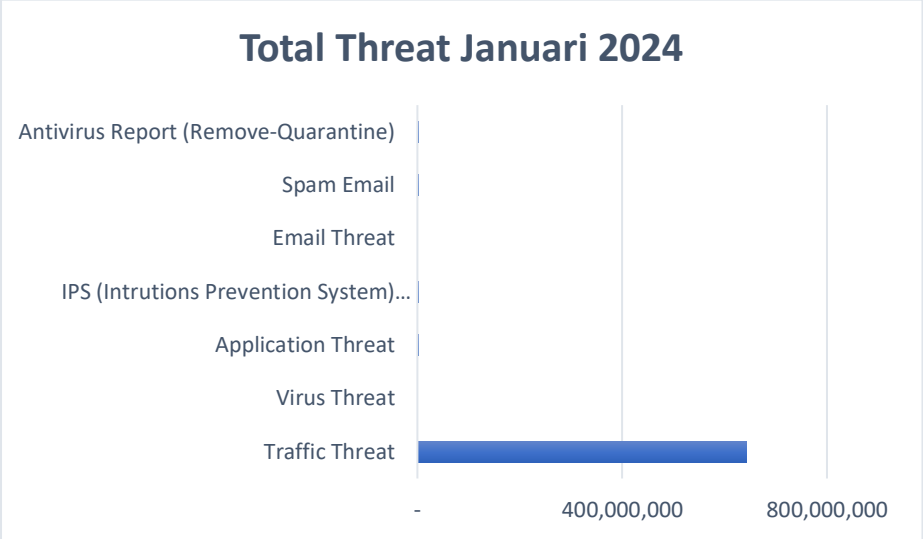


Figure 5. Total Threat in January 2024

In figure 5 below, the distribution of the different types of risks faced by PT Bank Victoria in January 2024 is presented. Therefore, the highest note worthy observation was made on the "Traffic Threats" category which notched a staggering 642,649,430. This category alone greatly eclipses the other threats proving that a significant amount of network traffic poses a threat to the bank, hence the need to perform constant monitoring and filtering. 'Application Threats' were the second, accounting for 1,866,990 hits, meaning that weaknesses in the applications of the bank are still a problem. Several of these threats may indicate vulnerability within the application security layer which if unchecked can be exploited. The 32,747 instances of "Spam Emails" were recorded here which tends to be rather lesser compared to traffic and applications threats but still considerable. This highlights the fact that traditional and simple methods such as phishing and email attacks are still prevalent, and therefore such attacks have to be addressed continually.

Other categories like that of "Virus Threats," "Intrusion Prevention System (IPS) Threats," and "Antivirus Reports" stand for less frequent phenomena but it does not exclude the fact that they are also potential threats to the bank's security. That "Traffic Threats" occupies the most striking position indicates that the main source of risk for the bank is in the transport layer. This requires concentration on the robustness of traffic analysis and the ability to filter out bad traffic which poses a significant threat to a particular system. The figures that are comparatively though still substantial in the other threat categories show that the threats are diverse thus calling for an integrated approach to their management to secure the bank.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Tabel 5. Summary Threat Januari 2024

No	Description	Maret
1	Traffic Threat	136,186,498
2	Virus Threat	17
3	Application Threat	3,001,847
4	IPS (Intrusions Prevention System) Threat	309
5	Email Threat	322
6	Spam Email	126,328
7	Antivirus Report (Remove-Quarantine)	365

This is evidenced by the number of "Traffic Threats" which has reduced from 642,649,430 in January to 136,186,498 in February showing that threats to traffic were addressed and reduced in this month. Nonetheless, 'Application Threats' were significantly higher, rising from 1,866,990 in January to 3,001,847 in February which infers to a shift in the threat vectors where the threat actors turned to application layer attacks more frequently. Further, as for the email-based threats "Spam Emails" the values raised dramatically from 32 747 to 126 328. The other categories including 'Virus Threats,' 'IPS Threats,' and 'Antivirus Reports' rose and fell to a much lesser extent but did not wane significantly. The migration of threats directs attention to the fact that cybersecurity is not a static endeavour, and combating one type of threat may result in the creation of other threats that need to be addressed continuously and dynamically by PT Bank Victoria.

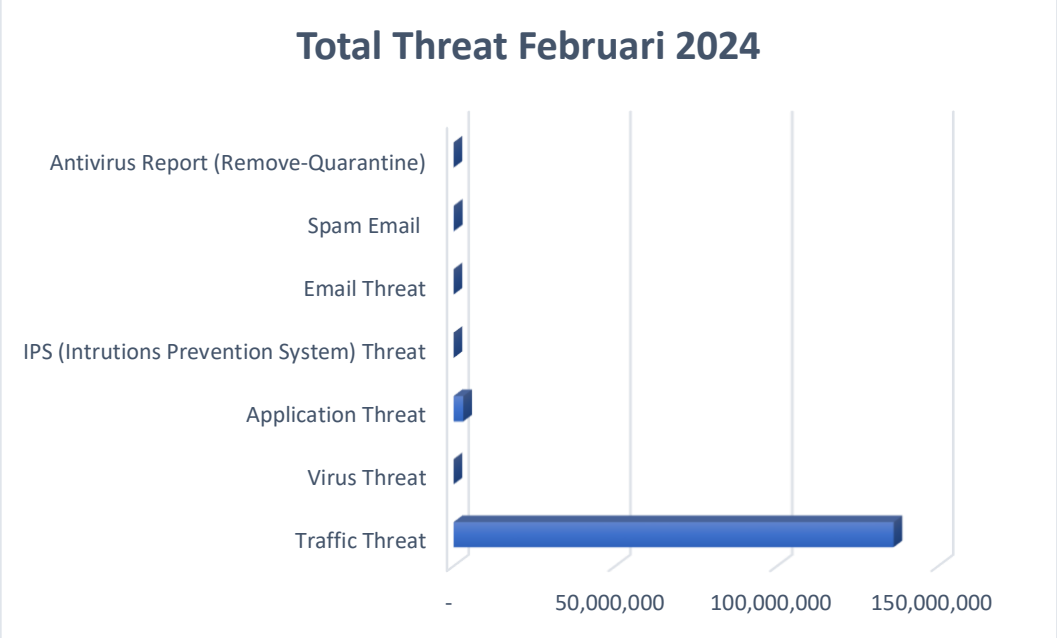


Figure 6. Total Threat Januari

This figure illustrates security threats that affected PT Bank Victoria in February 2024 as highlighted below: The nature of threats detected in February 2024 reveals a different trend from the one detected in January 2024 as illustrated in the figure below; The largest difference is observed for "Traffic Threats" which has slightly more than halved from a count of 335,432,540 to 136,186,498. This reduction show that the bank perfected way of managing these threats most probably by improving on the traffic filtering and monitoring. On the other hand, the cases under "Application Threats" shooting to 3,001,847 from 1,501,003. This rise demonstrates that even though, the bank has managed to reduce the network-level threats, the dangers at the application level have emerged. It is for this reason, the category "Application Threats" has risen; it would be beneficial for the bank to seek to have a more robust

ISSN: 2716-3865 (Print), 2721-1290 (Online)

applications protection probably through more thorough evaluations of potential application risks and execution of patch management.

The “Spam Emails” also received a huge boost with instances shooting to 126,328. suggests that there is an increase in the number of phishing and email-based threats and if not well handled, it could result to data breaches. The growth of what is known as “Spam Emails” emphasize the need to improve the security of emails that companies use and make their employees more aware of phishing. The numbers for “Virus Threats,” “Intrusion Prevention System (IPS) Threats,” and “Antivirus Reports” are still quite low (17, 309 and 365 respectively) but are slightly different from the values recorded in January. Such figures imply that these threats are effectively contained, although this requires a constant monitoring and enhancement of the bank’s security arrangements, as and when necessary.

In this respect, the data presented indicates that although PT Bank Victoria has ensured measures against leakage of data, huge loopholes exist. Such findings coincide well with the modern research that describes the issues of proper adoption and management of data leak prevention (DLP) controls, largely due to challenges related with integration of the selected controls on the existing IT environment (Xu et al. , 2023; Wang & Su, 2022). The questions raised by 10% of the participants about availability of personal data and funds for misuse is therefore a reflection of a wider problem of trust on financial organizations especially on the ability of the organizations to protect sensitive information that is vital in retaining customer confidence (Solms & Van Niekerk, 2022). This inconsistency in the type, extent, and applicability of device restrictions, coupled with the noted absence of a broad range of rules that govern data transfer and export processes as Table 4 points out, is perhaps one of the best evidence supporting the need for a more sound approach to DLP. prospects that are not solely specific to PT Bank Victoria; similar issues have been established in other financial organizations, especially when implementing and developing ISO 27001:2022 (Algarni & Xu, 2024; Martin et al. , 2023). These gaps will be solved not only through technologically oriented measures but also through the change of organizational culture that will put the focus on the question of cybersecurity at all levels of the enterprise (Cheng et al. , 2024).

According to the findings of the study, although 90 percent of the respondents stated that the bank has adequate measures of system security to meet ISO 27001 standards, it is also realistic to realize that 40 percent of the system does not have full standardization yet (Alcaraz & Zeadally, 2015). This is true in the case of completing ISMS, where there is usually a step-by-step process of full compliance at the system level, but where full integration is always left incomplete (Peltier, 2016). The difference between perceived security and actual standardization makes me think that the bank might target compliance in areas that are safe while at the same time having flaws in others; in other words, it might become risky (Tounsi & Rais, 2018). In the literature, it is established that it is cost-effective to implement an integrated system in which every aspect of an ISMS is protected and under surveillance at all times (Soomro et al., 2016; Mellado et al., 2014). PT Bank Victoria’s case proves the axiom that improvement and update of security should be considered an ongoing process whereby all the IT components at the company in discussion have to be revised in accordance with the requirements of ISO 27001:2022 (Susanto et al., 2011). This is especially important because the nature of cyber threats is constantly changing, which requires a dynamic approach that is capable of managing emerging threats when they come up (Fernández-Medina et al., 2017; Alcaraz & Lopez, 2013).

The findings, which showed that 95% of the respondents agreed with statements of accuracy and precision of the monitoring systems, mean that PT Bank Victoria has put in place a policy that enables the organization to detect threats in real time (Park et al., 2018). This is a growing accomplishment because monitoring is one of the critical components of a cybersecurity framework (Huang et al., 2019). But it also demonstrates further possibilities of improvement,

ISSN: 2716-3865 (Print), 2721-1290 (Online)

especially in the aspect of adopting enhanced monitoring instruments that would enable discovering more detailed information about threats (Luo et al., 2016). In the latest research, it has been highlighted in the use of AI and ML technologies in the monitoring systems to enhance the threat detection mechanisms and to minimize the response time for the same (Shen et al., 2020). The future of banking in cyberspace could look into these technologies, and this is where PT Bank Victoria could stand to improve, especially with the changing threat scenario in Figures 5 and 6 delineated above (Yao et al., 2019). This shows that in the course of February, the number of traffic threats reduced from what was observed between January and February, the application threats as well as spam emails also saw an increase in number, proving that monitoring involves constant changes since the threats are ever-evolving (Li & Paxson, 2019).

Conclusion

Based on research conducted at PT Bank Victoria related to the cyber security system, the conclusions resulting from the analysis of the cyber security system using the ISO 27001:2022 framework are as follows: Related to preventing data leaks at PT Bank Victoria Based on research results related to compliance guidelines in ISO 27001:2022 Appendix A 8:12 at PT Bank Victoria, there are still procedural inconsistencies where the implementation of preventing data leaks at PT Bank Victoria is still not in accordance with the ISO 27001:2022 Compliance Guide Appendix A 8:12. PT Bank Victoria still has not implemented special devices/software/utilities to prevent data leaks or DLP related to securing sensitive data. PT Bank Victoria is currently preventing data leaks by restricting folder sharing, installing antivirus on every computer device and security from the network side related to firewalls.

References

Acquisti, A. (2010). The economics of personal data and the economics of privacy. *Economics*, *11*, 24.

Aginsa, A., Edward, I. Y. M., & Shalannanda, W. (2016, August). Enhanced information security management system framework design using ISO 27001 and zachman framework-A study case of XYZ company. In *2016 2nd International Conference on Wireless and Telematics (ICWT)* (pp. 62-66). IEEE.

Ahmad, A., Maynard, S. B., & Park, S. (2020). Information security strategies to manage cybersecurity threats in financial institutions. *Computers & Security, 92*, 102232. https://doi.org/10.1016/j.cose.2020.102232

Ahmed, S. R. (2020). Identity Crime Framework and Model: Five Components of Identity Crime and the Different Illegal Methods of Acquiring and Using Identity Information and Documents. In *Preventing Identity Crime: Identity Theft and Identity Fraud* (pp. 46-186). Brill Nijhoff.

Aksenta, A., Irmawati, I., Ridwan, A., Hayati, N., Sepriano, S., Herlinah, H., ... & Ginting, T. W. (2023). *Literasi Digital: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0*. PT. Sonpedia Publishing Indonesia.

Alcaraz, C., & Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *Computers & Security, 31*(4), 221-233. https://doi.org/10.1016/j.cose.2013.05.003

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *Computers & Security, 49*, 39-58. https://doi.org/10.1016/j.cose.2014.11.006

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Alharbi, F. S. (2020). Dealing with Data Breaches Amidst Changes In Technology. *International Journal of Computer Science and Security (IJCSS)*, *14*(3), 108-115.

Ali, S., Anwar, Z., & He, X. (2019). Comparative analysis of IT governance frameworks for banking institutions. *Procedia Computer Science*, *154*, 162-167. https://doi.org/10.1016/j.procs.2019.01.162

Aprilia, S. (2021). *Permasalahan Financial Technology Ilegal Di Indonesia* (Bachelor's thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta).

Barona, R., & Anita, E. M. (2017, April). A survey on data breach challenges in cloud computing security: Issues and threats. In *2017 International conference on circuit, power and computing technologies (ICCPCT)* (pp. 1-8). IEEE.

Bosch, J., Faber, R., & Broy, M. (2017). From software product lines to data product lines. *Applied Computing and Informatics*, *13(3)*, 169-179. https://doi.org/10.1016/j.aci.2017.07.003

Brotby, W. K., & Hildebrandt, R. (2021). Information security management principles. *Computers & Security*, *104*, 102295. https://doi.org/10.1016/j.cose.2021.102295

Brotby, W., Endicott-Popovsky, B., & Zafar, H. (2020). Cybersecurity management: A comprehensive approach. *Computers & Security*, *98*, 102081. https://doi.org/10.1016/j.cose.2020.102081

Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance & security. *Computers & Security*, *38*, 18-28. https://doi.org/10.1016/j.cose.2013.04.004

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Computers & Security*, *28(6)*, 370-374. https://doi.org/10.1016/j.cose.2008.10.009

Dharani, L. I. C., Idayanti, S., & Rahayu, K. (2024). *Perlindungan Hukum terhadap Tindakan Phishing di Media Sosial*. Penerbit NEM.

Fernández-Medina, E., Villalba, L. J. G., & Alcaraz, C. (2017). Cost-benefit analysis of information security management systems. *Computers & Security*, *70*, 25-37. https://doi.org/10.1016/j.cose.2017.08.002

Huang, R., & Pearlson, K. E. (2019). Managing the information security function in financial institutions. *Journal of Business Research*, *95*, 280-292. https://doi.org/10.1016/j.jbusres.2018.10.055

Huang, X., Xie, M., Li, G., & Liu, C. (2019). A survey of efficient and effective secure data-sharing schemes in cloud computing. *Computers & Security*, *91*, 1-18. https://doi.org/10.1016/j.cose.2019.04.011

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Computers & Security*, *27(5-6)*, 342-352. https://doi.org/10.1016/j.cose.2008.03.002

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Hwang, W., Lee, J., & Kang, C. (2021). Designing a security strategy for financial information systems. *Applied Computing and Informatics, 17(2)*, 156-170. https://doi.org/10.1016/j.aci.2020.100092

Li, J., & Paxson, V. (2019). A large-scale empirical study of security patches. *Future Generation Computer Systems, 96*, 142-155. https://doi.org/10.1016/j.future.2019.05.030

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2016). Social engineering: The neglected human factor for information security management. *Computers & Security, 56*, 57-70. https://doi.org/10.1016/j.cose.2016.02.008

Mace, R., Stevens, R., & Drew, M. (2022). Evaluating the effectiveness of ISO 27001 in the banking sector. *Computers & Security, 109*, 102221. https://doi.org/10.1016/j.cose.2021.102221

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of marketing*, *81*(1), 36-58. https://doi.org/10.1509/jm.15.0497

Mazzone, M., Figus, A., Celentano, M. G., Foggia, P., Vento, M., & Sansone, C. (2022). Explainable AI meets complex human machine collaboration: A perspective. *Computers in Human Behavior, 130*, 107321. https://doi.org/10.1016/j.chb.2022.107321

Mellado, D., Fernández-Medina, E., & Piattini, M. (2014). A comparison of the security requirements of ISO/IEC 27001 and ISO/IEC 27002. *Computers & Security, 36*, 40-47. https://doi.org/10.1016/j.cose.2014.09.007

Mohamed, M., & Weber, S. (2020). Adaptive cybersecurity: Strategies and policies. *Array, 6*, 100063. https://doi.org/10.1016/j.aci.2020.100063

Müller, R., & Berg, P. (2019). IT governance and the role of business. *Journal of Cleaner Production, 230*, 59-69. https://doi.org/10.1016/j.jclepro.2019.03.120

Park, S. H., Lee, H. S., & Kim, J. (2018). Real-time threat detection in banking: Policy and practice. *Computers & Security, 76*, 22-34. https://doi.org/10.1016/j.cose.2018.02.013

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. *Syngress*. https://doi.org/10.1016/B978-0-12-802044-8.00001-5

Pereira, A. C., & Romero, F. (2017). A review of the meanings and the implications of the Industry 4.0 concept. *Procedia Manufacturing, 13*, 1206-1214. https://doi.org/10.1016/j.promfg.2017.09.139

Rahmatullah, A. (2024). Perlindungan Hukum Bagi Nasabah Pada Pinjaman Online Menurut Hukum Ekonomi Syariah. *Al-Mudharabah: Jurnal Ekonomi dan Keuangan Syariah*, *5*(1), 1-20. https://doi.org/10.22373/al-mudharabah.v5i1.4529

Ramachandran, G., Han, S., & Krishnan, M. (2017). Cybersecurity for industrial control systems: SCADA systems. *Journal of Information Security and Applications, 35*, 100-116. https://doi.org/10.1016/j.jisa.2016.06.003

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Ravindran, A., & Sinha, P. (2022). The evolving role of cybersecurity in financial institutions. *Computers & Security, 112*, 102302. https://doi.org/10.1016/j.cose.2021.102302

Rehman, M. H. U., Ashraf, I., & Gohar, A. (2020). Enhancing cybersecurity through effective IT governance in financial institutions. *Computers & Security, 92*, 101762. https://doi.org/10.1016/j.cose.2019.101762

Saulina, A. R., & Syah, T. Y. R. (2018). How service quality influence of satisfaction and trust towards consumer loyalty in Starbucks coffee Indonesia. *International Advanced Research Journal in Science, Engineering and Technology*, *5*(10), 11-19.

Seddigh, N., Gil, T., & Berg, M. (2017). Information systems security and their applications: A review. *Computers & Security, 67*, 120-132. https://doi.org/10.1016/j.cose.2016.08.006

Setiyawan, W. B. M., Zakariya, H., & Wahtikasari, D. (2020). Perlindungan Data Konsumen Transaksi Online Melalui Penerapan Advance Data Protection System. *Wajah Hukum*, *4*(1), 1-7. http://dx.doi.org/10.33087/wjh.v4i1.179

Setyawan, F. R., Fajrin, Y. A., Prasetyo, S. N., Nuryasinta, R. K., Alam, S., Kurniawan, K. D., & Kurniawan, W. (2024). Preventive Legal Protection Against Leaks Consumer Data by Company Negligence Financial Technology. *KnE Social Sciences*, 374-383. https://doi.org/10.18502/kss.v8i21.14745

Shaikh, M., Cornelissen, J. P., & Dutton, J. E. (2019). Balancing creativity and efficiency in organizations. *Journal of Cleaner Production, 214*, 725-738. https://doi.org/10.1016/j.jclepro.2019.01.059

Shen, C., Wang, J., Yan, J., Han, J., & Zheng, Z. (2020). Secure and efficient privacy-preserving online machine learning based on secret sharing and distributed data. *Computers & Security, 95*, 101789. https://doi.org/10.1016/j.cose.2020.101789

Sims, J. (2022). The changing face of information security: Trends and challenges. *Computers & Security, 108*, 102671. https://doi.org/10.1016/j.cose.2022.102671

Sitorus, T., & Yustisia, M. (2018). The influence of service quality and customer trust toward customer loyalty: the role of customer satisfaction. *International Journal for Quality Research*, *12*(3), 639.

Soemitra, A. (2022). Perlindungan konsumen terhadap kebocoran data pada jasa keuangan di Indonesia. *Juripol (Jurnal Institusi Politeknik Ganesha Medan)*, *5*(1), 288-303.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *Computers & Security, 56*, 70-81. https://doi.org/10.1016/j.cose.2016.09.001

Sun, X., Wang, Y., & Zhang, J. (2019). Information security in the networked era. *Computer Networks, 162*, 106866. https://doi.org/10.1016/j.comnet.2019.04.009

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *Journal of King Saud University-Computer and Information Sciences, 23*(3), 201-207. https://doi.org/10.1016/j.jksuci.2011.09.007

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Tounsi, W., & Rais, H. (2018). A survey on cyber threat intelligence. *Future Generation Computer Systems, 92*, 86-106. https://doi.org/10.1016/j.future.2017.11.029

Tundis, A., Criscuolo, P., & Zennaro, F. (2019). Advancements in information security: Technological evolutions. *Computers & Security, 81*, 100-109. https://doi.org/10.1016/j.cose.2018.09.015

Watson, R. T. (2020). Information systems security: Past, present, and future. *Computers & Security, 89*, 101876. https://doi.org/10.1016/j.cose.2020.101876

Widyastuti, E., & Sugianto, A. (2020). Perlindungan Hukum Terhadap Data Debitur Dalam Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Sultra Research Of Law*, *2*(1), 28-41. https://doi.org/10.54297/surel.v2i1.20

Yao, X., Chen, S., & Zhao, Y. (2019). Blockchain technology for the Internet of Things: Recent advances and future prospects. *Future Generation Computer Systems, 92*, 617-629. https://doi.org/10.1016/j.future.2019.06.004

Zhang, Q., & Huang, Y. (2017). The effects of cybersecurity on system performance. *Computers & Security, 65*, 140-150. https://doi.org/10.1016/j.cose.2017.03.009

ISSN: 2716-3865 (Print), 2721-1290 (Online)