International Journal of Advances in Data and Information Systems
Vol. 5, No. 1, April 2024, pp. 85~100
ISSN: 2721-3056, DOI: 10.59395/ijadis.v5i1.1315

Managing Inherent IT Business Risk against Cyber Threats: a Decision Analysis Case Study of an Oil and Gas Company

I Wayan Novit Marhaendra Putra[1], Meditya Wasesa[1]
[1]School of Business and Management, Institut Teknologi Bandung, Indonesia

Article Info

Article history:

Received Jan 31, 2024
Revised Apr 19, 2024
Accepted Apr 26, 2024

Keywords:

Cyber Resilience
Data Security
Information Security Management System
Information Security Control
IT Business Risk
IT Management

ABSTRACT

XYZ, an anonymized oil and gas company, aims to enhance cyber resilience by strategically managing inherent risk profiles in cybersecurity, aligned with business needs and stakeholder expectations. This research addresses challenges including Information Security Control determination, proficiency improvement in risk management, and ISMS preparedness. Additionally, it tackles procurement strategy for Security Operations Control across XYZ Group, operating under PSC Gross Split, Cost Recovery, and Non-PSC statuses. Utilizing diverse frameworks such as problem tree analysis, stakeholders' power-interest matrix, MITRE ATT&CK, NIST 800-53, COBIT 2019, ISO 27005:2022, KAMI 5.0, and SMART, data analysis includes risk documents, interviews, and cyber-attack data. The research establishes effective IS Control for risk mitigation, readiness for Information Security Management System ISMS implementation, strategic programs enhancing risk management capability, and refined Security Operations Control procurement. These outcomes, incorporated into a collaborative contract structure, significantly mitigate cyber threats and potential impacts, such as disruptions to operations, revenue reduction, increased costs, data theft, and non-compliance.

Corresponding Author:

I Wayan Novit Marhaendra Putra
School of Business and Management, Institut Teknologi Bandung, Indonesia
Email: i_putra@sbm-itb.ac.id

1. INTRODUCTION

XYZ, an anonymized oil and gas company, underwent significant organizational changes in 2021, resulting in the establishment of multiple subsidiaries within the same sector. This restructuring involved workforce transfers and organizational realignment, dividing the company into six major areas. XYZ Company holds majority shares in these six entities, focusing on upstream oil and gas and associated ventures. As a key player in oil and gas production operations, XYZ pursues comprehensive digital transformations aligned with the unique business processes of each subsidiary. Despite these advancements, the rapid evolution and widespread adoption of digital technologies expose XYZ Group and its subsidiaries to potential cyber threats and attacks[1]. Such incidents have the capacity to disrupt or halt company operations, leading to increased production costs or diminished revenue[2]. Consequently, there is an urgent need to enhance the management of inherent risk profiles to achieve cyber resilience[3], with the goal of safeguarding business and upstream data [4].

To assess and address these risks, XYZ Group utilizes the assessment tools provided by the Federal Financial Institutions Examination Council (FFIEC)[5]. These tools evaluate various domains influencing the Inherent Risk Profile (IRP), including technology, cyber threat trends, product-activities, distribution channels, and organizational character. The research, informed by brainstorming sessions, observations, and discussions with relevant stakeholders, identifies critical

considerations. For the technology and cyber threat domains, a thorough analysis of Information Security (IS) controls is essential. This involves examining cyber-attack trends within XYZ Group and the global oil and gas industry to identify appropriate IS controls for mitigation.

In the realms of product-activities and distribution channels, the focus shifts to managing IT Business Risk and IS Risk. These risks serve as reference points for researchers conducting assessments. To bolster information security management, XYZ Group opts for an integrated Security Operation Center (SOC). However, procurement challenges arise due to the company's varied statuses (PSC Gross Split, PSC Cost Recovery, and Non-PSC) resulting from its contractual agreements with the government [6], [7].

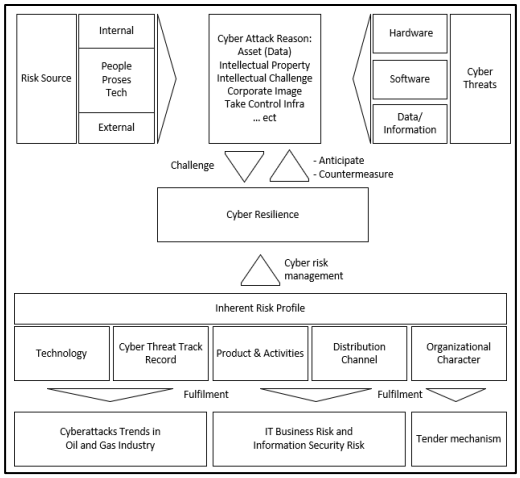


Figure 1. Inherent Risk Profile

Figure 1 depicts the Inherent Risk Profile illustration. Several strategies emerge from this analysis, highlighting deficiencies gaps in the company's extant condition namely.

(1) Inadequate analysis of IS Control in Cyber Threat Trend/ Record
(2) Existing policies for developing IT management capabilities lack comprehensive implementation, with ISMS not yet extended to subsidiaries. A readiness assessment for cyber and business risk management is imperative, and
(3) The SOC procurement strategy is not fully integrated across the company and its subsidiaries.

Within the organizational character domain, the research aims to identify optimal procurement strategies considering the diverse aspects associated with different company statuses. To address the aforementioned gaps and formulate effective IRP management, this research poses the following key research questions:

a. What Information Systems Control required to mitigate cyber risks from both internal and external sources within XYZ Group and the global oil and gas industry?
b. What measures need to be implemented to enhance capability levels in managing IT Business Risk and ensure compliance with IS Risk management?
c. What is the optimal procurement strategy for implementing an integrated Security Operations Control within XYZ Group?

2. RELATED LITERATURE

This research endeavors to synthesize a range of frameworks, tools, and standards essential for navigating the intricate landscape of inherent risk profiles within data security, ultimately fostering cyber resilience in upstream oil and gas enterprises. It emphasizes the crucial customization of these strategies to align with the unique business requirements and stakeholder expectations. This research seeks to integrate business needs by considering the expectations of all stakeholders on

various influential factors (5 domains in inherent risk profile [8]). Where in fulfilling stakeholder expectations, it produces various needs in improving the management of the right inherent risk profile according to the results of the assessment of the conditions of several companies in the oil and gas industry. The results of the inherent risk profile management considerations include determining Information Security Control (appropriate risk mitigation techniques from various cyber attacks), ISMS implementation readiness, internal policy assessment, capability level assessment, IT business risk management, and analysis to find the right procurement method for Integrated SOC services from 7 companies with different legal entity status[9]. In general, research related to risk in cyber security is technical, awareness raising and revolves around a framework, and does not take into account the entire inherent risk profile domain.The research endeavors to enrich existing methodologies by facilitating their seamless incorporation and integration into assessments, thereby refining the analysis process and enhancing the efficacy of risk profiling across diverse domains[10]. Table 1, positioned below, illustrates the distinctive contribution of this research within the context of existing research endeavors.

Table 1. This research's positioning.

No	Author	Year	Method(s)	Objective(s)	Inherent Risk Profile					Location
					Tech	Trend Cyber Threat	Product & Activities	Distribution Channel	Organization Character	
1	Thomas Richard McEvoy and Stewart James Kowalski	2019	Literature Review	Original contribution to the practice of risk analysis and management and provides practitioners.			√		√	Norway
2	George Stergiopoulos, Dimitris A. Gritzalis, And Evangelos Limnaios	2020	Systematic Review, MITRE ATT&CK	To assess documented attacks using standardized impact assessment techniques	√	√				Athens, Greece
3	Roger Kwon, Travis Ashley, Jerry Castleberry, Penny Mckenzie and Sri Nikhil Gupta Gourisetti	2020	Cyber Threat Dictionary Development Process	To present a tool called the "Cyber Threat Dictionary" to solve the problem.	√	√				Washington, USA
4	Georgios Kavallieratos and Sokratis Katsikas	2020	ISO 31000, STRIDE and DREAD	To assess the cyber risk of Cyber Physical Systems qualitatively and quantitatively on board digitalized contemporary and future ships.			√	√		Norway
5	Sara Ricci, Vladimir Janout, Simon Parker, Jan Jerabek, Jan Hajny, Argyro Chatzopoulou, and Remi Badonnel	2021	PESTEL	To present the results of PESTLE analysis for cybersecurity education.			√		√	Czech Republic
6	Iosif Progoulakis, Nikitas Nikitakos, Paul Rohmeyer, Barry Bunin, Dimitrios Dalaklis and Stavros Karamperidis	2021	Survey	An overview of available literature in the field of cyber security for offshore (upstream) oil and gas assets.	√				√	Basel, Switzerland
7	Yuchong Li and Qinghui Liu	2021	Literature Review	To survey and comprehensively review the standard advances presented in the field of cyber security			√		√	Henan, China

8	Mariana G. Cains, Liberty Flora, Danica Taber, Zoe King, and Diane S. Henshel	2022	Expert Elicitation, Data-driven thematic analysis.	Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context			√			Indiana, US
9	Melissa Indah Fianty and Maximillian Brian	2023	COBIT-2019 framework, Gap Analysis	Mapping of IT Governance in companies, aligned with IT-related goals derived from stakeholder interviews			√			Indonesia, Jakarta
10	This Research	2024	PESTEL, SMART, Problem Tree, Power-Interest Map, Gap Analysis	Assist management to improve cyber risk management, find the right data/information security controls, tender mechanism for integrated SOC XYZ Company Group	√	√	√	√	√	Indonesia Compan, Jakarta

3. RESEARCH METHOD

Figure 2 portrays the research framework of this research, delineating its key phases. Each stage is meticulously crafted to contribute to the overarching objective of enhancing information security risk management by tackling challenges within the inherent risk profile. The framework encompasses several distinct phases:

a. Business Issue Exploration: Employing divergent thinking, researchers utilized Political, Economic, Social, Technological, Legal, dan Environment (PESTLE) [11] analysis to delve into external factors. During problem formulation, causes, root problems, and effects were discerned using Problem Tree Analysis [12].

b. Stakeholder Analysis: During the divergent thinking phase, researchers identified stakeholders for analysis. The results were then aligned with the imperative to enhance the Inherent Risk Profile in managing information security risks.

c. Convergent Thinking Phase: Researchers conducted various analyses, including Stakeholder analysis with the Power-Interest Grid Matrix grouping, identification of the right IS Control using MITRE ATT&CK [13], mapping results correlated with Control and NIST 800-53 [14], IS Risk Policy gap analysis at XYZ utilizing Clauses in ISO 27005:2022 [15], analysis of ISMS implementation readiness using KAMI 5.0 [16] at XYZ, and evaluation of Capability Level gaps in managing IS Business Risk at XYZ utilizing APO 12 in COBIT 2019 [17]. Additionally, the procurement strategy was analyzed based on specific aspects using the Simple Multi Attribute Rating Technique (SMART) method [18].

d. Business Solution for Information Security: This section involves summarizing the results of the analyses and brainstorming the needs of stakeholders.

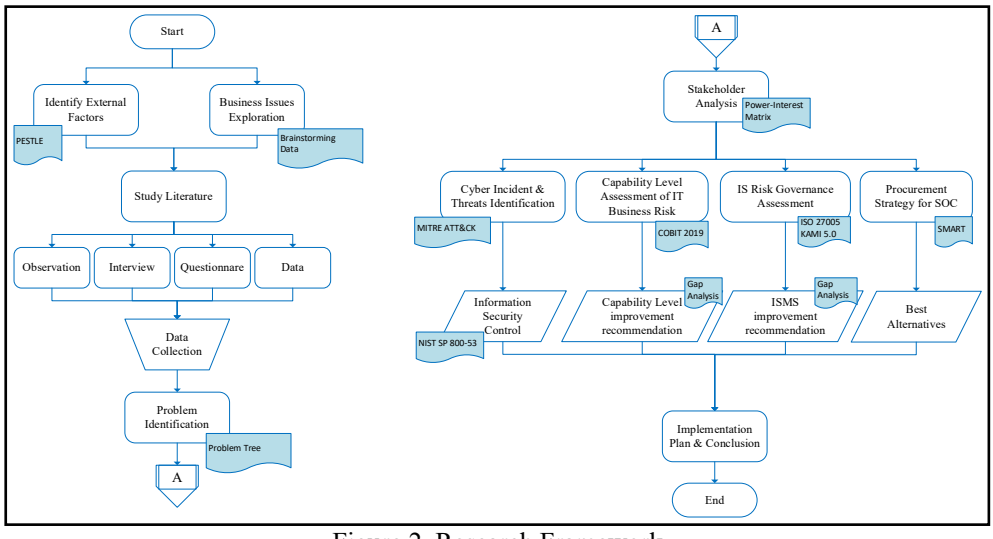


Figure 2. Research Framework

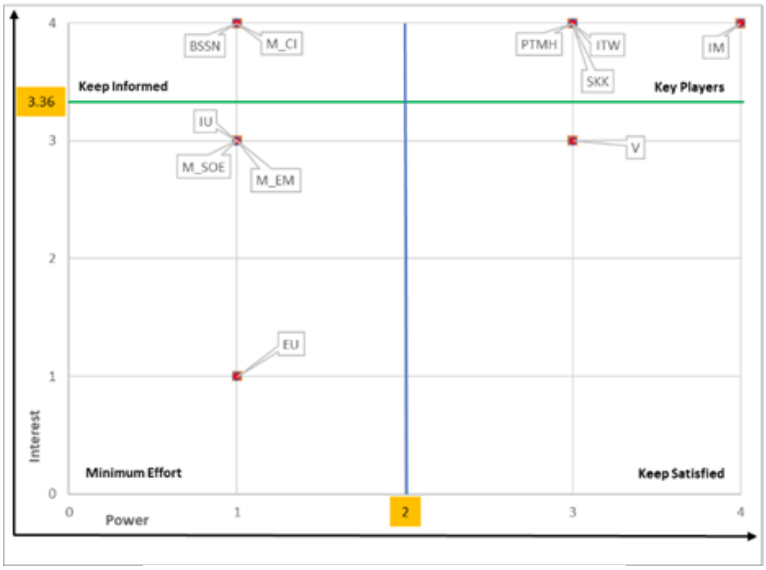
In this mixed-method approach, researchers conducted interviews with the PIC of risk management from each subsidiary entity, totaling 13 personnel. Internal XYZ interviews involved risk management PICs, management personnel, and procurement personnel, totaling 9 personnel—all working in the IT Department of each company entity. In the questionnaire method, 117 respondents from the internal IT department of XYZ participated. Furthermore, 60 cyber-attack/threat events within the company and the oil and gas industry were analyzed using specific methods to determine the right IS Control.

The instruments in this research include company policy documents related to information security, IS risk registers, IT Business Risk Registers, SOC implementation plans, and procurement guidelines for Non-PSC, PSC Gross Split, and PSC Cost Recovery. Interviews and observations were conducted using Clauses in ISO 27005:2022, KAMI 5.0, APO 12 in COBIT 2019, MITRE ATT&CK cyber-attack tactics and techniques database (ICS and Enterprise), and NIST SP 800-53 revision 5. Qualitative data collection was carried out through interviews.

4. RESULTS AND DISCUSSION

4.1. Problem and Stakeholder Analyst

Through interviews conducted with IT Management and relevant stakeholders at XYZ, the research obtained results of problem analysis using Problem Tree Analysis, encompassing Causes, Effects, and Core Problems. The analysis indicates that the primary cause of various potential issues in risk management, spanning political, legal, social, technological, environmental, organizational, and economic aspects, is the lack of enhancement in managing inherent risk profiles. To commence the research, stakeholders were identified and categorized within a power-interest matrix chart. Figure 3 presents the internal and external stakeholders mapping, each characterized by their respective power and interests. These insights were derived from the interview process involving relevant parties.



Code	Description
IM	Internal - Management
IU	Internal – Customer/User
ITW	Internal – IT Workers/Teams
BSSN	External – National Cyber and Crypto Agency
M_SOE	External - Ministry of State Own Enterprise
M_EM	External - Ministry of Energy and Mineral Resources
M_CI	External - Minister of Communication and Informatics
SKK	External - Regulator
PTMH	External – Holding Company
EU	External – Customer/User
V	External – Partner/Third Party

Figure 3. Stakeholders Map

Figure 4 illustrates the problem tree analysis, indicating that the primary cause of potential risk management issues lies in the failure to enhance capabilities for managing inherent risk profiles

across various domains. Using this analysis, researchers aim to prioritize factors within the inherent risk profile through weighting.

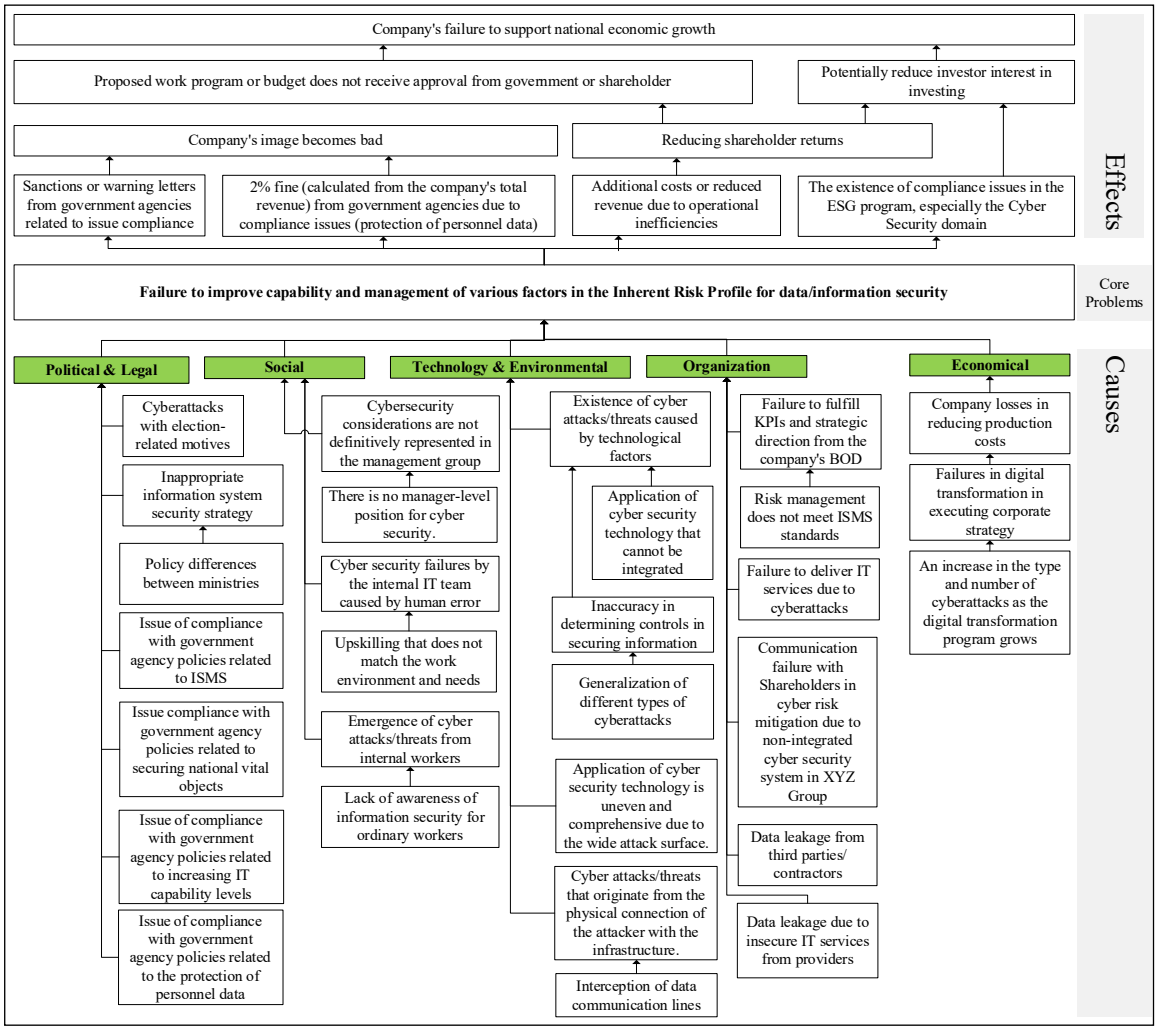


Figure 4. Problem Tree Analysis

Subsequently, they determine the priority of increasing the inherent risk profile according to stakeholder expectations, utilizing the power-interest matrix through internal company interviews. This research employs a weighting method based on stakeholder expectations and power-interest dynamics, with Table 2 presenting the priority list.

Table 2. Risk profile prioritization

No	Prioritization	Inherent Risk Profile
1	Information Technology (IT) Business Risk	Product, Activities and Distribution Channel Domain
2	Information Security Management System (ISMS) & Information Security (IS) Risk	Product, Activities and Distribution Channel Domain
3	Security Operation Center (SOC) Implementation	Organizational Character Domain
4	Information Security (IS) Control	Technology and Cyber Threat Record Domain

4.2. Cyber Threat Trend

Figure 5 displays data sources utilized related to the quantity of cyber attacks. The term "control" refers to the pattern of cyber attacks and threats observed both within XYZ and across the oil and gas industry. This analysis serves as a basis for recommending risk mitigation strategies, ensuring the implementation of appropriate information security controls to prevent cyber incidents.

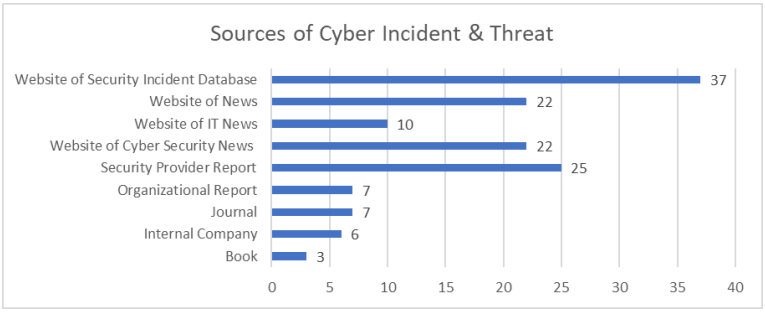


Figure 5. Cyber-attacks statistics

Researchers gathered data on 6 cyber threats within the XYZ group and 54 incidents within the oil and gas industry. Employing a scientific approach and leveraging the MITRE ATT&CK (Enterprise & ICS) framework [19], researchers identified various tactics and techniques as follows:

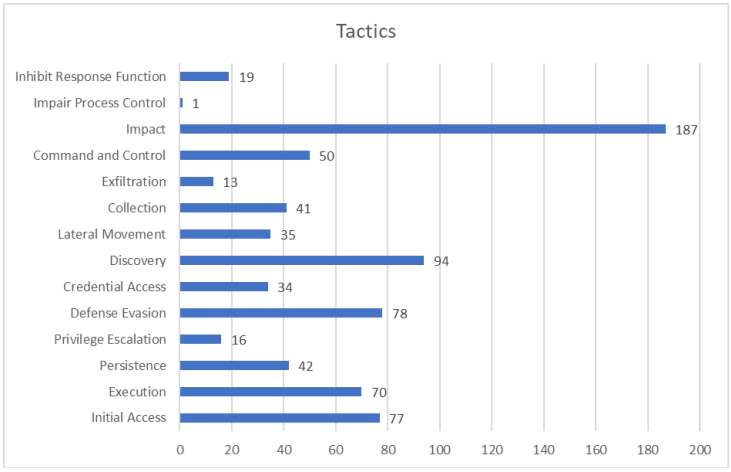


Figure 6. Tactics of Cyber Incident & Threat

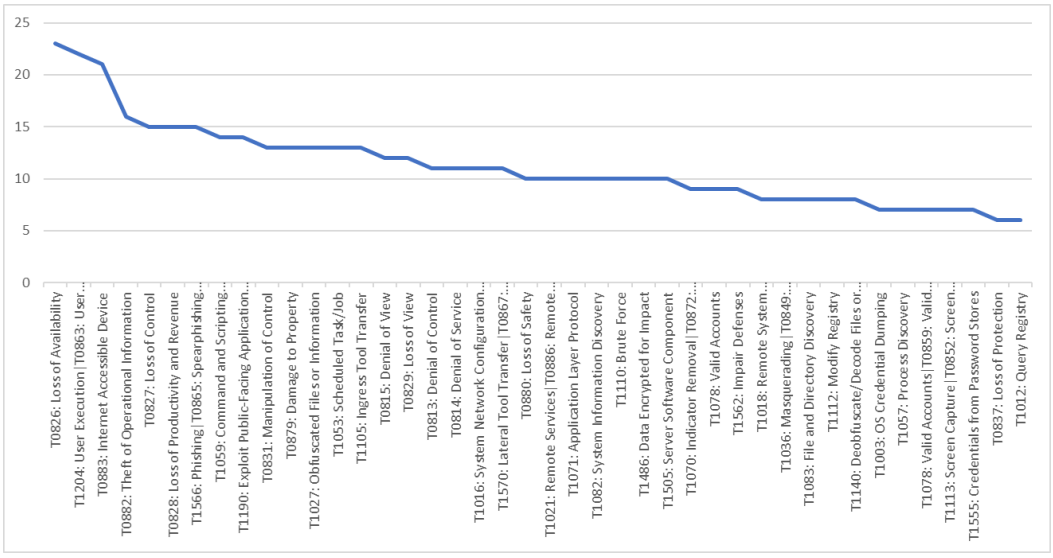


Figure 7. Use of Cyber Attack Techniques in the Oil and Gas Upstream Industry

This research outlines the tactics and techniques utilized in cyber attacks, as depicted in Figures 6 and 7. These charts quantify the dominant tactics and techniques observed. Subsequently, researchers mapped these techniques with the appropriate Information Security (IS) Controls outlined in NIST SP 800-53, utilizing the mechanism detailed in Figure 8.

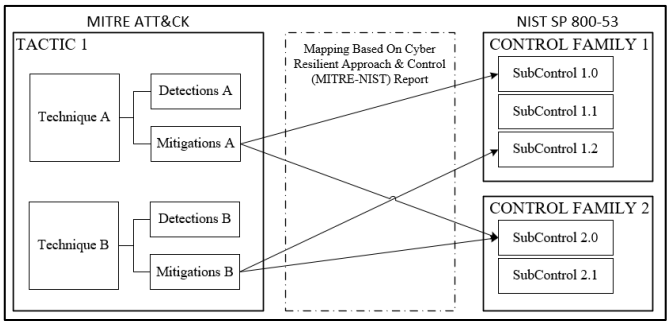


Figure 8. Mapping MITRE ATT&CK to Controls NIST SP 800-53

During this mapping process, researchers referred to the 2021 MITRE Technical Report titled "Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs)[20]." They categorized the recommended IS Controls, distinguishing between those applicable to cyber attacks and threats originating from internal XYZ Group Companies and those related to incidents in the oil and gas industry. Based on the mapping results, the predominant application of IS Controls is outlined as follows. Figures 9 and 10 illustrate the Information Security Controls necessary for mitigating the causes of cyber threats.

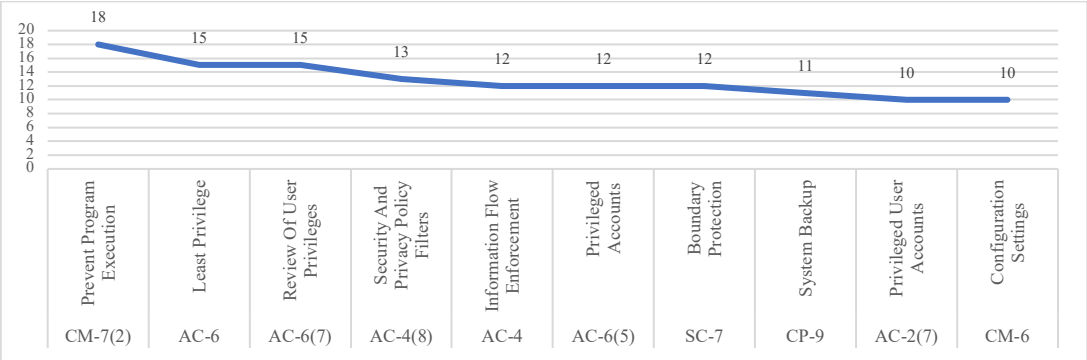


Figure 9. Top 10 NIST SP 800-53 controls that need to be implemented (partial)

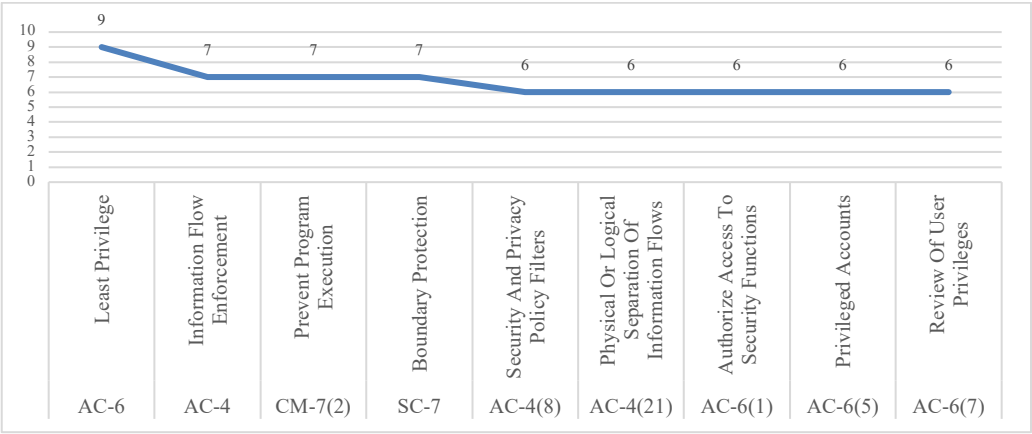


Figure 3. Techniques used by cyber attackers in cyber-attacks

4.3. IT Business Risk

In compliance with ministerial regulations, risk management mandates accelerating to capability level 3 in COBIT 2019. Analyzing the proficiency of IT business risk management aims to identify gaps between existing risk management practices and the targeted capability level. Researchers conducted assessments, comprising brainstorming sessions, document reviews, and interviews across 7 corporate entities within the XYZ Group. APO 12 in COBIT 2019 served as the reference framework, employing the scaling ranges of None, Partially, Largely, and Fully

Implemented, as outlined in COBIT 2019. Table 3 displays the results of the capability level assessment for each entity in this research.

Table 3. IT Business Risk Management Capability Level Assessment Results

Entity	Level 1	Level 2	Level 3	Level 4	Level 5	Result
Area A	100%	69,17%				Level 1
Area B	100%	95,00%	85,56%	68,50%		Level 3
Area C	100%	86,67%	85,56%	75,50%		Level 3
Area D	100%	75,00%				Level 1
Area E	100%	75,00%				Level 1
Area R	100%	69,17%				Level 1
XYZ	100%	92,50%	86,67%	77,00%		Level 3

Area B, Area C, and XYZ entities have achieved Capability Level 3 and are advised to sustain and enhance these capabilities. For corporate entities that have not attained Capability Level 3, the assessment yielded recommendations for APO 12 COBIT 2019 activities through gap analysis. Table 4 illustrates the identified gaps that require improvement to reach Capability Level 3.

Table 4. Activity Number in APO 12 COBIT 2019 (Gap Analysis for Area A, D, E, R)

Target Cap. Level	Area A	Area D	Area E	Area R
2	Non-Conformity:	Non-Conformity:	Non-Conformity:	Non-Conformity:
	APO12.03.01	APO12.03.01	APO12.03.01	APO12.03.01
	APO12.03.03	APO12.03.03	APO12.03.03	APO12.03.03
	OFI:	OFI:	OFI:	OFI:
	APO12.03.02	APO12.03.02	APO12.01.03	APO12.03.02
3	Non-Conformity:	Non-Conformity:	Non-Conformity:	Non-Conformity:
	APO12.04.03	APO12.04.03	APO12.04.03	APO12.04.03
	APO12.06.01	OFI:	OFI:	OFI:
	OFI:	APO12.01.03	APO12.01.03	APO12.01.03
	APO12.01.03	APO12.02.01	APO12.02.01	APO12.02.02
	APO12.02.01	APO12.02.03	APO12.02.03	APO12.02.03
	APO12.02.04	APO12.02.04	APO12.02.04	APO12.02.04
	APO12.02.06	APO12.02.05	APO12.02.05	APO12.02.06
	APO12.03.04	APO12.02.06	APO12.02.06	APO12.03.04
	APO12.03.05	APO12.03.04	APO12.03.04	APO12.03.05
	APO12.04.01	APO12.03.05	APO12.03.05	APO12.04.01
	APO12.04.02	APO12.04.01	APO12.04.01	APO12.04.02
	APO12.04.04	APO12.04.02	APO12.04.02	APO12.04.04
	APO12.05.03	APO12.04.04	APO12.04.04	APO12.05.03
	APO12.06.02	APO12.05.03	APO12.05.03	APO12.06.01
		APO12.06.01	APO12.06.01	APO12.06.02
		APO12.06.02	APO12.06.02	

After identifying the gaps, the next step is to establish programs prioritization in corporate entities that have not yet achieved level 3 capability. Based on interviews with relevant stakeholders, seven capability improvement programs have been identified for implementation, each with its full scope and weightings. Researchers utilize Weighted Scoring Prioritization to determine the priority of implementing these programs. Each program focus is assigned a value reflecting its impact on implementing the recommended activities. Table 5 presents the strategic program priorities for addressing the capability level gap analysis. The seven prioritized program focuses outlined above are recommendations that XYZ must implement to attain capability level 3.

Table 5. Program Prioritization

No	Programs	Total	Rank
1	Internal Policy Implementation	400	1
2	Upskilling Workers	215	5
3	Risk Management Process Control	380	3
4	Formation of Taskforce Team	360	4
5	Documented Process	200	6
6	Correspondences Process	150	7
7	Decision Making on Internal Teams	400	2

4.4. Information Security Management System (ISMS) and Information Systems (IS) Risk

In the Product, Activities, and Distribution Channel Domain of the Inherent Risk Profile, ISMS implementation and IS Risk management play crucial roles. At this stage, researchers conducted an ISMS assessment using KAMI 5.0 (Konsultasi dan Assessment Indeks/National Cyber & Crypto Agency) to measure ISMS implementation readiness. Additionally, they reviewed the IS Risk and Risk Treatment Plan implemented at XYZ according to the ISO 27005 version 2022 standard. To measure the readiness of ISMS implementation, researchers assessed various factors, including Electronic System Category, Information Security Governance, Information Security Risk Management, Information Security Framework, Information Asset Management, Technology Management, and Protection of Personal Data. A summary of the results of the ISMS implementation readiness assessment is presented in Table 6.

Table 6. KAMI 5.0. Assessment Results

Security Category	Question & Evaluation Area						Total
	Governance	Risk	Framework	Asset	Technology	PPD	
1	8	10	12	27	14	4	75
2	8	4	11	19	15	12	69
3	6	2	10	7	6	0	31
Max. Score	126	72	192	258	186	84	918
Score	115	59	174	255	170	71	844
Percentage	91,27%	81,94%	90,63%	98,84%	91,40%	84,52%	
Maturity Lvl	3+	3	3+	3	3+	3	

Based on the assessment results, maturity levels 3 and 3+ were achieved, with a total score of 844. The strategic level for the Electronic System Category, scoring 612, falls within the "good enough" range, which spans values from 761 to 864. Consequently, the conclusion drawn is that the level of maturity and completeness in the application of ISO/IEC 27001 warrants both internal and external audits. Gap analysis reveals the percentage obtained in each domain, with the Information Security Risk Management and Protection of Personal Data domains showing the lowest percentages. The gap analysis of the ISMS readiness assessment results is outlined in Table 7.

Table 7. The results of gap analysis of ISMS implementation readiness assessment (using KAMI 5.0)

ISMS Domain (KAMI 5.0)	Gap Analysis
Risk Management	• Documentation related to the identification of ownership, management, and use of data assets. Including the threats and weaknesses. • There are measurements related to the effectiveness of resources, regular monitoring, objective, measurable and consistent evaluation. • There is an accurate and valid risk profile research and an effective risk management.
Protection of Personnel Data	• The existence of internal policies and specialized teams or departments that focus on the implementation of Protection of Personnel Data. • For personnel data owners, there is a policy that describes the approval process, incident reporting, guarantees and ensures the accuracy of personnel data. As well as the process of disclosing personnel data to legal authorities legally.

Furthermore, researchers conducted an assessment of various internal policies concerning Information Security Risk management. In this instance, researchers utilized various clauses listed in ISO 27005:2022. Specifically, Clauses 5 to 10 were employed, totaling 42 points as assessment

criteria in the interview process with relevant parties. Table 8 provides a summary of the results of the internal policy assessment in cyber risk management.

Table 8. Quantity of conformity ISMS risk management guidelines and documents to ISO 27005:2022

Result	Qty (%)	References
Conformity	35 (83,3%)	All Clause 5, all clause 6, all clause 7, 8.1, 8.2, 8.6.1, 8.6.2, 8.6.3, all clause 9, 10.1, 10.2, 10.3, 10.5.1, 10.5.2, 10.6, 10.7.
Need Improve	6 (14,3%)	8.3, 8.4, 8.5, 10.4.1, 10.4.2, 10.4.3
No Conformity	1 (2,4%)	10.8

Based on the assessment results, several implementations and additions are necessary for inclusion in the information security risk management guidelines:

1. Clause 8.3 requires the determination of controls necessary for information security implementation. Additionally, a comparison between the risk treatment plan and the control activities listed in Annex A of ISO/IEC 27001:2022 (Clause 8.4) and Statement of Applicability (Clause 8.5) is essential.
2. Clause 10.4.1 concerning Documented Information - General mandates comprehensive documentation of all activities related to risk assessment, risk treatment plans, and the outcomes of risk management.
3. The entire process of risk assessment activities, encompassing risk identification, analysis, evaluation, and treatment plans, must be meticulously documented (Clause 10.4.2 and 10.4.3).
4. Clause 10.8 addresses Continual Improvement, emphasizing activities aimed at enhancing risk management, such as increasing capability levels, aligning with organizational business objectives, addressing trends in potential vulnerabilities, and re-evaluating risk events/threats for further risk cause determination or treatment plan adjustments.

Furthermore, researchers conducted reviews and interviews related to the risk management process outlined in the Information Security Risk Register and Risk Treatment Plan documents. Specifically, references were made to ISO 27005 version 2022, specifically Clauses 7.2 for Risk Identification, Clauses 7.3 for Risk Analysis, Clauses 7.4 for Risk Evaluation, and Clauses 8 for Risk Treatment Plan. The assessment revealed that XYZ adequately executes the risk assessment process, meeting the requirements outlined in Clauses 7.2, 7.3, 7.4, and 8.

4.4. Strategy Procurement of Security Operations Center (SOC) Services

The aim of this research stage is to identify the optimal procurement strategy for SOC implementation across various corporate entities within the XYZ group, each governed by distinct procurement regulations and system integrity requirements. The researcher employs the Simple Multi Attribute Rating Technique (SMART) method with the following steps:

1. Determine and identify the decision maker: This involves engaging with IT management and the team responsible for the SOC procurement process.
2. Identify Several Alternative Solutions: Through study and interviews with relevant parties, 7 alternative procurement strategies were identified, aligning with procurement guidelines for Gross Split PSC (A7-001) and Cost Recovery PSC (PTK-007). These strategies are detailed in Table 9.

Table 9. Several Alternative for Procurement Strategy

No	Name	Alternatives
1	Alternative 1	All Gross Split PSCs and Cost Recovery PSCs enter joint contracts using PTK 007 across Area's. After going through the Winner Appointment process, XYZ Company conducts procurement with Direct Assignment to the Joint Contract.
2	Alternative 2	Non-PSC and Gross Split PSC entities execute contracts together with A7001. In parallel, Cost Recovery PSCs run joint contracts with PTK 007. Both joint contracts are executed across Area's.
3	Alternative 3	Non-PSC Company Entities and Gross Split PSCs execute joint contracts using A7001 on a cross-area basis. After the joint contract has been awarded and the system to be built has been defined, PSC Cost Recovery will carry out a cross-area joint contract using PTK 007 Procurement Guidelines with the requirement that the system to be built must be integrated with the Non-PSC - PSC Gross Split joint contract.
4	Alternative 4	PSC Cost Recovery entities execute joint contracts across Area using PTK 007 Procurement Guidelines. After the joint contract has gone through the winner appointment process, all Non-PSC and PSC Gross

		Split company entities execute joint contracts using Procurement Guideline A7001, directly appointing the winning vendor on the PSC Cost Recovery joint contract.
5	Alternative 5	PSC Cost Recovery Company entities execute joint contracts across Area using PTK 007 Procurement Guidelines. After the joint contract has gone through the winner appointment process, each Area for the Gross Split PSC company entity executes a joint contract using Procurement Guideline A7001 by directly appointing the winning vendor on the PSC Cost Recovery joint contract. XYZ Company also does the same for contracts that are specific to XYZ only.
6	Alternative 6	XYZ Company implements a special contract for XYZ only, using the A7001 Procurement Guidelines. After the contract at XYZ has gone through the process of appointing the winner and approving the system to be built, the Cost Recovery PSC and Gross Split PSC carry out a joint contract with the condition that the system built must be integrated with the contract at XYZ. In parallel, other Non-PSC Entities also carry out separate contracts with the condition that the system to be built must be integrated with the XYZ contract.
7	Alternative 7	XYZ Company implements a special contract for XYZ only, using Procurement Guidelines A7001. After the contract at XYZ has gone through the process of appointing the winner and approving the system to be built, the Cost Recovery PSC with Gross Split PSC carries out a joint contract in each Area with the condition that the system built must be able to be integrated with the contract at XYZ, using the PTK 007 Procurement Guidelines. For other Non-PSC Entities also carry out separate contracts with the condition that the system to be built must be integrated with the XYZ contract.

3. Identify relevant aspects/attributes for decision-making: Factors affecting the procurement strategy include compliance with procurement guidelines, tender methods (for cost-effectiveness and budget recovery), procurement processing time, competitive vendor landscape, and system integration for operations.
4. Determine the value of each alternative solution/action on each attribute: Table 10 presents the assessment results of each alternative solution derived from discussions and interviews with relevant stakeholders.

Table 10. Scoring Matrix with Attributes and Alternatives

No	Alternatives	Compliance	Tender Method & Recover Budget	Integrated System for Operational	Competitive Business	Time For Procurement
1.	Alternative 1	100,00	73,33	73,33	73,33	53,33
2.	Alternative 2	100,00	100,00	73,33	100,00	70,00
3.	Alternative 3	100,00	100,00	93,33	96,67	53,33
4.	Alternative 4	100,00	46,67	73,33	46,67	36,67
5.	Alternative 5	100,00	46,67	73,33	46,67	50,00
6.	Alternative 6	100,00	100,00	100,00	93,33	46,67
7.	Alternative 7	100,00	100,00	73,33	93,33	60,00

5. Determine the weighting of each aspect/attribute: Table 11 showcases the weighting results of each aspect, obtained through interviews with various relevant parties.

Table 11. Attributes Normalized Weight

No.	Attributes	Raw Weight	Normalized
1	Compliance with procurement guidelines	100	25.00
2	Tender Method (For Reasonable Price) & Recover Budget	70	17.50
3	Procurement processing time	80	20.00
4	Competitive business environment	60	15.00
5	System Integration in Operations	90	22.50
	Total Weight	400	100

6. Calculate the weighted average of the values assigned to each alternative. For each alternative, the weight assigned to each attribute is determined. Researchers sum up the weights of each attribute to obtain the final aggregate score, as presented in Table 12.

Table 12. Score for alternative (%)

No	**Alternatives**	**Compliance with procurement guidelines**	**Tender Method**	**Integrated System for Operational**	**Competitive Business**	**Procurement processing time**	**Total**	**Aggregate Benefit (%)**	**Rank**
1.	Alternative 1	2500,00	1283,33	1650,00	1100,00	1066,67	7600,00	76,00	5
2.	Alternative 2	2500,00	1750,00	1650,00	1500,00	1400,00	8800,00	88,00	3
3.	***Alternative 3***	***2500,00***	***1750,00***	***2100,00***	***1450,00***	***1066,67***	***8866,67***	***88,67***	***1***
4.	Alternative 4	2500,00	816,67	1650,00	700,00	733,33	6400,00	64,00	7

5.	Alternative 5	2500,00	816,67	1650,00	700,00	1000,00	6666,67	66,67	6
6.	Alternative 6	2500,00	1750,00	2250,00	1400,00	933,33	8833,33	88,33	2
7.	Alternative 7	2500,00	1750,00	1650,00	1400,00	1200,00	8500,00	85,00	4

5. CONCLUSION

This research addresses identified gaps and offers recommendations for enhancing the capability and readiness of ISMS implementation within the XYZ Company Group. Adopting a holistic approach to the inherent risk profile, this research emerges as a valuable and sustainable resource for navigating future challenges in cyber risk management. However, the research has certain limitations, such as the exclusion of financial calculations related to cyber issues, information security assurance, and the evolving landscape of cyber-attacks post-AI/ML.

Aligned with the company's business needs and stakeholder expectations, as well as responses to previous cyber-attacks/threats at XYZ Company, this research on improving inherent risk profile management becomes instrumental in maintaining cyber resilience and safeguarding data and information. The research addresses three key questions:

What Information Systems Control required to mitigate cyber risks from both internal and external sources within XYZ Group and the global oil and gas industry? This research underscores the importance of Information Security Control implementation, focusing on Account & Access Management, Security & Segmentation for Physical & Data Flow, Data/Content Filtering, Program Execution Security, Backup System, and Configuration Management. These measures, denoted as AC-6, AC-4, CM-7, SC-7, CP-9, AC-2, and CM-6 in NIST SP 800-53, are continuously monitored, controlled, and integrated through change management mechanisms in cyber risk management.

What measures need to be implemented to enhance capability levels in managing IT Business Risk and ensure compliance with IS Risk management? Strategic programs, prioritized by internal policy implementation, upskilling of workers, risk management process control, task force team formation, documented processes, correspondences process, and internal team decision-making, are recommended. These strategic initiatives are to be implemented by corporate entities in Areas A, D, E, and R, subsidiaries of XYZ Company. Additionally, guidelines for information security risk management within XYZ Company can be updated based on research recommendations, aligning with the ISO 27005 version 2022 standard, particularly focusing on specific clauses.

Research Question 3: What is the optimal procurement strategy for implementing an integrated SOC within XYZ Group, considering the unique characteristics of each entity? Procurement is proposed to occur through a joint contract in two phases, involving the first phase for all Non-PSC and PSC Gross Split entities and the second phase for all PSC Cost Recovery entities. Following the winner appointment process in the first phase, the procurement in the second phase mandates integration of SOC services with those in the first phase, ensuring a comprehensive approach.

REFERENCES

[1] A. J. G. de Azambuja, T. Giese, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Digital Twins in Industry 4.0 – Opportunities and challenges related to Cyber Security," *Procedia CIRP*, vol. 121, pp. 25–30, 2024, doi: https://doi.org/10.1016/j.procir.2023.09.225.

[2] S. Quinn, N. Ivy, M. Barrett, G. Witte, and R. K. Gardner, "Staging cybersecurity risks for enterprise risk management and governance oversight," Feb. 2022. doi: 10.6028/NIST.IR.8286C.

[3] I. Progoulakis, N. Nikitakos, P. Rohmeyer, B. Bunin, D. Dalaklis, and S. Karamperidis, "Perspectives on Cyber Security for Offshore Oil and Gas Assets," *J Mar Sci Eng*, vol. 9, no. 2, 2021, doi: 10.3390/jmse9020112.

[4] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126.

[5] Federal Financial Institutions Examination Council (FFIEC), "FFIEC Cybersecurity Assessment Tool," May 2017. Accessed: Apr. 20, 2024. [Online]. Available: https://www.ffiec.gov/cyberassessmenttool.htm

[6] Satuan Kerja Khusus Pelaksana Kegiatan Usaha Hulu Minyak dan Gas Bumi, *Pedoman Tata Kerja No. PTK-007/SKKIA0000/2023/S9 Revisi 5 Pedoman Pelaksanaan Barang dan Jasa*. Indonesia, 2023.

[7] Pertamina Hulu Energi, *Panduan Pengadaan Barang dan Jasa* . Indonesia, 2021.

[8] O. J. K. Departemen Penelitian dan Pengaturan Perbankan, "Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum," 2021. Accessed: Apr. 20, 2024. [Online]. Available:

https://www.ojk.go.id/id/kanal/perbankan/implementasi-basel/Documents/Pages/Consultative-Papers/Consultative%20Paper%20Manajemen%20Risiko%20Keamanan%20Siber%20Bank%20Umum.pdf
[9] B. Roach and A. Dunstan, "The Indonesian PSC: the end of an era," *The Journal of World Energy Law & Business*, vol. 11, no. 2, pp. 116–135, Apr. 2018, doi: 10.1093/jwelb/jwy001.
[10] Douglas W. Hubbard and Richard Seiersen, *How To Measure Anything In Cybersecurity Risk*. New Jersey: John Wiley & Sons.
[11] S. Ricci *et al.*, "PESTLE Analysis of Cybersecurity Education," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, in ARES '21. New York, NY, USA: Association for Computing Machinery, 2021. doi: 10.1145/3465481.3469184.
[12] W. W. Walubengo, D. N. Kyalo, and A. S. Mulwa, "Analytical Review of Application of Problem Tree Analysis As a Project Design Tool For Enhancing Performance of Community Based in Kenya," *European Journal of Business & Management Research*, vol. 4, Nov. 2019.
[13] G. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, "Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns," *IEEE Access*, vol. 8, pp. 128440–128475, 2020, doi: 10.1109/ACCESS.2020.3007960.
[14] Joint Task Force Transformation Initiative Interagency Working Group, "Security and Privacy Controls for Information Systems and Organization," Gaithersburg, Jul. 2020. Accessed: Apr. 20, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[15] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Comput Sci*, vol. 161, pp. 1206–1215, 2019, doi: https://doi.org/10.1016/j.procs.2019.11.234.
[16] Badan Siber dan Sandi Negara, *Konsultasi dan Assessment Indeks KAMI*. Indonesia, 2023. Accessed: Apr. 20, 2024. [Online]. Available: https://www.bssn.go.id/indeks-kami/
[17] S. A. Wulandari, A. P. Dewi, M. R. Pohan, D. I. Sensuse, M. Mishbah, and Syamsudin, "Risk Assessment and Recommendation Strategy Based on COBIT 5 for Risk: Case Study SIKN JIKN Helpdesk Service," *Procedia Comput Sci*, vol. 161, pp. 168–177, 2019, doi: https://doi.org/10.1016/j.procs.2019.11.112.
[18] F. H. Barron and B. E. Barrett, "The efficacy of SMARTER — Simple Multi-Attribute Rating Technique Extended to Ranking," *Acta Psychol (Amst)*, vol. 93, no. 1, pp. 23–36, 1996, doi: https://doi.org/10.1016/0001-6918(96)00010-8.
[19] Deborah J. Bodeau, Richard D. Graubart, Linda K. Jones, Ellen R. Laderman, and David Black, "Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs)," Dec. 2021. Accessed: Apr. 20, 2024. [Online]. Available: https://www.mitre.org/news-insights/publication/cyber-resiliency-approaches-controls-mitigate-tactics-rev2
[20] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," in *2020 Resilience Week (RWS)*, 2020, pp. 106–112. doi: 10.1109/RWS50334.2020.9241271.

I Wayan Novit Marhaendra Putra received his bachelor's degree in informatics engineering from Universitas Pembangunan Nasional Veteran, Yogyakarta, Indonesia. He is currently attending a postgraduate program at the School of Business Management and Administration (MBA), Institut Teknologi Bandung, Indonesia. Currently, he is working at one of the state-owned enterprises in Indonesia.

Meditya Wasesa is an assistant professor at the School of Business and Management, Institut Teknologi Bandung. He holds a Ph.D. in Management Information Systems from Rotterdam School of Management, Erasmus University, Netherlands, an M.Sc. in Logistics Engineering from Duisburg-Essen University, Germany, and a Bachelor of Mechanical Engineering (S.T.) from Institut Teknologi Bandung. His career spans work with international companies, including General Motors Europe - Germany and Rotterdam School of Management - the Netherlands. In Indonesia, he has served as an executive and consultant for a diverse range of organizations, from private companies and state-owned enterprises (BUMN) to notable start-up unicorns and ministries. His primary research and teaching areas revolve around leveraging advanced information systems to enhance business decisions, with a particular emphasis on business analytics. His work has been featured in

renowned publications like IEEE Access, Journal of Enterprise Information Management, Decision Support Systems, Journal of Cleaner Production, etc.