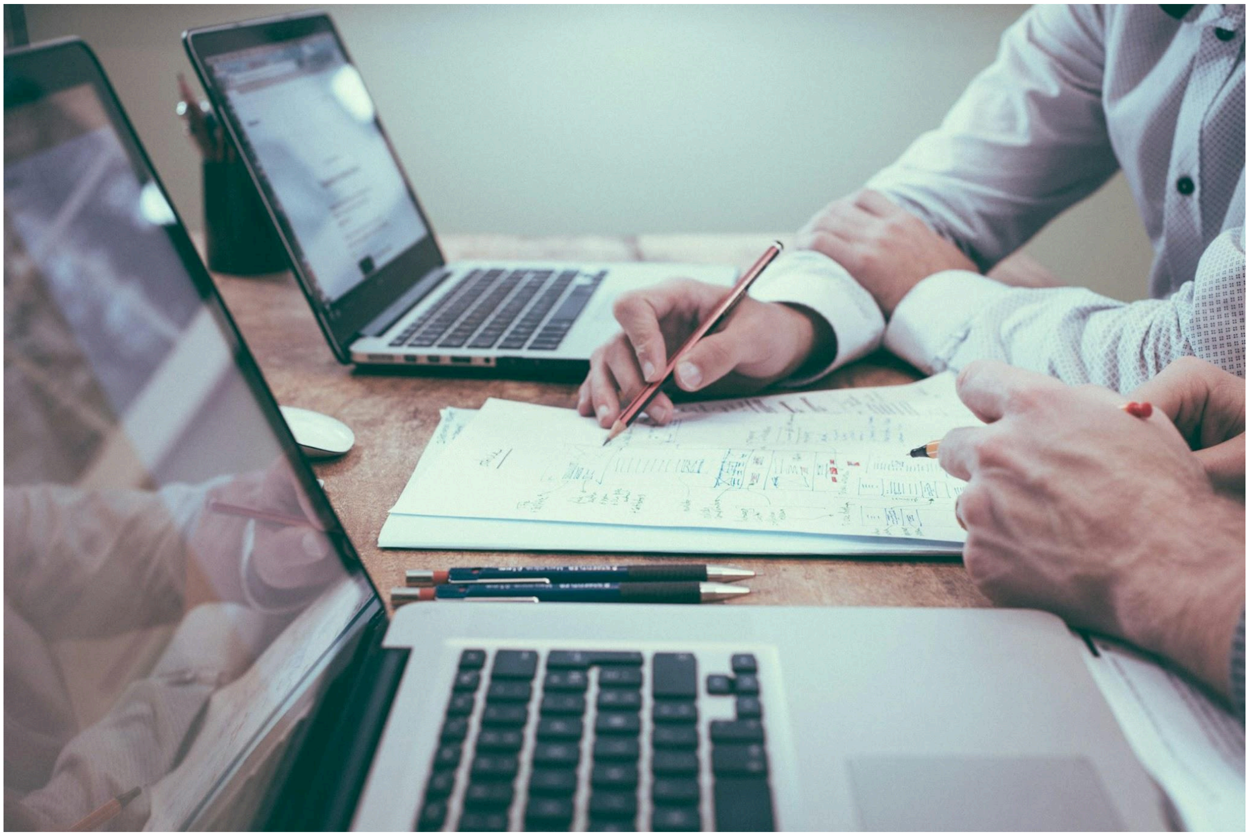


Audit Report

PT. Indo Audit (IndoDit)

04.30.2024

Ryufath Alief Adhyaksa Putera Soepeno (2021400015)

Christopher Gerard Lissants (2021400012)

Allister Totong (2021400008)

Andi Muhammad Imam Akbar (202140001)

Table of Contents

Audit Plan

I. Introduction

As multinational supply chain companies are establishing their ventures in Indonesia, our audit team is committed to conducting an audit to thoroughly provide a structured approach to examining and evaluating the company's IT infrastructure, access controls, and data management processes. PT. IndoDit's audit plan would provide an evaluation of the company's IT infrastructure policies, guidance, and standard operating procedures (SOPs), while also assessing the access privileges granted to different stakeholders such as customers, transportation vendors, suppliers, company employers, and employees, ensuring the security, integrity, and efficiency of the main portal and its associated applications.

II. Objectives

A successful audit is one that identifies potential risks, weaknesses, and inefficiencies in the company's IT infrastructure and data management processes, providing actionable recommendations for improvement. Our team's objectives include:

- Assess the risk management and quality assurance processes across all offices, particularly focusing on the identification and mitigation of supply chain vulnerabilities.
- Review the alignment of IT infrastructure policies and standard operating procedures (SOPs) with global security standards, ensuring consistency and resilience across all regions.
- Confirm the functionality and security of the Global Corporate Website, particularly regarding its integration with CRM, Vendor Management, and Warehouse and Logistic Management Systems for seamless customer transactions and data management.
- Verify the segregation of duties and access controls within the IT systems, ensuring that troubleshooting, upgrades, and patching activities are conducted securely and transparently.
- Evaluate the effectiveness of the ERP systems (HRMS, FAMS, CRM) in integrating global operations while maintaining regional specificity for warehouse and logistic management systems (WLMS).

III. Roles & Responsibilities

Name	Auditor Role	Description	Contact
Ryufath Alief Adhyaksa Putera Soepeno	Head of Audit Team with Risk Management	● Leads audit team with a focus on risk management. ● Oversees the auditing process and reports findings. ● Collaborates with stakeholders for process improvement.	ryufath@indodit.id
Christopher Gerard Lissants	Risk Management	● Manages organizational risk effectively. ● Conducts risk assessments and implements mitigation strategies. ● Guides teams to maintain compliance and awareness.	christopher@indodit.id
Allister Totong	Audit Testing	● Conducts and executes detailed audit testing. ● Identifies deficiencies and suggests improvements.	allister@indodit.id
Andi Muhammad Imam Akbar	Audit Testing	● Conducts and executes detailed audit testing. ● Identifies deficiencies and suggests improvements.	imam@indodit.id

IV. Company Overview

The Company is a multinational supply chain enterprise specializing in consumer goods, that aims to expand its ventures globally. With headquarters in Toronto, Canada, and regional offices across Europe, Asia, Africa, South America, and Oceania, the company demonstrates a commitment to serving diverse markets worldwide. With a strategic network comprising four offices strategically located across the archipelago – Medan, Jakarta, Surabaya, and Makassar – The Company is primed to efficiently cater to the diverse regions of Indonesia, including Sumatera, Bangka Belitung, Jawa, Kalimantan, Bali, Sulawesi, Maluku, Nusa Tenggara, and Papua. Led by a top-level management team overseeing departments such as IT, finance, accounting, risk management, and sales, each office will be equipped with dedicated departments tailored to meet the unique demands of their respective regions.

With a focus on streamlining operations, The Company employs a sophisticated IT infrastructure supported by an extensive range of systems such as HR management, finance and accounting, vendor management, warehouse and logistics, customer relationship management (CRM), and a global corporate website. To ensure smooth communication and operational efficiency, the company follows standardized IT infrastructure rules, standards, and SOPs, which are supported by robust email systems, file systems, intranet, Active Directory, and VPN.

V. Scope

The scope outlines the boundaries and objectives of the audit process of IndoDit, focusing on evaluating the effectiveness, efficiency, and security of an organization's information technology systems and infrastructure. Our team aims to assess the alignment of IT practices with business goals, identify risks and vulnerabilities in IT systems and provide recommendations for improvements to enhance overall IT governance, security, and performance. The audit process is to be conducted in a total of about 930 hours - to optimize efficiency, certain activities will be carried out concurrently on overlapping dates within the project timeline

Phases	Deliverables	Estimated Hours	Timeline
Planning: ● Company Requirements	● Audit Plan	● 40 hours	22 Apr - 30 Apr 2024

Gathering • Identify Specific Resources Required • Define IT Audit Regulation and Standards			
Risk Management: • Recognize Company requirements • Identify potential risks • Assess identified risks to analyze the likelihood and impact • Implement mitigation measures for risk control • Establish a risk monitoring system	• Risk Identification • Risk Assessment • Risk Controls	• 20 hours per region	2 May - 24 May 2024
Access Control Audit: • User Access Rights and Privileges • User Provisioning and De-provisioning (Giving out and revoking access) • Authentication Mechanisms	• IS Control Testing	• 20 hours per region	27 May - 26 July 2024
Infrastructure Audit: • Servers • Network Devices • Security Devices • Endpoints	• Infrastructure Audit Report	• 40 hours per region	27 May - 26 July 2024
Application Audit: • HR Management System • Finance and Accounting Management System • Vendor & Supplier Management System • Warehouse and Logistic Management	• Application Audit Report	• 40 hours per region	27 May - 26 July 2024

System ● Customer-Relationship Management System ● Global Corporate Website			
Data Protection and Privacy Audit: ● Assess company's data protection measure ● Review compliance with data privacy regulations (GDPR & CCPA) ● Evaluate procedures for handling sensitive data	● Data Protection and Privacy Audit Report	● 20 hours per region	29 July - 23 Aug 2024
Incident Response and Business Continuity Audit: ● Review company incident response plan and procedure ● Evaluate backup and disaster recovery plan effectiveness	● Incident Response and Business Continuity Audit Report	● 40 hours	29 July - 23 Aug 2024
Vendor and Third-Party Risk Management Audit: ● Assess company's vendor and third-party risk management practice ● Review contracts, service level agreements, and security assessments for third-party vendors ● Evaluate monitoring and managing vendor security risks process	● Vendor and Third-Party Audit Report	● 20 hours per region	29 July - 23 Aug 2024

Reporting: ● Finalize Plan ● Draft Report ● Follow-up Meeting and Recommendations ● Finalize Report ● Submit Report	● Draft Report ● Final Report	● 20 hours	26 Aug - 30 Aug 2024

VI. Policies & Standards

PT. IndoDit's auditing is based on ISO/IEC 27001:2022 which is one of the world's best-known standards for information security management systems (ISMS). This standard defines requirements an ISMS must meet.

ISO/IEC 27001 standard ensures that business processes and its ISMS adheres to the CIA triad which are confidentiality (in which only the right people can access the information held by the organization), information integrity (in which the data that the organization uses to pursue its business or keeps safe for others is reliably stored and not erased or damaged), and the availability of data (in which the organization and its clients can access the information whenever it is necessary so that business purposes and customer expectations are satisfied. (ISO, 2022)

Risk Management

I. Risk Identification

The first step in the risk management process is to identify potential risks that the company may face. The company should review various sources of information, including local laws and regulations, market conditions, competition, infrastructure, and geopolitical risks. The company can also gather information from local partners and consultants.

● Conduct a thorough review of the local laws and regulations in Indonesia to ensure compliance.

● Analyze the market conditions, including competition, customer demand, and supply chain capabilities.

● Assess the infrastructure in the areas where the company plans to set up offices, including transportation, power supply, and communication networks.

● Identify geopolitical risks that may affect the company's operations, such as political instability, social unrest, and natural disasters.

II. Risk Assessment

Once potential risks are identified, the next step is to assess the likelihood and impact of each risk. This process can be done by using a risk matrix to categorize risks based on their likelihood and impact.

● Develop a risk matrix to categorize risks based on likelihood and impact.

● Assign a numerical value to each risk based on the likelihood and impact.

● Evaluate the risks and identify the top risks that require immediate attention.

● Develop a risk mitigation plan for each high-priority risk.

III. Risk Controls

After identifying and assessing the risks, the final step is to implement risk control measures to mitigate the risks.

● Develop a risk control plan for each high-priority risk identified in the risk assessment phase.

● Implement risk control measures, such as contingency plans, risk transfer mechanisms, and risk avoidance strategies.

● Establish a risk monitoring system to track the effectiveness of the risk control measures.

Test Plan to test the IS Controls

I. Access Control

There are many roles and functions that use the application. So, for security purposes, not all have the same access level. Limitation of certain user’s authority and access.

A. **Test objectives**: Ensure that every user access has the appropriate restriction, roles and responsibilities.

B. **Test deliverables:** A comprehensive document detailing the role of each user and its restrictions and responsibilities.

C. **Strategies**: Test each role or access level to see if each of them have the correct access and have certain functions sealed off for certain roles.

D. **Environment**: ID Card, MFA(Multi-level Authentication), Passwords, and Biometric Scan.

E. **Test data**: All of the user's role and its corresponding access have been assigned appropriately.

II. Infrastructure Controls

The procedures, and technical measures put in place to safeguard an organization's IT infrastructure of the software, hardware from external threats. This involves the networks, servers, databases, applications, and other critical components that support business operations.

A. **Test objectives**: Assess whether it has met standardize industry grade requirements for infrastructure. Evaluate the infrastructure's effectiveness in mitigation and defense from risks. Identify any possible weakness.

B. **Test deliverables**: Infrastructure analysis report including any weakness, strengths, and any possible improvements.

C. **Strategies**: Review of policy and procedures that has been prepared by the company regarding access control, network segmentation, encryption, and patch management. Check the comprehensiveness of the policies. Assess the technical parts of the infrastructure. Conduct tests for incident response, access control, and data protection.

D. **Environment**: Conduct tests within the organization infrastructure.

E. **Test data**: The system that is used by the organization to use synthetic data to conduct simulation.

III. Application Controls

Specific procedures, policies, and automated measures implemented within an application to ensure the accuracy, completeness, integrity, and security of data throughout its lifecycle. The security of the software, hardware from external threats.

A. **Test objectives**: Validate the accuracy, completeness, and timeliness of data processing. Ensure the presence and capabilities of the antivirus and firewall installed.

B. **Test deliverables**: Report of any external threats that can interrupt the system. Note any weaknesses and any possible improvement that can be made to the application.

C. **Strategies**: Conduct test input validation, error handling, and transaction processing to see how the application handles misuse of the application. It is done to see whether these misuse or mis-input can be prevented from entering the system, which could endanger the processes within the system. Also check if the output also functions properly, displaying the result as how it must be. Testing of how monitoring & logging can also be done to ensure logs are done correctly. Configuration management reviews are also done to ensure proper settings and any other risk prevention that can happen through the application.

D. **Environment**: Conduct testing either in the organization's system or in a sandbox environment.

E. **Test data**: Application architecture to understand the data flow, components, and interfaces. Data set that will be used would be synthetic data.

IV. Data Security and Privacy Controls

Data security and privacy are the policies, procedures, and measures that are taken for the protection of data during transit and rest.

A. **Test objectives**: Test the encryption of data to ensure that the data remains safe from unauthorized readers during transit or rest. Assess data masking, tokenization, and anonymization techniques. And lastly, verify data integrity and confidentiality.

B. **Test deliverables**: Data security analysis report, mentioning any strength, weaknesses, and possible improvements that can be made for the security

C. **Strategies**: Review the policies and methods used for encryption to ensure that it is done maximally. Run tests to decode the encryptions. See how long it would take to decrypt the code and before attempts are detected.

D. **Environment**: Test is conducted during data transfer and data storing be it in the server, vendor, or the application used by the users.

E. **Test data**: Synthetic data are used to check if the security can keep the confidentiality and integrity.

V. Incident Response and Business Continuity Controls

In the event of a risk coming to reality, there are plans on how to respond to an incident and the recovery from the incident.

A. **Test objectives**: Test the effectiveness of the monitoring and response team.

B. **Test deliverables**: A comprehensive report containing the testing strategies, testing result/data and recommendation for future mitigation. List down any strength or weakness.

C. **Strategies**: Review the protocols that the company has set up for the method of detecting and responding to an incident. Test logging, monitoring, and alerting mechanisms. Check for the detection system capabilities to ensure that it has the most updated to detect and counter the attacks. Another set of actions are to conduct a mock up test. Launch an attack against the system and see how fast detection is and the effectiveness of the response team.

D. **Environment**: Conduct testing virtually within the company's network, server, or test devices as the users.

E. **Test dat**a: All levels of effectiveness and its detection capability has been reached to the acceptable level of result.

VI. Vendor and Third-Party Risk Management Control

Third parties or vendors may be employed by the organization. This is controlled with policies, procedures, and practices to identify, assess, mitigate, and monitor risks associated with its vendors, suppliers, and third-party service providers.

A. **Test objectives**: Testing the personnel that are involved with the system regarding their knowledge, effectiveness in work, and identify gaps.

B. **Test deliverables**: A comprehensive report containing the training control and its corresponding testing result/data.

C. **Strategies**: Conduct investigation to see if the personnel in the vendor and third-party have sufficient knowledge for the task from interview or reviewing documents. Check the system and the flow of the usage of third party and vendors to ensure that the system has met the standard. Next is to conduct testing with a scenario to see how the third party personnels react to the test.

D. **Environment**: Conduct tests virtually within the organization network.

E. **Test data**: The data used for the testing are synthetic data within a simulated scenario to test the personnels.

VII. Exit Parameters

To close and finalize the auditing process, the following exit parameters must be satisfied in order for the testing to be deemed finished and the audit procedure to be finished, they are:

1. Ensuring the completion of all planned deliverables, including reports and documentation, to satisfaction.
2. Verifying the adherence to ISO/IEC 27001:2022 standards throughout the audit, maintaining consistency with (ISMS).
3. Ensuring all possible risks and deficiencies can be mitigated
4. Reviewing all audit documentation for accuracy, completeness, and clarity, engaging relevant stakeholders.
5. Conducting a quality review of audit reports to validate accuracy, relevance, and reliability.

The audit team will evaluate the actual results to the expected outcomes to assess the audit's performance and the effectiveness of the company's IS controls. If major discrepancies or concerns are discovered, further testing or follow-up actions may be suggested.

Information System Audit

PT. Indo Audit (IndoDit)

- Ryufath A. A. P. Soepeno
- Allister Totong
- Andi M. Imam Akbar
- Christopher G. Lissants

TABLE OF CONTENTS

01 About Company

02 Company Overview

03 Audit Standards

04 Audit Components

05 Risk Management

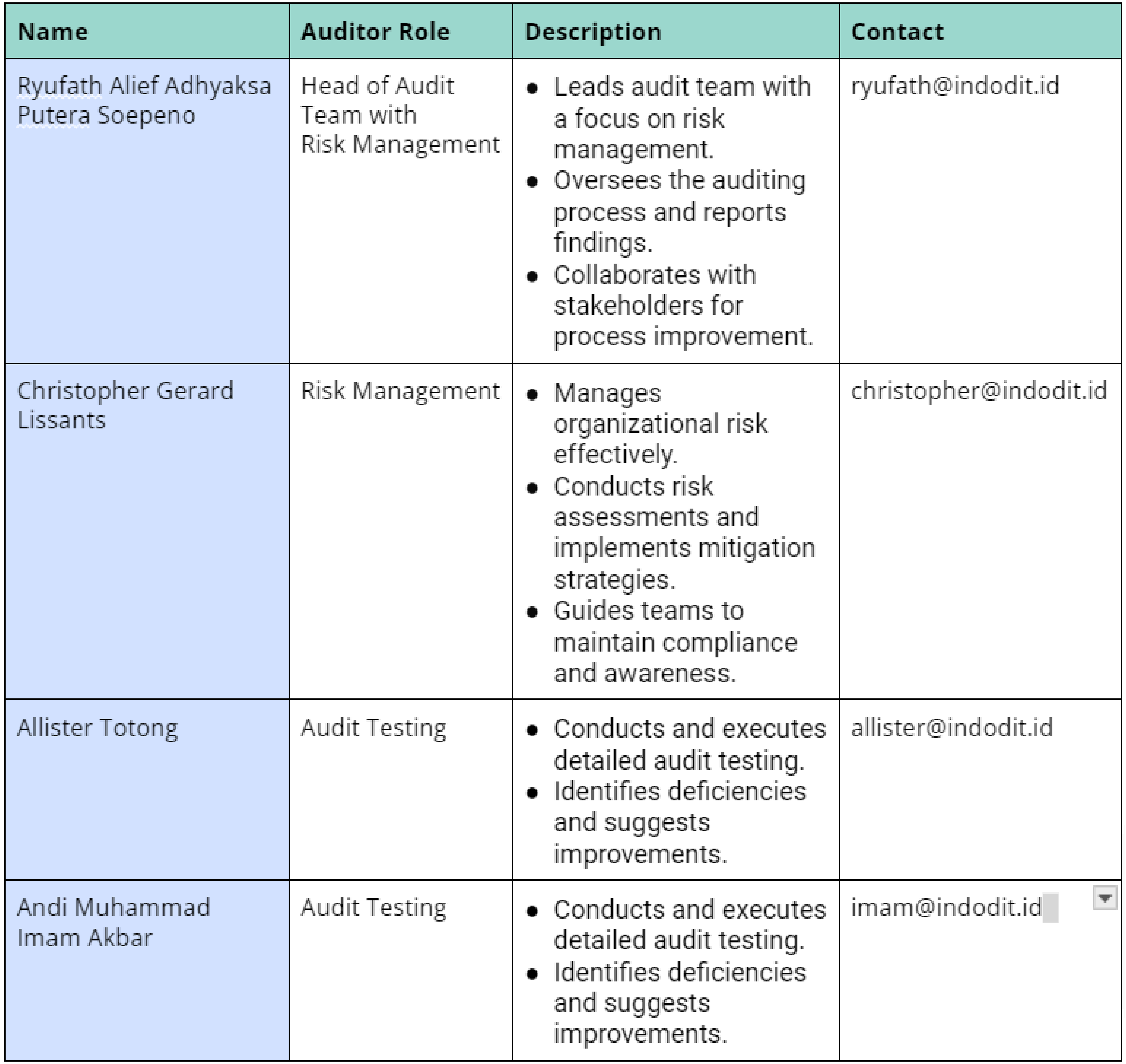
06 Testing Control

INTRODUCTION

As multinational supply chain companies are establishing their ventures in Indonesia, our audit team is committed to conducting an audit to thoroughly provide a structured approach to examining and evaluating the company's IT infrastructure, access controls, and data management processes.

Our audit plan will assess the company's IT infrastructure policies, Standard Operating Procedures (SOPs), and access privileges for stakeholders, ensuring the security, integrity, and availability of the main ISMS and its applications.

Company Members & Responsibilities



Name	Auditor Role	Description	Contact
Ryufath Alief Adhyaksa Putera Soepeno	Head of Audit Team with Risk Management	• Leads audit team with a focus on risk management. • Oversees the auditing process and reports findings. • Collaborates with stakeholders for process improvement.	ryufath@indodit.id
Christopher Gerard Lissants	Risk Management	• Manages organizational risk effectively. • Conducts risk assessments and implements mitigation strategies. • Guides teams to maintain compliance and awareness.	christopher@indodit.id
Allister Totong	Audit Testing	• Conducts and executes detailed audit testing. • Identifies deficiencies and suggests improvements.	allister@indodit.id
Andi Muhammad Imam Akbar	Audit Testing	• Conducts and executes detailed audit testing. • Identifies deficiencies and suggests improvements.	imam@indodit.id

Company Overview

Geographic Expansion

Strategic network strategy goals comprising offices in Medan, Jakarta, Surabaya, and Makassar, Indonesia

IT Infrastructure

Sophisticated infrastructure supporting diverse operations (HR, vendor, logistcs, CRM, etc.), with standardized protocols.

Management Structure

Top-level management (IT, Finance, Risk Management) overseeing key departments, with tailored regional teams

Operational Efficiency

Focus on streamlined operations supported by efficient IT systems and protocols to ensure adherence to SOPs and standards.

Audit Standard

ISO/IEC 27001:2022

- One of the Best Standards for Information Systems Management Systems
- Ensures business process adheres to CIA Triad

Why ISO 27001?

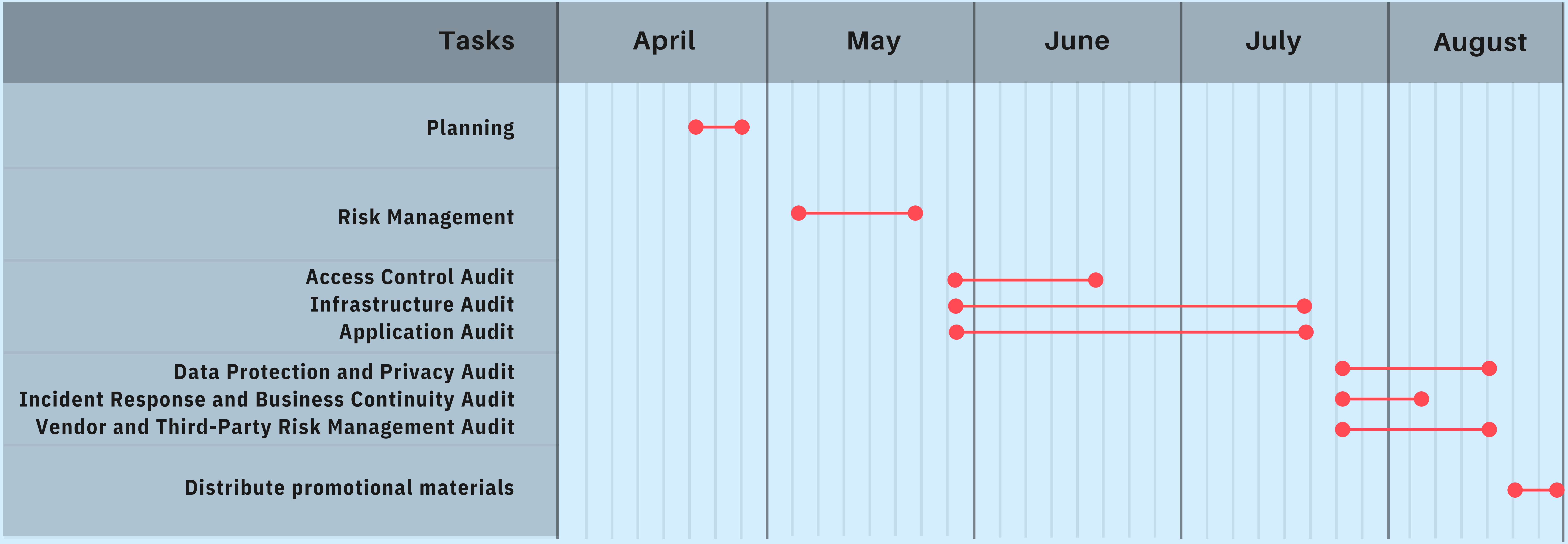
- Raises cyber-risk awareness
- Proactively identify and address weaknesses
- Vetting People, Policies, and Technology

Audit Components

- Access Control
- Infrastructure
- Application
- Incident Response
- Data Security & Privacy
- Vendor & Third-party Risk
- Risk Management

AUDIT SCOPE

Scheduling



Risk Management

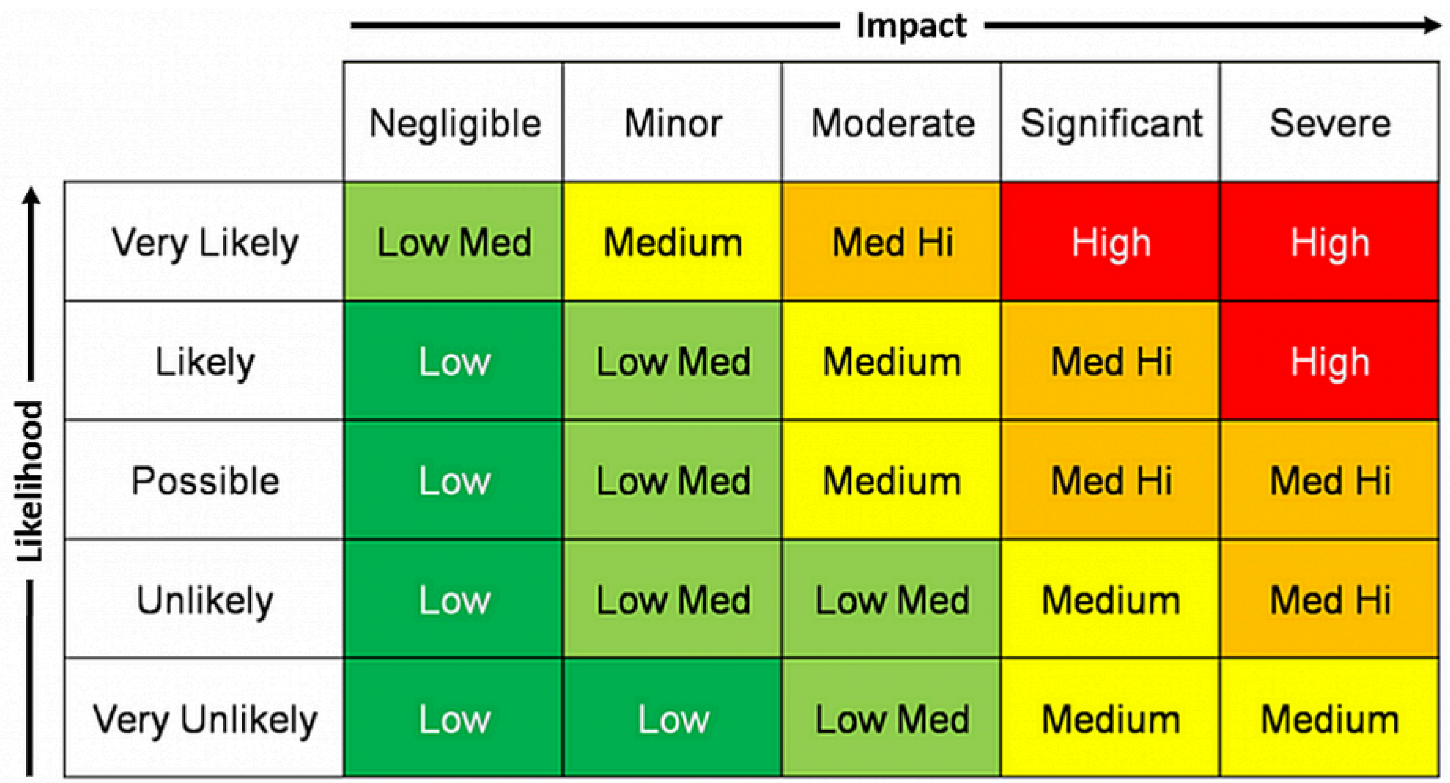
1. Risk Identification

The first step in the risk management process is to identify potential risks that the company may face, which is done by:

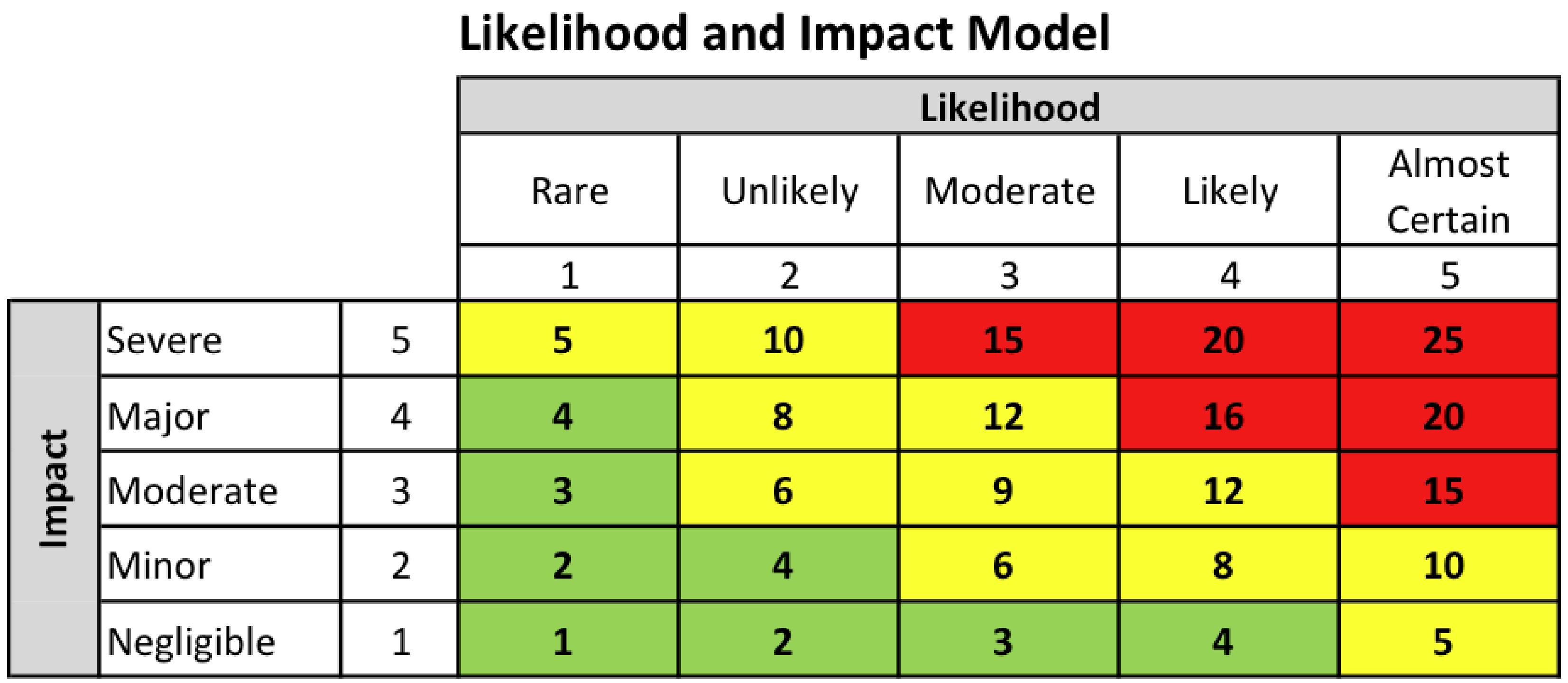
- Analyze the market conditions, including competition, customer demand, and supply chain capabilities.
- Conducting a thorough review of the local laws and regulations in Indonesia to ensure compliance.
- Assess the infrastructure in the areas where the company plans to set up offices, including transportation, power supply, and communication networks

2. Risk Assesment

- Risk Matrix to Categorize Risk based on Likelihood & Impact
- Assign numerical value to each risk based on Likelihood & Impact
- Evaluate & Identify Top Risks that need Immediate Attention
- Develop Risk Mitigation Plan for each High-Priority Risk



Likelihood	Impact				
	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium



Likelihood and Impact Model

			Likelihood				
			Rare	Unlikely	Moderate	Likely	Almost Certain
			1	2	3	4	5
Impact	Severe	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5

3. Risk Control

- Develop risk control plan for each high-priority risk
- Implement risk control measures:
  - Contingency Plan
  - Risk Transfer Mechanism
  - Risk Avoidance Strategy
- Establish Risk Monitoring System

Testing

ACCESS CONTROL

OBJECTIVES

Ensure user access has the appropriate access level.

STRATEGY

Test each role/access level to check for correct access and authorization.

ENVIRONMENT

ID Card, MFA, Passwords, and Biometric Scan.

DELIVERABLES

Document for users role.

TEST DATA

All user's role function.

INFRASTRUCTURE CONTROL

OBJECTIVES

Evaluate infrastructure effectiveness and compliance.

DELIVERABLES

Infrastructure analysis report

STRATEGY

Review of policy and procedures about:

- Access control
- Network segregation
- Encryption
- Patch management
- Technical parts
- Incident report
- Data protection

ENVIRONMENT

In organization infrastructure

TEST DATA

Synthetic data set for simulation

APPLICATION CONTROL

OBJECTIVES

Validate the accuracy, completeness, and timelines.

DELIVERABLES

Report of any external threats to application.

STRATEGY

- Input validation test
- Error handling test
- Transaction processing test
- Monitoring test
- Logging test
- Review configuration

ENVIRONMENT

Organization system or sandbox environment.

TEST DATA

Application architecture and synthetic data set.

DATA SECURITY & PRIVACY CONTROL

OBJECTIVES

To evaluate sensitive data handling and ensure that the Company adheres to regulation

DELIVERABLES

- Assess data security & privacy control effectiveness.
- Generate Audit Report, highlighting concerns and prioritizing remediation action.

STRATEGY

- Review Data Classification Policy & Procedure, including assessment of regulation compliance (GDPR/CCPA/UU PDP)
- Review Access Control Mechanism and Test User Authentication.
- Assess Data Encryption Implementation and Data Loss Prevention solutions

ENVIRONMENT

Environments include, Organization, Business Application, Vendors, and Third-Party

TEST DATA

Synthetic data set for testing.

INCIDENT RESPONSE ANF BUSINESS CONTINUITY CONTROL

OBJECTIVES

Evaluate organization's ability to detect and respond to an incident and their continuity

DELIVERABLES

- Assessment of IR/BC control effectiveness
- Generate Audit Report, highlighting areas of concern and prioritizing remediation action

STRATEGY

- Review Incident Response Plan and assess member roles, responsibilities, and awareness.
- Conduct security incident simulation.
- Monitor detection and response time.
- Test of maintaining critical business operations and time to activate business continuity measures.

ENVIRONMENT

Organization's network, server, and user devices

TEST DATA

Detection system, logs during test

VENDOR AND THIRD-PARTY RISK MANAGEMENT CONTROL

OBJECTIVES

Evaluate knowledge, effectiveness, and gaps in third party personnel.

DELIVERABLES

Training control report and corresponding testing result/data

STRATEGY

- Interviewing personnel
- Review records
- Check system flow of third party
- Test scenario

ENVIRONMENT

Organization network simulation.

TEST DATA

Synthetic data set.

EXIT PARAMETERS

To close and finalize the auditing process, the following exit parameters must be satisfied in order for the testing and the audit procedure to be considered finished, they are:

- Ensuring completion of all planned deliverables, including reports and documentation, to satisfaction.
- Verifying adherence to ISO/IEC 27001:2022 standards throughout the audit, maintaining consistency with (ISMS).
- Ensuring all possible risks and deficiencies can be mitigated
- Reviewing all audit documentation for accuracy, completeness, and clarity, engaging relevant stakeholders.
- Conducting a quality review of audit reports to validate accuracy, relevance, and reliability.

If major discrepancies or concerns are discovered, further testing or follow-up actions may be suggested

From PT. Indo Audit, we would like to say:

Thank You!