Information System Audit

PT. Indo Audit (IndoDit)

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

TABLE OF CONTENTS

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?

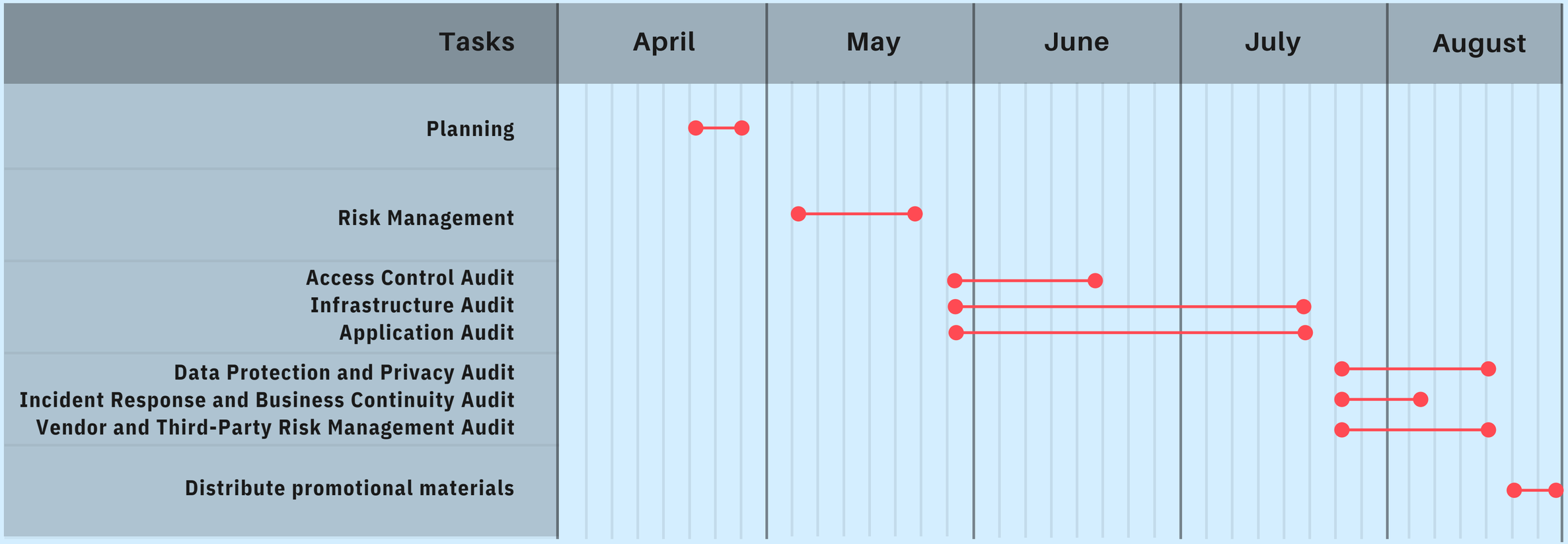
- Raises cyber-risk awareness
- Proactively identify and address weaknesses
- Vetting People, Policies, and Technology

Audit Components

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

AUDIT SCOPE

Scheduling



Risk Management

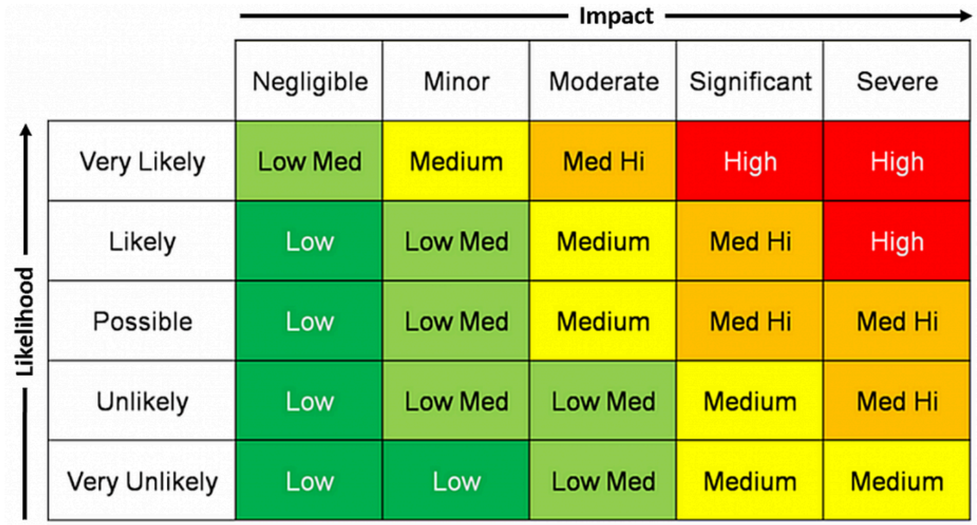
1. Risk Identification

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.

STRATEGY

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

ENVIRONMENT

Organization network simulation.

DELIVERABLES

Training control report and corresponding testing result/data

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!