

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

After the discussion, we create these SOP with the following information:

Document Number : KG/FBC/SOP-EN/009/00
Title : Risk & Opportunity Assessment
Document Owner : Finance – Business Process
Effective Date : 01-11-2021

DOCUMENT APPROVAL

Created by	Reviewed by	Approved by	Approved by
			
JIMMY KOSASIH	PRADEEP KUMAR	ANUJ KUMAR MAHESHWARI	HITESH BHARWANI
Business Process Excellence Manager	Business Control Executive Manager	Group CFO, Finance & Accounting	Group Managing Director

NOTE

1. When the latest revision has been approved, the previous document is declared invalid (Obsolete).
2. Submission for revision requested by each Sub Department Manager, must be reviewed by Head of Department and Business Process Excellence Manager, and approved by the Director in Charge.
3. The approved SOP must be socialized to the relevant Kanmo Group employees.

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

Contents

1. PURPOSE 3

2. SCOPE..... 3

3. DEFINITION..... 3

4. REFERENCE 4

5. RESPONSIBILITY 6

6. POLICY..... 6

7. PROCEDURE..... 7

8. ATTACHMENT 8

9. DOCUMENT HISTORY 8

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

1. PURPOSE

The purpose of this SOP is to provide guidance to each Head of Department (HOD) as a Risk Owner, in terms of risk assessment.

2. SCOPE

This SOP covers the process of making an Information Security Management System Risk Assessment (SMKI), starting from identifying external and internal issues, risks and opportunities from these issues, to determining mitigation methods to deal with identified risks.

3. DEFINITION

- 3.1. **Risk** is the effect of uncertainty on the target or uncertainty that has an impact (effect) on the target. The effect is deviation (deviation) from the expected target. It can be positive, negative or both, and can address, create or generate opportunities and threats.
- 3.2. **Risk Assessment** is an activity carried out by risk owners to identify events, causes, impacts, types, levels, ongoing controls and handling of risks related to their functions or work units.
- 3.3. **Risk Management** is a coordinated activity to direct and control the organization related to risk.
- 3.4. **Risk Owner** is an individual who is responsible for ensuring that risk is managed properly in a single section or work unit. Risk Owner has direct responsibility for risk management, supervision, and activities to manage each risk. Risk Owner is attached to the positions of Directors, Directors of subsidiaries, Head of Department, and Project Manager.
- 3.5. **Risk Champion** is a person appointed to assist the Risk Owner in analyzing risk management. The Risk Champion is usually a part of the management within the institution that supports the risk management process in its area or function.
- 3.6. **Risk Expert** is a person appointed to validate a specific risk based on his/ her capabilities and expertise.
- 3.7. **Consequence/ Impact** is a result of events that affect the target.
- 3.8. **Probability** is the possibility of something happening.

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

4. REFERENCE

- 4.1. Manual Information Security Management System.
- 4.1. ISO/IEC 27001:2013: Information Security Management System.

Clause	Clause Statement
6.1.1	<p>General actions to address risks and opportunities.</p> <p>When planning for the information security management system, the organization shall consider the issues referred to in 4.1: Understand the organization and its context, and the requirements referred to in 4.2: Understanding the needs and expectations of interested parties, and determine the risks and opportunities that need to be addressed to:</p> <ul style="list-style-type: none"> a) Ensuring the information security management system can achieve its intended outcome(s); b) Prevent, or reduce undesired effects; c) Achieve continual improvement. <p>The organization shall plan:</p> <ul style="list-style-type: none"> d) Actions to address these risks and opportunities; and e) How to integrate and implement actions into its information security management system processes, and evaluate the effectiveness of these actions.
6.1.2	<p>Information Security Risk Assessment.</p> <p>The organization shall define and apply an information security risk assessment process, that:</p> <ul style="list-style-type: none"> a) Establishes and maintains information security risk criteria that include: <ul style="list-style-type: none"> 1) The risk acceptance criteria; and 2) Criteria for performing information security risk assessments. b) Ensuring that repeated information security risk assessments produce consistent, valid and comparable results; c) Identifies information security risks; <ul style="list-style-type: none"> 1) Apply the information security risk assessment process to identify risks associated with loss of confidentiality, integrity and availability for information within the scope of ISMS; and 2) Identify the risk owners.

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

	<p>d) Analyze the information security risks;</p> <ol style="list-style-type: none"> 1) Assess the potential consequences that would result if the risks identified at 6.1.2 c) 1) were to materialize; 2) Assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) Determine the levels of risk. <p>e) Evaluates the information security risks;</p> <ol style="list-style-type: none"> 1) Compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) Prioritize the analyzed risks for risk treatment. <p>The organization shall retain documented information about the information security risk assessment process.</p>
6.1.3	<p>Information security risk treatment</p> <p>The organization shall define and apply an information security risk treatment process to:</p> <ol style="list-style-type: none"> a) Select appropriate information security risk treatment options, taking account of the risk assessment results; b) Determine all controls necessary to implement the information security risk treatment option(s) chosen; c) Compare the controls specified at 6.1.3 b) above with those in Appendix A and verify that no control is required; d) Produce a Statement of Applicability containing the necessary controls (see 6.1.3 b) and c)) and the reasons for inclusion, whether or not the control is applied, and the reasons for the exclusion of control from Appendix A; e) Formulate a plan for handling information security risks, and f) Obtain the owner's approval of the risk to the information security risk management plan and accept the remaining information security risks.

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

5. RESPONSIBILITY

- 5.1. **Risk Owner** is responsible for ensuring that risk is managed appropriately within one part or work unit.
- 5.2. **Risk Champion** is responsible for analyzing risk management within the scope of the department where the Risk Champion is assigned.
- 5.3. **Risk Expert** is responsible for validating, assessing risk based on their capabilities and expertise. Risk Expert also serves as a facilitator at the corporate level of Kanmo Group, managing: risk registers, generating risk reports, coordinating control functions from the second line and coordinating with functions from the third line (assurance service providers).

6. POLICY

The related policies are used as a reference for SOP of Risk & Opportunity Assessment, including but not limited to:


- 6.1. The main responsibility for Risk Management lies in stages with all parties who are included in the first line of the Three Lines of Defense, namely the Risk Owner.
- 6.2. The second line supports the first line in the form of guidance, direction, monitoring and advice on risk management.
- 6.3. The third line, namely External Audit, Internal Audit and other “assurance” service providers, conducts independent reviews on the effectiveness of control and risk management.
- 6.4. Each Risk Owner of each department in the Head Office and Warehouse, must fill out/ update **Risk & Opportunity Assessment Form**.
- 6.5. Each Risk Owner is assisted by a Risk Champion - required to carry out a risk assessment. Each risk that has been identified must be determined by the level of probability, impact and priority. The level of probability, impact and priority can be seen in the **Risk & Opportunity Assessment Work Instruction**.
- 6.6. For identified opportunities, it is not necessary to assess probability and impact levels.
- 6.7. The Risk Champion reports the results of the Risk & Opportunity Assessment to the Business Process: Risk Management Unit.
- 6.8. Each Risk Owner must reduce the risk it manages to an acceptable level, with reference to the established principles, action guidelines and risk management behavior guidelines.

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

- 6.9. The risk owner must measure risk and control (impact, occurrence and indicators) using both quantitative (speak by data) and qualitative methods that can be accounted for.
- 6.10. The Risk Champion coordinates the PIC Risk at the operational level, compiles the results of the PIC Risk and facilitates risk analysis together with the Risk Owner.
- 6.11. Risk Experts provide an assessment of the specific risks that are their area of expertise.
- 6.12. Business Process: Risk Management Unit, serves as a facilitator at the corporate level of the Kanmo Group, manages: risk registers, produces risk reports, manages the Risk Management framework, coordinates the control functions of the Second Line and coordinates with the functions of the Third Line (assurance service providers) .
- 6.13. Controlled risks must be integrated into the Company's ISMS document.

7. PROCEDURE

- 7.1. Each Risk Owner determines external issues and internal issues.
- 7.2. The Risk Owner determines the risks/opportunities associated with the issue.
- 7.3. Each risk that has been identified must be determined by the level of probability and impact. Probability and impact levels can be seen in **Risk & Opportunity Assessment Work Instruction**.
- 7.4. For identified opportunities, it is not necessary to assess probability and impact levels.
- 7.5. Evaluate the risk value by comparing it with the criteria listed in **Risk & Opportunity Assessment Work Instruction**.
- 7.6. If the evaluation result of the priority value is Low Risk, the Risk Owner determines the action that functions to maintain the identified risk. And write the status close in the status column.
- 7.7. If the evaluation result of the priority value is still of High Risk and Medium Risk, then the Risk Owner determines the action to overcome the potential risk along with the time limit and the person/team responsible for carrying out the action so that the priority value can be reduced to Low Risk.
- 7.8. Prepare and implement actions that have been determined and approved by Management.
- 7.9. After passing the time limit, the Risk Owner will assess the residual risk by re-determining the level of Probability, Impact and Priority. Probability, Impact and priority evaluation results can be seen in **Risk & Opportunity Assessment Work Instruction**.

 KANMO GROUP www.kanmogroup.com	STANDARD OPERATING PROCEDURE		RISK & OPPORTUNITY ASSESSMENT
	DOCUMENT NUMBER: KG/FBC/SOP-EN/009/00	REV...: 00	

- 7.10. If the priority evaluation results are still High Risk and Medium Risk, the Risk Owner determines alternative actions to address the identified risks.
- 7.11. If the results of the priority evaluation are Low Risk, the Risk Owner determines actions that function to maintain the identified risks. And write the status close in the status column.
- 7.12. The Risk & Opportunity Assessment will be reviewed and updated every 3 (three) months or if there are changes in internal or external issues.
- 7.13. Discussion on risk & opportunity assessment that has been made by each Risk Owner, assisted by the Risk Champion from his department, held a joint meeting with the Business Process: Risk Management unit.

8. ATTACHMENT

- 8.1. KG/FBC/WI-EN/001/00: Risk & Opportunity Assessment Work Instruction.
- 8.2. KG/FGC/FORM/021/00: Risk & Opportunity Assessment Form.

9. DOCUMENT HISTORY

Revision	Date (DD-MM-YYYY)	Description