HUMANICA

Risk Management Policy

Document Version: 1.0

Document No: ISMS-PL-12

Document Owner: ISMR/ISMA

Last Updated: 31-07-2020

Document Control

Document Approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Approved by
IT Security	*Head of Department*	*Chief Technology Officer*
Date : 01-07-2020	**Date :** 08-07-2020	**Date :** 15-07-2020

Version History

The following table lists all the revisions made to this document:

Version	Date	Description	Revised By
1.0	31-07-2020	Initial version	

Reference: ISO 27001:2013 Requirement

Clause	Requirement
8	Operation 8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment

HUMANICA

Table of Contents

Risk Management policy

Purpose

- Establish a framework for the organization risk management process to provide understanding and knowledge of concept, methodology, assessment and processes of risk management to management team and staffs.
- For securing the Information systems that store, process, or transmit organizational information.

Scope

This policy and procedure are setup for all information systems that connected to the ISMS scope. All employees, contractors, sub-contracts, trainee, partners who work on the Information system should be followed this policy.

Definition

Risk is the sum or consequence of an event that uncertainty affecting an objective. It has potential to happen both positive and negative impacts in the future. If the negative impacts such as damage, leakage, crash, waste or unwanted incident happen, it will cause the organization failed to achieve its purpose. It is important to consider the likelihood of occurrence and the impact of the events.

Risk Management is the process of managing the factors and controlling the activities, including the operational processes by reducing the cause of opportunity to cause the damage from nonconforming operation plan. And to manage the level of damage and impacts that might be occurs in the future to the company acceptable levels.

Risk Management Framework is the principle and approach used to manage risk, determine the policies or objectives, including the design and management for implementation, follow up or improve the continuity of risk management in every department in the organization to reduce the damage cause of company and maintain level of risks and impacts into acceptable levels.

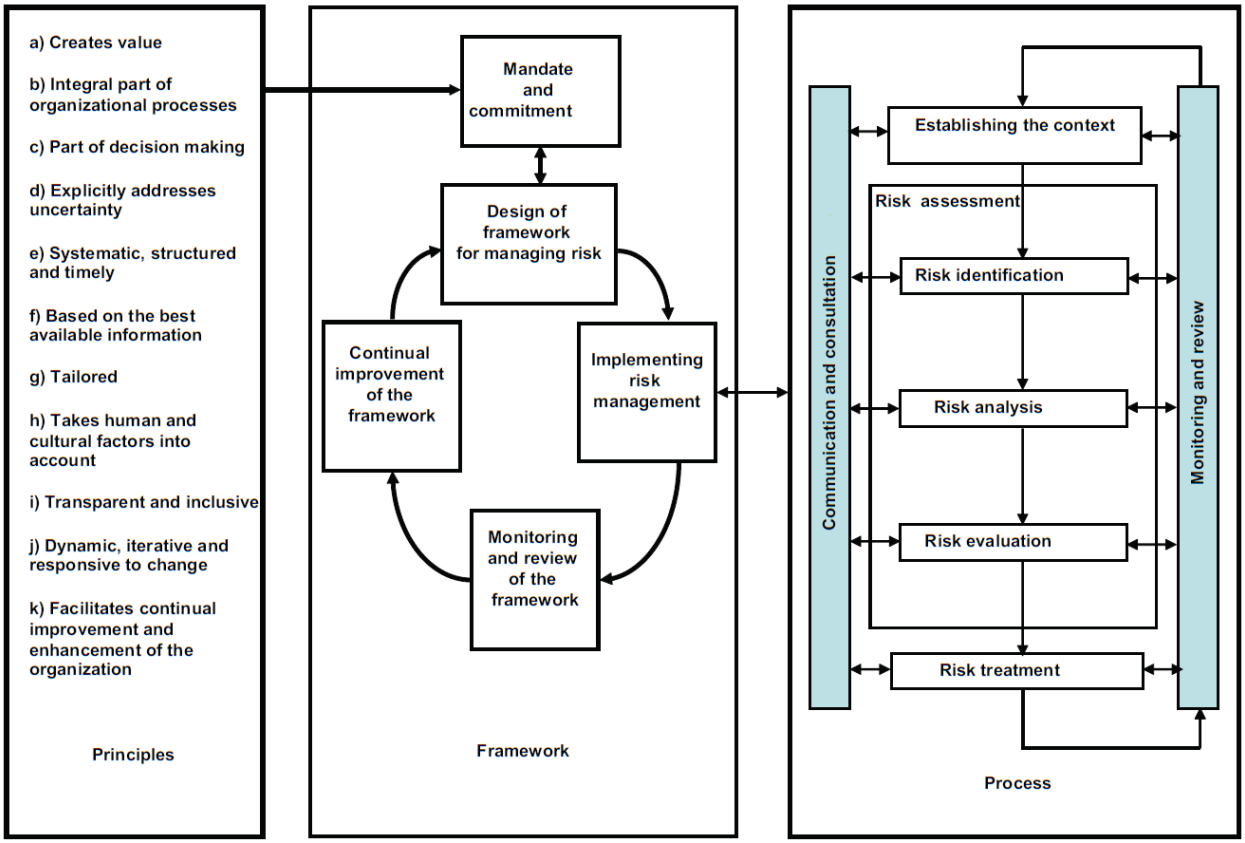
Risk Assessment is the process of identifying risk items and issues, Analyze the cause or factors that may hinder the achievement corporate objective. To determine the level of impact

if the risk is actually happened. Determine the risk value and the risk event. The risk rating is based on the likelihood and impact of the damaging occurs if the risk occurs

Risk Register is a database of risks that face an organization at any one time. Always changing to reflect the dynamic nature of risks and the organization's management of them, its purpose is to help managers prioritize available resources to minimize risk and target improvements to best effect.

Risk Management Framework

The risk management process focuses on providing the business with an understanding of risks to allow effective decision-making to control risks. The risk management process is an ongoing activity that aims to continuously improve efficiency and effectiveness of the Information Security Management System (ISMS). The relationship between the elements of risk management in accordance with ISO 31000:2009 is divided into 3 main parts 1) Principle of Risk management 2) Framework of risk management 3) Process of Risk management.



Principle

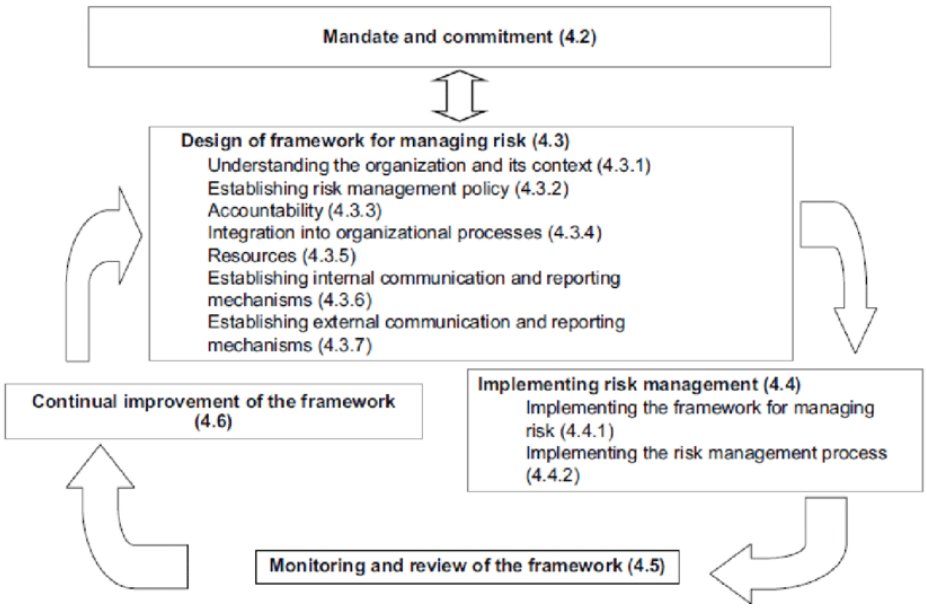
for risk management to be effective, company shall comply at all levels with the following principles.

1. Creates and protect company value
2. An integral part of all organization processes
3. Part of decision making
4. Explicitly address uncertainty
5. Base on the best available information
6. Risk management is tailored to organization
7. Take human and cultural factors into account
8. Transparent and inclusive.
9. Dynamic, iterative and responsive to change
10. Risk management facilitates continual improvement of the organization

Encryption in Portable Computer Devices

The framework assists in managing risks effectively through the risk management process. Divided into 4 parts.

1. Design of framework for managing risk
2. Implementing risk management
3. Monitor and review the framework.
4. Continual improvement of the framework.



1) Mandate and commitment

The company management boards have direction of “Being a world class of professional HR and Payroll outsourcing provider in Asia Pacific” which can be trusted and reliable. To achieve this, organization will incorporate various factors into the risk assessments to improve services do the company can become a leader in service delivery. Consist of

1. Define and endorse the risk management policy
2. Ensure the organization culture and risk management policy are aligned.
3. Determine risk management performance indicators that align with performance indicators of the organization
4. Align risk management objectives with the objectives and strategies of the Organization
5. Ensure legal and regulatory compliance.
6. Ensure that the necessary resources are allocated to risk management.
7. Ensure that the framework for managing risk continues to remain appropriate.

2) Design of framework for managing risk

The process of designing an organization’s risk management begins with an understanding of the internal environment, outside organization. Understanding the internal and external issues of an organization has several issues related to ISO31000:2009 as follows

1. Understanding of the organization and its context.
   Evaluating the organization’s external context may include but not limited to
   - The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment
   - Key drivers and tends having impact on the objectives of the organization.
   - Relationships with and perceptions and values of external stakeholders.
2. Evaluating the Organization’s Internal context
   - Policies, objectives and the strategies that are in place to achieve them
   - Information systems, information flows and decision-making processes
   - Relationship with and perceptions and values of internal stakeholders
   - The organization’s cultures
   - Standards, guideline, and models adopted by the organization.
3. Establishing risk management policy
   The risk management policy should clearly state the organization’s objectives for, and commitment to.
   - Link between the organization’s objectives and policies and the risk management policy

- Accountabilities and responsibilities for managing risk
- Commitment to make the necessary resources available to assist those accountable and responsible for managing risk.

3) Implementing risk management

1. The organization should define the appropriate timing and strategy for implementing the framework
2. Apply the risk management policy and process to the organizational processes
3. Comply with legal and regulatory requirements.
4. Ensure that decision making
5. Hold information and training sessions
6. Communicate and consult with stakeholders to ensure that its risk management framework remains

4) Monitoring and review of the framework

1. To ensure that risk management is effective and continues to support organizational performance, the organization should
2. Measure risk management performance against indicators.
3. Periodically measure progress against and deviation from the risk management plan
4. Periodically review the risk management framework, risk assessment, policy and plan are still appropriate.
5. Review the effectiveness of the risk management framework

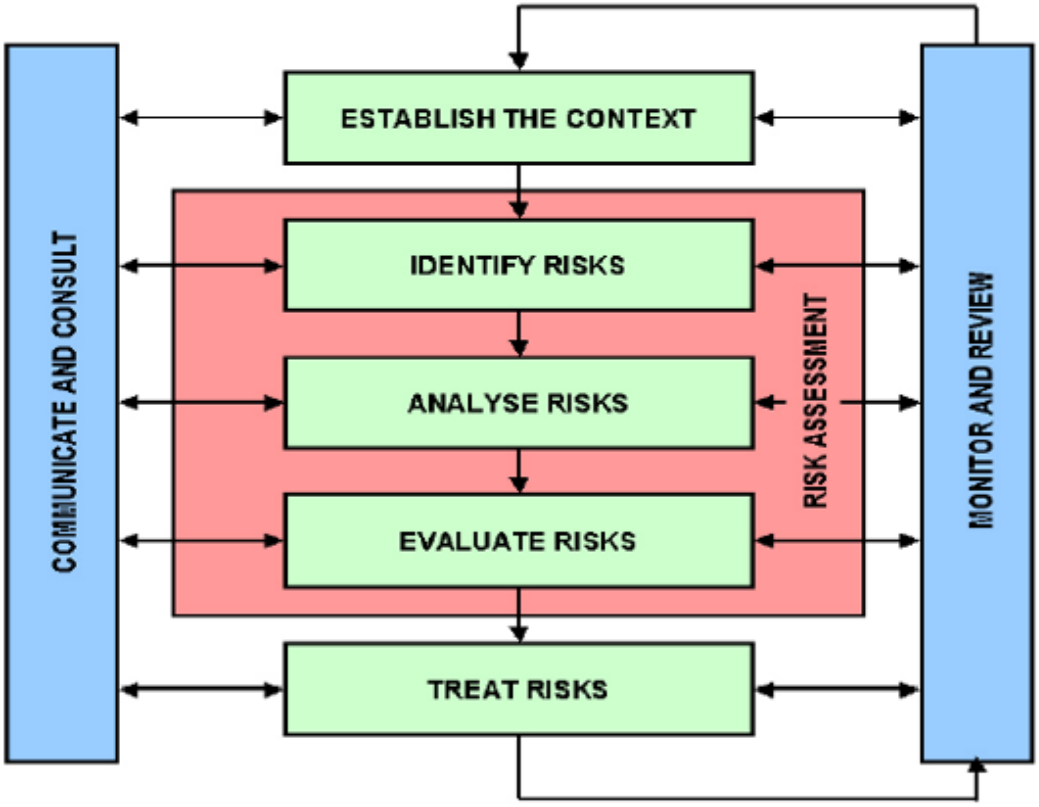
5) Continual improvement of the framework

Based on results of monitoring and reviews, decision should be made on how the risk management framework, policy and plan can be improved.

Process

Risk management process should be

1. An integral part of management
2. Embedded in the culture and practices
3. Tailored to the business processes of the organization.


ESTABLISH THE CONTEXT
IDENTIFY RISKS
ANALYSE RISKS
EVALUATE RISKS
TREAT RISKS
RISK ASSESSMENT
COMMUNICATE AND CONSULT
MONITOR AND REVIEW

Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

1. Identify the risks

   When the context of the business has been defined, we use this information to identify risks that may affect, either negatively or positively to the objectives of the business and all its activity.

   Risks can be retrospective risks or prospective risks. Retrospective risks identification is the most common way to identify risk and the easiest. Its impact has already been experienced. Retrospective risks are seen in incidents or accidents that have occurred in the past. It is easier to quantify its impact and to evaluate the damage.

   Sources of information about retrospective risk can be found from

   - Incident logs or audit reports
   - Customer complaints
   - Staff or client surveys
   - Newspapers, journal, website
   - Accreditation documents and reports

   Prospective risks are harder to identify. These are things that have not yet happened, but might happen in the future. Identification should cover all risks, whether or not they are currently managed. The plan will be to record all significant risks and monitor the effectiveness of their treatment.

   Methods for identifying prospective risks include:

   - Brainstorming
   - Interviewing staff and clients to identify potential problems
   - Flow charting a process
   - Reviewing system design

2. Risk Analysis

   To access and evaluate the risks will determine which risks have a greater consequence. Evaluating the risks is about the possible impact of a risk, and the likelihood of it occurring. The business owner shall determine the level of risk that a business is willing to accept. Result from this process will lead to decisions whether risks are acceptable or need treatment, resources that required controlling the risks, and a prioritized list of risks that require further action. Risk analysis involves combining the possible consequences, or impacts, of an event, with the likelihood of that event occurring. The result is called a "level of risk". The risks are calculated from the combination of asset values expressing the likely impact resulting from a loss of confidentiality, integrity, and/or availability, and the assessed likelihood of related likelihood or related threats and vulnerabilities to come together and cause an incident.

   RISK = Impact x likelihood

   Determining the level of impact and the criteria for the organization. Depending on the damage that may be affecting which based on the results of the risk assessment of each risk factor.

   Evaluating the likelihood of a potential risk. Based on the analysis. The vulnerability of the system or property is also related to the analysis of the threat that is caused by the vulnerability.

3. Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. When the opportunity value and the risk from the risk are calculated, then compare in the table to see the level of risk. Define opportunities for risk and the impact of risk. The criteria for determining the risk is the likelihood or chance of the risk.

Risk Map		Impact				
		Very Low	Low	Medium	High	Very high
Likelihood		1	2	3	4	5
Unlikely	1	1	1	2	2	3
Rare	2	1	2	2	3	3
Possible	3	2	2	3	4	4
Likely	4	2	3	4	4	5
Extremely Likely	5	3	3	4	5	5

Risk Assessment

Risk treatment involves selecting one or more options for modifying risks and implementing and the options has been selected based on the table below for required action and risk acceptable level of organization

Risk Level	Required Action
Very High	Risk cannot be accepted. Immediate action is needed to implement or improve controls on urgent basis.
High	Risk cannot be accepted. Action is needed to implement or improve controls within appropriate time.
Medium	Risk is in moderate level. Correction needs to be considered but with justification, it can be considered accepting the risk.
Low	Risk can be accepted. Unlikely to require specific or significant application resources.
Very Low	

1. Reduce

   By reducing the chance or frequency of the risk, reduce impact or damage or both. The risk is reduced. In addition to the level of acceptance, such as the training of employees to have knowledge of data security. Organize the operating manual. Make a backup if an emergency occurs.

2. Transfer

   Transfer of risk to other internal or external entities outside the organization is to reduce the chance of risk or the severity of the impact of the risk, such as insurance from insurance companies or the management of outsourced expertise.

3. Accept

   Acceptance of risk, when an organization reduces its risk, it recognizes the level acceptable to it. The chances are low. or the impact of the risk cause no damage.

4. Avoid

   The avoidance of risky activities by deciding not to continue in risky activities, it will have an impact on the organization's objectives, such as stopping operations or cancel the project.

Monitor and Review

Monitoring and auditing is part of the risk management plan. The organization determine the responsible person and timeframe for the implementation. Apply lessons from past events, analyze changes to improve internal context, and risk criteria including risks. The results of the audit and review, the organization shall also record and report results. It is determined that after the risk assessment plan and the risk management plan have been prepared. Follow up the risk management plan and report to ISMS-C at 3-month intervals.

End of document