ISO/IEC 17025:2017
RISK MANAGEMENT

By:

SIRIM STS Sdn Bhd
<table>
<thead>
<tr>
<th>TIME</th>
<th>ACTIVITIES</th>
<th>Risk Management Process:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- (Exercise 2)</td>
</tr>
<tr>
<td>1015 – 1030</td>
<td>Break</td>
<td>Break</td>
</tr>
<tr>
<td>1030 - 1300</td>
<td>Risk Management Based on ISO 31000:2018 Principles and Framework</td>
<td>Risk Management Process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Risk Analysis and Evaluation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-(Exercise 3)</td>
</tr>
<tr>
<td>1300 – 1400</td>
<td>Lunch Break</td>
<td>Lunch Break</td>
</tr>
<tr>
<td></td>
<td>- Establish context</td>
<td>- Risk Treatment</td>
</tr>
<tr>
<td></td>
<td>- Exercise 1</td>
<td>-(Exercise 4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Presentation</td>
</tr>
<tr>
<td>1530 – 1545</td>
<td>Break</td>
<td>Break</td>
</tr>
<tr>
<td>1545 – 1700</td>
<td>Presentation</td>
<td>Procedure Risk Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Risk management procedure</td>
</tr>
</tbody>
</table>
COURSE OBJECTIVE

• to explain on risk-based thinking in ISO/IEC 17025
• to explain the risk management process
  - Establish context
  - Risk Identification
  - Risk Analysis and Evaluation
  - Risk Treatment
  - Monitoring and Review
What do we know about RM?

• RM is part of our every day lives:

  • Crossing the road – Risk of getting run-over
  • Managing our finances – Risk of going broke
  • Purchase of insurance – Risk of fire, theft, storm
  • Choosing to smoke – Risk of cancer
  • Going for a swim – Risk of drowning

• The choices we make in choosing to accept these risks is part of who we are
Understanding Risk Management
Risk is around us...

✔ Risk arises from uncertainties that can deviate our goals
✔ Risk are to be managed – “no risk, no gain”
3.1 Risk – Effect of uncertainty on objectives

Note 1 An effect is a deviation from expected – positive and / or negative, and can be address, result in opportunities and threats

Note 2 Objective can have difference aspects and categories (such as financial, health and safety, and environmental goal) and can apply at different levels (such as strategic, organization-wide, project, product and process)

Note 3 Risk is usually expressed in term of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7).

(Source ISO 31000)
DEFINITION OF RISK MANAGEMENT

• coordinated activities to direct and control an organization with regards to risk.
  (Adaptation From ISO 31000:2018 Risk Management - Principles And Guidelines)

• Risk Management Comprises a framework and process that enable an organization to manage uncertainty in a systemic, effective, efficient and systematic way from strategic, programme, project and operational perspectives, as well as supporting continual improvement
What is risk management?

Risk 1
Risk 2
Risk 3
Risk n

MANAGE
Policy, Resources, Communication, Risk Assessment, Reporting, Monitoring & Review

Reduce / Transfer/
Eliminate / Accept Risk

Achieve Objective
RISK ASSESSMENT PROCESS

Identify

Analyze

Evaluate

BUT there is no requirement for a formal risk management or a documented risk management process in ISO/IEC 17025:2017
A COHERENT SET STANDARDS

• ISO 31000:2018 “Risk management – Principles and guidelines”
• ISO Guide 73 “Risk management – Vocabulary”
• ISO/IEC 31010 “Risk management – Risk assessment techniques”
• HB 327:2010 – Communicating and consulting about risk
• AS/NZS 5050:2010 Business Continuity – Managing disruption-related risk
• HB 266:2010 – Guide for managing risk in not-for-profit organization
• ISO/IEC 27005 – ISMS – RISK MANAGEMENT
Risk Management is to reduce the uncertainties in order to

- Increase the likelihood of achieving the objectives
- Improve the identification of opportunities and threats, and
- Effectively allocate and use resources for risk treatment
Understanding Risk Management

Why Manage Risk

Compliance:

In compliance with ISO ISO/IEC 17025 :2017

Benefits:

- Minimize threat and maximize opportunity
- Reduce operational surprises and losses
- Resources are rationalized
- Less management time on fire fighting
Understanding Risk Management
Consequences of Improper Risk Management

In today's world, organisations cannot afford to be caught “off guard” by unexpected events that can cause:

- Physical Damage
- Loss of Reputation
- Potential Legal Suit
- Fatality & Major Injuries
- Operational Losses
- Non-compliance Costs
- Non Compliance To Regulatory Requirements
What is “Risk-Based Thinking”

- Risk-based thinking is something we all do automatically and often sub-consciously.
- The concept of risk has always been implicit in ISO 9001 – the 2015 revision makes it more explicit and builds it into the whole management system.
- Risk-based thinking is already part of the process approach.
- Risk-based thinking makes preventive action part of the routine.

- *Risk is often thought of only in the negative sense. Risk-based thinking can also help to identify opportunities. This can be considered to be the positive side of risk.*
Risk Management FOR ISO/IEC 17025:2017 Based On ISO 31000:2018
8.5 Action to address risk and opportunities (Option A)

8.5.1 The organization shall consider the risks and opportunities associated with the laboratories activities in order to:

a) Give assurance that management system can achieve its intended result
b) Enhance opportunities to achieve the purpose and objectives of the laboratory
c) Prevent/reduce undesirable effects and potential failures in the laboratory activities
d) Achieve improvements

8.5.2 The laboratory shall plan:
   a) Actions to address risks and opportunities;
   b) How to:
      1) Integrate & implement actions into its management system;
      2) Evaluate the effectiveness of these actions.

8.5.3 Actions taken to address risks and opportunities shall be proportionate to the potential impact on the validity of laboratory result.

Source: ISO/IEC 17025
### RISK IN ISO/IEC 17025:2017 CLAUSES

<table>
<thead>
<tr>
<th>Clause</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.4</td>
<td>The laboratory shall identify <strong>risks</strong> to its impartiality on an on-going basis. This shall include those risks that arise from its activities, or from its relationships, or from the relationships of its personnel. However, such relationships do not necessarily present a laboratory with a risk to impartiality.</td>
</tr>
<tr>
<td>4.1.5</td>
<td>If a <strong>risk</strong> to impartiality is identified, the laboratory shall be able to demonstrate how it eliminates or minimizes such risk.</td>
</tr>
<tr>
<td>7.8.6.1</td>
<td>When a statement of conformity to a specification or standard is provided, document the decision rule employed, taking into account the <strong>level of risk</strong> (such as false accept and false reject and statistical assumptions) associated with the decision rule employed and apply the decision rule.</td>
</tr>
<tr>
<td>7.10b</td>
<td>Take actions based upon the <strong>risk levels</strong> (including halting or repeating of work and withholding of reports, as necessary).</td>
</tr>
<tr>
<td>8.7 e</td>
<td>update risks and opportunities determined during planning, if necessary;</td>
</tr>
<tr>
<td>8.9.2a</td>
<td>changes in internal and external issues that are relevant to the laboratory</td>
</tr>
<tr>
<td>8.9.2m</td>
<td>results of risk identification;</td>
</tr>
</tbody>
</table>

Communication & Consultation (6.2)

- Establishing the context (6.3)

Risk Assessment (6.4)

- Risk Identification (6.4.2)
- Risk Analysis (6.4.3)
- Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Monitoring and review (6.6)

- 8.5.1, 8.5.2
- 8.5.3
- 8.9.2 & 8.7

Recording & Reporting (6.7)

Legend:
- ISO 31000 clause
- ISO/IEC 17025 clause
ISO 31000:2018 - STRUCTURE
RISK MANAGEMENT FRAMEWORK

• To ensure the organization in integrating risk management into significant activities and functions.
• The effectiveness of risk management will depend on its integration into governance of organization, including decision making.
• Required support from stakeholder- top management
INTEGRATION INTO ORGANIZATIONAL PROCESSES

• Risk management should be embedded in and not be separated from organizational practices and processes

• Especially policy development, strategic planning and change management

• Risk management plan to ensure:
  • Implementation of Risk Management policy
  • Risk Management is embedded in all practices and processes
EXAMPLE OF TECHNIQUE

- Hazard Identification, Risk Assessment and Determining Control (HIRADC)
- Hazard and Operability Study (HAZOP).
- Hazard Analysis Critical Control Points (HACCP)
- Aspect And Impact - ISO 14001
- Hazard Analysis - OHSAS 18001
- Fault Tree Analysis (FTA)
- Failure Mode and Effect Analysis (FMEA)
Risk Management Process

1. Understanding the organisation and its context

2. Understanding the needs and expectations of interested parties

3. 8.5 Action to address risk and opportunities
• Document used for recording risk management process for identified risks.

• The risk register will cover the significant risks facing the organization or project.

• It will record the results of the risk assessment related to the process, operation, location, business unit or project under consideration.
## RISK ASSESSMENT FORMAT

<table>
<thead>
<tr>
<th>Location:</th>
<th>Dept.</th>
<th>Prepared by:</th>
<th>Checked by:</th>
<th>Approved by:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Date:</td>
<td>Date:</td>
<td>Date:</td>
</tr>
<tr>
<td>Review Date:</td>
<td>1.</td>
<td>2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Process</th>
<th>Risks</th>
<th>Cause</th>
<th>Effect</th>
<th>Current Risk Control</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Risk Rating</th>
<th>Recommended Action /Additional Control</th>
<th>PIC (Due Date/Status)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Management Process
RISK MANAGEMENT PROCESS

Establishing the context (6.3)

Risk Assessment (6.4)

- Risk Identification (6.4.2)
- Risk Analysis (6.4.3)
- Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Recording & Reporting (6.7)

Communication & Consultation (6.2)

Monitoring and review (6.6)
Establish Context

Establish context means defining the **external and internal** parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.

Source: ISO 31000

4.1 Understanding the organization and its context
The organization shall determine external and internal issues that are relevant to its purpose and its **strategic direction** and that affect its ability to achieve intended result of its quality management system.

i. **Issues can include positive and negative** factors or conditions for consideration

ii. **Understanding the external context** can be facilitated by considering **issues arising** from legal, technological, competitive, market, cultural, social and economic environments, whether international, national, regional or local.

iii. **Understanding the internal context** can be facilitated by considering **issues** related to values, culture, knowledge and performance of the organization.

Source: MS ISO 9001:2015

4.2 Understanding the needs and expectations of interested parties
Due to their effect or potential effect on the organization’s ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, the organization shall determine:

i. The interested parties that are relevant to the quality management system.

ii. **The requirements of these interested parties** that are relevant to the quality management system.

The organization shall monitor and review information about these interested parties and their relevant requirements.

Source: MS ISO 9001:2015
Sources of Risks

**Internal**
- Resources
  - Inadequate internal controls, Human errors (incompetence, inexperienced, corruption)
  - IT failure
  - Inadequate human resources
- Processes
  - Operational Risks
  - Legal Risks

**External**
- Political risk
- Country Risk
- Market Risk
- Currency Risk
- Interest Rate Risk
- Counter-part Risk
- Credit or default Risk
- Environmental Risk
RELATION BETWEEN STRATEGY, OBJECTIVES AND RISK MANAGEMENT

SWOT Analysis

Strategies

Objectives

Identify Risks

Action / Mitigation Plan

Analysis
<table>
<thead>
<tr>
<th>NO.</th>
<th>STRATEGIC DIRECTION</th>
<th>CATEGORY OF ISSUES (INTERNAL / EXTERNAL)</th>
<th>STRATEGIC ISSUES</th>
<th>INTERESTED PARTIES INVOLVED</th>
<th>RISK</th>
<th>OPPORTUNITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>[KPI 2018]</td>
<td>P.E.S.T.E.L</td>
<td>[Issues impacted organization’s strategic direction]</td>
<td>[Issues may affect or potential affect requirements from interested parties]</td>
<td>[Specific Risk] (*Specific risk shall register in Risk Management Template; It can be Enterprise Risk Management or Operational Risk Management)</td>
<td>[Specific Opportunities]</td>
</tr>
</tbody>
</table>
| 1.  | Revenue and New Project launched (Project LINAS on testing of waste water analysis) | ECONOMIC       | Loosing potential no. of businesses for full commercialization due to obsolete testing method and not marketable. | 1. Material Testing Lab & Microbiological Lab  
2. Customer  
3. Rating Agency of Malaysia | Decreasing & fluctuating of revenue | Maximize Testing Scope and Competitive Pricing |
| 2.  | 1. Land Matters  
2. Timely & completion of Divisional Risks program (New Laboratory legislation requirements)  
3. OSHE Compliances | LEGAL          | 1. Non-compliance to applicable statutory bodies, government agencies, local authorities.  
2. Customer (External)  
3. External Provider  
4. Own Management committee  
5. Own group & subsidiaries | Potential penalty or Lawsuit. | 100% compliance to applicable statutory requirements. |
<table>
<thead>
<tr>
<th>Category</th>
<th>Issue</th>
<th>Interested Party</th>
<th>Risk</th>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal/Regulatory</td>
<td>New Standard for ISO17025:2017</td>
<td>SFM lab Top management Lab client Lab employee Standard Malaysia</td>
<td>Delay in accreditation</td>
<td>✓ Improve our management system ✓ Gain knowledge</td>
</tr>
<tr>
<td>Technology</td>
<td>SmartiLab</td>
<td>Staff Customer IT Department Chemist Supplier</td>
<td>Delay in registering and reporting the result</td>
<td>✓ More systematic ✓ Traceability</td>
</tr>
<tr>
<td></td>
<td>New equipment for Protein Distillation 8400 Analyzer</td>
<td>Chemist Supplier</td>
<td>High maintenance cost Chemist unfamiliar with the equipment</td>
<td>✓ Expose to up to date technology ✓ Save the working time ✓ Submit testing report to customer on time</td>
</tr>
<tr>
<td>Economic</td>
<td>Minimum wage</td>
<td>PCR officer Worker HR department Labor supply agency</td>
<td>Increase of minimum wage for cleaner</td>
<td>✓ Not shortage of manpower ✓ Satisfaction on routine work</td>
</tr>
</tbody>
</table>
1. External context includes all external environment parameters and factors that influence how an organization manages risk and tries to achieve its objectives. What are the examples of external context?

2. Internal context includes all internal environment parameters and factors that influence how an organization manages risk and tries to achieve its objectives. What are the examples of internal context?
4.2 Understanding the needs and expectations of interested parties (ISO 9001:2015)

- Customers
- Communities
- Suppliers
- Regulators
- NGOs
- Investors
- Employees

Needs and expectations (Requirements)

Relevant statutory & regulatory requirements

Monitor and review
4.2 Understanding the needs and expectations of interested parties (ISO 9001:2015)

<table>
<thead>
<tr>
<th>No</th>
<th>Interested Parties</th>
<th>Need and Expectations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Local government authority such as</td>
<td>Compliance to statutory and regulatory</td>
</tr>
<tr>
<td></td>
<td>• Ministry of Human resource : Department of occupation safety and health,</td>
<td>Employee welfares</td>
</tr>
<tr>
<td></td>
<td>Department of occupation safety and health, Human resource development fund</td>
<td>Conductive of safe work</td>
</tr>
<tr>
<td></td>
<td>• Feed Act 2009- Federal Government Gazette - Feed (Prohibited antibiotics,</td>
<td>No fine and penalty</td>
</tr>
<tr>
<td></td>
<td>hormones and other chemicals) Regulation 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ministry of health Food Act 1983 and Food regulations, Malaysia</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Product and system certification body and accreditation body  eg.</td>
<td>Assess conformity of te company against the</td>
</tr>
<tr>
<td></td>
<td>SIRIM, SGS (Thailand ), SGS (Malaysia), DOF, DVS SAMM  etc.</td>
<td></td>
</tr>
</tbody>
</table>
Risk Identification
RISK MANAGEMENT PROCESS

Establishing the context (6.3)

Risk Assessment (6.4)

Risk Identification (6.4.2)

Risk Analysis (6.4.3)

Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Recording & Reporting (6.7)

Monitoring and review (6.6)

Communication & Consultation (6.2)
TYPES OF RISKS (RISK CATEGORY)

Selection of risk category as input for risk identification parameter must consider established context that influence objective achievement !!!
### EXAMPLES OF RISKS

<table>
<thead>
<tr>
<th>Categories</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Politic</td>
<td>Risks associated with changes in national leadership, stability and change leadership</td>
</tr>
<tr>
<td>Legal</td>
<td>Risks related to national legislation, contracts, MOU, procedures and policies.</td>
</tr>
<tr>
<td>Operation</td>
<td>Risks associated with the work can not be completed on time.</td>
</tr>
<tr>
<td>Financial</td>
<td>Risk associated with financial management, transfers, fraud, etc</td>
</tr>
<tr>
<td>Manpower</td>
<td>Risks associated with the ability of the workforce, motivation to perform work, high labour turnover, skills shortages, high costs, injury.</td>
</tr>
</tbody>
</table>
# EXAMPLES OF RISKS

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Risks associated with the resulting information being inaccurate, incomplete, inappropriate, out dated.</td>
</tr>
<tr>
<td>Strategy</td>
<td>Risks associated with the strategy or policy failures or mistaken.</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>Risks related to failure to achieve the requirements of stakeholders.</td>
</tr>
<tr>
<td>Technology</td>
<td>Risks associated with technology infrastructure which is incompatible with the objectives of the business, integrity, relevance, data security and business continuity.</td>
</tr>
<tr>
<td>Organization</td>
<td>Risks associated with the organizational structure, accountability, responsibility, which will disturb communication to achieve business objectives.</td>
</tr>
</tbody>
</table>
Structure of Risk (Example)

To complete project on time

- Financial
  - Lack of funding
  - Liquidity
  - Loss Market
  - Fraud
  - Interest Rate

- Operation
  - Not complete on time
  - Lack of resources
  - Low quality
  - defect
  - High cost

- Political
  - Tax policy
  - Political stability
  - Employment law
  - tariff
  - Legal change

- Legal
  - Not flexible
  - Increase Tax
  - Not comply
Some common laboratory errors

- label error
- lost sample
- sample delayed in transit
- contaminated samples
- wrong test performed
- test performed inconsistent with the written procedure

- proficiency testing error
- no action on out of range controls
- false negative result
- late reports
- missing reports
- Complaints
- laboratory accident
- “near miss”
Common causes of error

- Equipment not properly maintained
- QC not performed
- Test kits not stored properly
- Individual responsibilities unclear
- No written procedures
- Written procedures not followed
- Training not done or not completed
- Transcription errors checks not done
- No written procedures
- Individual responsibilities unclear
- Equipment not properly maintained
- QC not performed
- Test kits not stored properly
- No written procedures
- Written procedures not followed
- Training not done or not completed
- Transcription errors checks not done
Process Risk Management
Risk Identification

Do you know your risk?

Describe the risk!

- Identify key process
- Identify objective of the key process
- What is the risk and how it affects the process?
- Who owns the risk?
- What are the root cause of the risk?
- What is the consequences of the risk?
Process Risk Management

Risk Identification

**CORE PROCESS OBJECTIVE**

Minimize equipment downtime and control maintenance costs

**RISK**

Poor equipment maintenance

**ROOT CAUSE**

Non compliance to equipment maintenance SOP

Incompetent people

**CONSEQUENCES**

Frequent equipment breakdown

Increase in equipment maintenance cost

**CORE PROCESS**

- Equipment Provision
- Equipment Disposal
- Equipment Operation
- Equipment maintenance
# Process Risk Management

## Risk Identification

### Examples of Process Risk

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>Equipment Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS OBJECTIVE</td>
<td>Minimize equipment downtime, increase operator / user / analyst satisfaction and control fleet maintenance costs</td>
</tr>
<tr>
<td>RISK</td>
<td>Poor Equipment Maintenance</td>
</tr>
</tbody>
</table>
| ROOT CAUSE | RC1 Non compliance to Equipment maintenance SOP  
 | RC 2 Incompetent people |
| CONSEQUENCES | C1 Frequent Equipment breakdown  
 | C2 Increase in Equipment maintenance costs |
Identify Process Function Requirements

- Identify a description of the process or operation being analyzed.
- Process function requirement describes the purpose of the process step / operation.
- Determine the purpose of each process step or process function. May have multiple requirements.
Describe Process Step/ Function/Objective/Requirements

- Enter a simple description of the process or operation being analyzed.
  - (e.g. Receiving purchasing item, Inspection, Storage, Specimen checking, Waste disposal, etc.)
- Determine the function of each process step
- Indicate as concisely as possible the purpose of the operation being analyzed.

“*You cannot identify a failure unless the process characteristic and its requirement have been identified*”
<table>
<thead>
<tr>
<th>Category</th>
<th>Activity</th>
<th>Specific Risk</th>
<th>Root Causes</th>
<th>Consequences</th>
<th>Existing Control</th>
<th>Likelihood &amp; Justification</th>
<th>Impact &amp; Justification</th>
<th>Risk Rating</th>
<th>Additional Control</th>
<th>Control Owner/ Due Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ Enter the risk category]</td>
<td>[Determine activity in the core process address the risk &amp; opportunities]</td>
<td>[Type of risk]</td>
<td>[Detection of risk trigger in core processes]</td>
<td>[Effect of risk occurred]</td>
<td>[Determine action already implemented to control the risk]</td>
<td>[Level of probability risk occur &amp; provide justification]</td>
<td>*Refer to Risk Appetite</td>
<td>[Level of Risk] *Refer to Risk Appetite</td>
<td>[To list down additional key control require to control the risk for improvement] * If needed</td>
<td>i.e – In Progress / Completed</td>
<td></td>
</tr>
</tbody>
</table>

**Describe the manner in which the process could potentially fail to meet the intended process function (s) /requirement (s) described in the previous column. What could possibly go wrong?**
<table>
<thead>
<tr>
<th>Category</th>
<th>Activity</th>
<th>Specific Risk</th>
<th>Root Causes</th>
<th>Consequences</th>
<th>Existing Control</th>
<th>Likelihood &amp; Justification</th>
<th>Impact &amp; Justification</th>
<th>Risk Rating</th>
<th>Additional Control</th>
<th>Control Owner/ Due Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter the risk category]</td>
<td>1. 1. Determine activity in the core process address the risk &amp; opportunitie</td>
<td>Detection of risk trigger in core processes</td>
<td>Effect of risk occurred</td>
<td>[Determine action already implemented to control the risk]</td>
<td></td>
<td>Level of probability risk occur &amp; provide justification</td>
<td>Level of consequences risk occurred &amp; provide justification</td>
<td>Level of Risk</td>
<td></td>
<td></td>
<td>i.e – In Progress / Completed</td>
</tr>
<tr>
<td>Operation</td>
<td>Confidentiality of information</td>
<td>Leak of customer information</td>
<td>Unauthorized release of confidential information</td>
<td>Complain to customer</td>
<td>Policy Statement on Confidentiality</td>
<td>Notification to the customer on the information released</td>
<td></td>
<td></td>
<td>Technical Manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Root Cause Of risk**
Defined as how the risk could occur, described in terms of something that can be corrected and controlled.
**Risk Identification**

<table>
<thead>
<tr>
<th>Category</th>
<th>Activity</th>
<th>Specific Risk</th>
<th>Root Causes</th>
<th>Consequences</th>
<th>Existing Control</th>
<th>Likelihood &amp; Justification</th>
<th>Impact &amp; Justification</th>
<th>Risk Rating</th>
<th>Additional Control</th>
<th>Control Owner/ Due Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ Enter the risk category]</td>
<td>1. [Determine activity in the core process address the risk &amp; opportunities]</td>
<td>[Type of risk]</td>
<td>[Detection of risk trigger in core processes]</td>
<td>[Effect of risk occurred]</td>
<td>[Determine action already implemented to control the risk]</td>
<td>[Level of probability risk occur &amp; provide justification]</td>
<td>[Level of consequences risk occurred &amp; provide justification]</td>
<td>[To list down additional key control require to control the risk/for improvement]</td>
<td>[Responsible person to conduct monitoring and evaluate the effectiveness of these actions &amp; Date to review]</td>
<td>i.e – In Progress / Completed</td>
<td></td>
</tr>
</tbody>
</table>

**Operation**

| Confidentiality of information | Leak of customer information | Unauthorized release of confidential information | Complaint by customer | Policy Statement on Quality, Confidentiality and Impartiality | Notification to the customer | Technical |

**Effect of risk**

Identify potential effects/impact of the risk as perceived by customers. Should be described as what customer might notice or experience.
Effect(s) of risk

- Brainstorming the “effect of risk” - How does the risk effect the customer.
- Describe the effects of the risk in terms of what the customer might notice or experience.
- State clearly if the risk could impact safety or cause noncompliance to regulations.
- Customer may be external and internal.
Group Exercise  Risk Identification

Know Your Process Risk?

1. Identify Key Process Name, Process Objective & Process Owner

2. Identify risk/root cause & consequences based on your respective key processes

3. Complete the form given for this activity.

Do not complete Existing Controls & Control Type & Risk Rating section as this will addressed in Risk Analysis & Evaluation session
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Review of request, tenders, and contracts</td>
<td>Incomplete information on analytical form</td>
<td>Lack of cooperatio from Customer</td>
<td>Wrong test performed, Waste of resource</td>
</tr>
<tr>
<td></td>
<td>Current Risk Control</td>
<td>Likelihood</td>
<td>Severity</td>
<td>Risk Rating</td>
</tr>
</tbody>
</table>
Risk Analysis & Risk Evaluation
RISK MANAGEMENT PROCESS

Establishing the context (6.3)

Risk Assessment (6.4)

Risk Identification (6.4.2)

Risk Analysis (6.4.3)

Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Recording & Reporting (6.7)

Communication & Consultation (6.2)

Monitoring and review (6.6)
Process Risk Management
Risk Analysis & Evaluation

Process to determine

EXISTING CONTROLS TO MITIGATE RISK

LIKELIHOOD OF THE RISK
- Evaluation regarding the chances of risk happening

IMPACT OF THE RISK
- Outcome of the risk (Consequences)
- Financial or Non financial

RISK RATING
- Level or position of risk
### Categories of control

<table>
<thead>
<tr>
<th>Type of Control</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| **Preventive**  | These controls are designed to limit the possibility of an undesirable outcome being realised | • Elimination or removal of the source of the hazard  
• Substitution of the hazard with something less risky |
| **Corrective**  | These controls are designed to limit the scope for loss and reduce undesirable outcomes that have been realized | • Exposure reduction by job rotation or limitation on hours worked  
• Post implementation review |
| **Detective**   | These controls are designed to identify occasions of undesirable outcomes having been realized (or example Audit, Inspection & Testing) | • Medical check up (inspection) to seek early symptoms |
Current risk control

Safety: PPE, emergency stop button, relief valve, sop
Financial: 3rd party financial audit, deposit, Level of authority
Operational: SOP, Quality control inspection
Legal: Contract

But most important, the current risk control must be effective, otherwise it is considered none
RISK ANALYSIS METHODOLOGY

1) Using qualitative or quantitative methods
2) Developing the likelihood scale (e.g: 1-low (Impossible), 5-high (Almost Certain))
3) Developing risk consequences scale (e.g: 1-low (Negligible), 5-high (Critical))
4) Develop risk assessment format (template)
# RISK ASSESSMENT FORMAT

<table>
<thead>
<tr>
<th>Location:</th>
<th>Dept.</th>
<th>Prepared by:</th>
<th>Checked by:</th>
<th>Approved by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>Date:</td>
<td>Date:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review Date:</td>
<td>1.</td>
<td>2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk category</td>
<td>Process</td>
<td>Risks</td>
<td>Cause</td>
<td>Effect/consequences</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


**Process Risk Management**
**Risk Analysis - Likelihood (Assessing Probabilities)**

- For actual or recurring events, we use the quantitative method to calculate the probability of risk happening.
- For potential event, we use the qualitative method to determine the probability of risk happening based on expert opinion or experience in other companies.

<table>
<thead>
<tr>
<th>Level</th>
<th>Level Of Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rare</td>
<td>The event may occur only in exceptional circumstances – e.g. once in every 3 years or chances of probability is 10% and below</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>The event could occur at some time – e.g. once in every 2 years or chances of probability is above 10% to 25%</td>
</tr>
<tr>
<td>3</td>
<td>Possible</td>
<td>The event might occur at some time – e.g. once in every 1 year or chances of probability is more than 25% to 50%</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>The event will probably occur in most circumstances – e.g. once in 6 months or chances of probability is beyond 50% to 75%</td>
</tr>
<tr>
<td>5</td>
<td>Almost Certain</td>
<td>The event is expected to occur in most circumstances – e.g. on a monthly basis or chances of probability is above 75%</td>
</tr>
</tbody>
</table>
### Process Risk Management

Risk Analysis – Example of likelihood measurement

<table>
<thead>
<tr>
<th>Example of Risk</th>
<th>Likelihood measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fall from height (Accident)</td>
<td>Occurrence of incidents involving fall from height</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jan</th>
<th>Feb</th>
<th>Mac</th>
<th>April</th>
<th>Mei</th>
<th>Jun</th>
<th>Julai</th>
<th>Ogos</th>
<th>Sept</th>
<th>Okt</th>
<th>Nov</th>
<th>Dis</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>2</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>4</td>
</tr>
</tbody>
</table>

The statistics indicate that incidents took place in 3 months (March, April and December). Therefore, risk likelihood is **Unlikely** (3 months/12 months x 100 = 25%)

**UNLIKELY**: The event could occur at some time – e.g. once in every 2 years or chances of probability is above 10% to 25%
Process Risk Management
Risk Analysis – Example of financial impact measurement

Variance against targets / budget on financial indicators, e.g. EBITDA, PATAMI, OPEX or REVENUE

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>LEVEL OF IMPACT</th>
<th>MEASUREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>INSIGNIFICANT</td>
<td>&lt; 2% variance *</td>
</tr>
<tr>
<td>2</td>
<td>MINOR</td>
<td>&lt; 3% variance *</td>
</tr>
<tr>
<td>3</td>
<td>MODERATE</td>
<td>&lt; 4% variance *</td>
</tr>
<tr>
<td>4</td>
<td>MAJOR</td>
<td>&lt; 5% variance *</td>
</tr>
<tr>
<td>5</td>
<td>CATASTROPHIC</td>
<td>&gt; 5% variance *</td>
</tr>
<tr>
<td>LEVEL</td>
<td>DESCRIPTOR</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>Service disruption involving state level or emergency services below 1 hour</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>Service disruption involving state level or emergency services between 1 - 3 hours</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Service disruption involving state level or emergency services between 3-6 hours</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Service disruption involving state level or emergency services exceeding 6 hours</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Nationwide Service Disruption</td>
</tr>
</tbody>
</table>

- Each key risk owner may suggest the appropriate impact measurement based on the type of risk
<table>
<thead>
<tr>
<th>Risk Identification</th>
<th>Risk Analysis &amp; Evaluation</th>
<th>Risk Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity</strong></td>
<td><strong>Specific Risk</strong></td>
<td><strong>Root Causes</strong></td>
</tr>
<tr>
<td>1. [Determine activity in the core process address the risk &amp; opportunities]</td>
<td>[Type of risk]</td>
<td>[Detection of risk trigger in core processes]</td>
</tr>
<tr>
<td>Confidentiality of information</td>
<td>Leak of customer information</td>
<td>Unauthorized release of confidential information</td>
</tr>
</tbody>
</table>

Current Control (Prevention, Detection) Descriptions of the controls that either prevent the cause of risk from occurring or detect the risk if it occur.
<table>
<thead>
<tr>
<th>Risk Identification</th>
<th>Risk Analysis &amp; Evaluation</th>
<th>Risk Treatment</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>Specific Risk</td>
<td>Root Causes</td>
<td>Consequences</td>
</tr>
<tr>
<td>1. [Determine activity in the core process address the risk &amp; opportunities]</td>
<td>[Type of risk]</td>
<td>[Detection of risk trigger in core processes]</td>
<td>[Effect of risk occurred]</td>
</tr>
<tr>
<td>Confidentiality of information</td>
<td>Leak of customer information</td>
<td>Unauthorized release of confidential information</td>
<td>Complaint by customer</td>
</tr>
</tbody>
</table>

Likelihood
Likelihood of specific cause of risk will occur.
### Risk Identification

<table>
<thead>
<tr>
<th>Activity</th>
<th>Specific Risk</th>
<th>Root Causes</th>
<th>Consequences</th>
<th>Existing Control</th>
<th>Likelihood &amp; Justification</th>
<th>Impact &amp; Justification</th>
<th>Risk Rating</th>
<th>Additional Control</th>
<th>Control Owner/ Due Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. [Determine activity in the core process address the risk &amp; opportunities]</td>
<td>[Type of risk]</td>
<td>[Detection of risk trigger in core processes]</td>
<td>[Effect of risk occurred]</td>
<td>[Determine action already implemented to control the risk]</td>
<td>[Level of probability risk occur &amp; provide justification]</td>
<td>[Level of consequences risk occurred &amp; provide justification]</td>
<td>[Level of Risk]</td>
<td>[Level of Risk]</td>
<td>[To list down additional key control require to control the risk/for improvement]</td>
<td>[Responsible person to conduct monitoring and evaluate the effectiveness of these actions &amp; Date to review]</td>
</tr>
</tbody>
</table>

### Risk Analysis & Evaluation

- **Impact Rank associated with the most serious effect for a given risk mode.**
Process Risk Management
Risk Analysis – Determining Impact

1. Road Accident

Example of Risk

Impact

The effects of the risk injury or death (Non-financial)
Cases that occurred did not cause death, only serious injury. Thus, the impact is MAJOR

MAJOR - Extensive bodily injuries/
permanent disability
Analyse risk based on the risk that was identified during previous group exercise
What is Risk Appetite?

- **Amount and type of risk** that an organisation is prepared to seek, accept and tolerate.
  
  
  (Source: British Standard 31100)

- **Amount and type of risk** that an organisation is willing to pursue or retain.
  
  (Source: ISO 31000 (Guide 73))

**Risk Tolerance (Limit)**

- Organization’s or stakeholder’s **readiness to bear the risk** after risk treatment in order to achieve its objectives.
  
  (Source: ISO 31000 (Guide 73))

- **The maximum amount of risk** that the company can bear despite controls.

  (Source: European Confederation on Institutes of Internal auditing ECIIA and Federation of European Risk Management Associations FERMA)
RISK MANAGEMENT PROCESS

Communication & Consultation (6.2)

- Establishing the context (6.3)

Risk Assessment (6.4)

- Risk Identification (6.4.2)
- Risk Analysis (6.4.3)

Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Recording & Reporting (6.7)

Monitoring and review (6.6)
Process Risk Management
Risk Analysis– Coming with a risk rating

Once the likelihood and impact of the risk have been established, we can then combine them to determine the level of risk. In arriving at this level, the risk rating matrix is used.

<table>
<thead>
<tr>
<th>Level Of Likelihood</th>
<th>Level Of Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Insignificant</td>
</tr>
<tr>
<td>Almost Certain</td>
<td>Significant</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
</tr>
</tbody>
</table>

Risk rating is calculated using the following formula

\[
\text{Risk Rating} = \text{Likelihood} \times \text{Impact}
\]

Example:

[Diagram showing a risk rating matrix with an example calculation]
## RISK ACTION PLAN TABLE

<table>
<thead>
<tr>
<th>RISK LEVEL</th>
<th>ACTION AND TIMESCALE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCEPTABLE 1-4</td>
<td>No additional controls are required. Consideration may be given to a more cost effective solution or improvement that imposes no additional cost burden. Monitoring is required to ensure that the controls are maintained.</td>
</tr>
</tbody>
</table>
| MODERATE 5-12  | Efforts should be made to reduce the risk, but the costs or prevention should be carefully measured and limited. Risk reduction measures should be implemented within a defined time period.  
Where the moderate risk is associated with extremely harmful consequences, further assessment may be necessary to establish more precisely the likelihood of harm as a basis for determining the need for improved control measures. |
| UNACCEPTABLE 15-25 | Work should not be started or continued until the risk has been reduced.  
If it is possible to reduce risk even with unlimited resources, work has to remain prohibited |
Risk Treatment
RISK MANAGEMENT PROCESS

Establishing the context (6.3)

Risk Assessment (6.4)

Risk Identification (6.4.2)

Risk Analysis (6.4.3)

Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Recording & Reporting (6.7)

Monitoring and review (6.6)

Communication & Consultation (6.2)
ULTIMATELY, WE NEED TO DECIDE WHETHER…
# RISK TREATMENT

<table>
<thead>
<tr>
<th><strong>AVOID</strong></th>
<th><strong>REDUCE</strong></th>
<th><strong>TRANSFER</strong></th>
<th><strong>ACCEPT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>not taking</strong> or continuing the activities</td>
<td>• Likelihood and Impact by training, testing, control, improve the management system.</td>
<td>• Involves another party to share in whole or in part through contracts, insurance, MOU.</td>
<td>• Identified risks can not be eliminated or avoided or no treatment process that can be done.</td>
</tr>
</tbody>
</table>
• When the **likelihood of a risk is low** but the **consequences is high**, the organization will wish to **transfer** that risk.

• When a risk is **both of high** likelihood and **high consequences**, the organization will wish to **avoid or eliminate** the risk.
ACCEPT AND REDUCE THE RISK

• When the risk is considered to be within the risk appetite of the organization, the organization will accept that risk.

• When the level of risk exposure (likelihood) is high but the potential loss (impact) associated with it is low, the organization will wish to treat to reduce the risk.
Communication, Monitoring & Review
RISK MANAGEMENT PROCESS

Establishing the context (6.3)

Risk Assessment (6.4)

Risk Identification (6.4.2)

Risk Analysis (6.4.3)

Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Recording & Reporting (6.7)

Communication & Consultation (6.2)

Monitoring and review (6.6)
DEVELOPMENT OF RISK MANAGEMENT CULTURE

CULTURE
• Risk is the way of work done

MANAGE
• Include risk in all planning

TRAINING
• Train employee to see risk during conducting their job
## COMMUNICATION AND REPORTING

<table>
<thead>
<tr>
<th>RISK LEVEL</th>
<th>COMMUNICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>• Notify to top management</td>
</tr>
<tr>
<td></td>
<td>• Immediate action to be taken</td>
</tr>
<tr>
<td>High</td>
<td>• Notify to top management</td>
</tr>
<tr>
<td></td>
<td>• Refer to strategic planner</td>
</tr>
<tr>
<td>Medium</td>
<td>• Action to be taken without notifying to top management</td>
</tr>
<tr>
<td>Low</td>
<td>• Accept risk but need monitoring</td>
</tr>
</tbody>
</table>
RISK MANAGEMENT PROCESS

- Establishing the context (6.3)
- Risk Assessment (6.4)
  - Risk Identification (6.4.2)
  - Risk Analysis (6.4.3)
  - Risk Evaluation (6.4.4)
- Risk Treatment (6.5)
- Recording & Reporting (6.7)

Communication & Consultation (6.2)

Monitoring and review (6.6)
Always monitoring and conduct strategy evaluation as the context or risk may change or other factors that might arise such as:

1) New risks
2) Existing risk assessment result might be change
3) The risk may be lost
4) Treatment may not be effective
# MONITORING & REVIEW

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>Monitoring conducted at planned interval, audit and review has been conducted to measure the effectiveness of the system.</td>
</tr>
<tr>
<td>Good</td>
<td>Monitoring conducted. Action has been taken</td>
</tr>
<tr>
<td>Moderate</td>
<td>Monitoring conducted but no action taken</td>
</tr>
<tr>
<td>Weak</td>
<td>No monitoring been done</td>
</tr>
</tbody>
</table>
AUDIT

• See the involvement of management
• See the methodology used
• See the members of the group involved
• See what kind of risks are taken into account
• See how the marks given
• View the data used
• See Actions treatment
• See follow-up actions
EFFECTIVE RISK MANAGEMENT

• Maintain global perspective
• Initiate open communication
• Integration of Risk Management in daily operation
• Continual improvement in risk management
• Team cooperation
• To avoid loss business / profit / company image
Establishing the context (6.3)

Risk Assessment (6.4)

Risk Identification (6.4.2)

Risk Analysis (6.4.3)

Risk Evaluation (6.4.4)

Risk Treatment (6.5)

Recording & Reporting (6.7)

Monitoring and review (6.6)

Communication & Consultation (6.2)

RISK MANAGEMENT PROCESS
Thank you

sarimah@sirim.my
Tel 03-55446237
H/P :012-2348594