Understand Risk to Improve Management System

PRESENTED BY,
FATEMA TUZ ZOHRA
MANAMA, BAHRAIN
MANAGEMENT SYSTEMS CONSULTANT
Reading Material

ISO 31001:2018 – Risk Management Guidelines
ISO 9001:2015 – Quality Management Systems
Benefits of Risk Management

- Improve Governance and Internal Control
- Respect Laws and Regulation
- Reducing Losses
- Improve over all Management
- Better Finance Performance
- Enhance Reputation
Use of Risk Management

- Long-Term
  - Strategy Development
- Planning of Projects
- Operation

- Short-Term
Who Needs Risk Management?

User Group

Corporate Level: Policy, program, framework

Operation Level: Project, activity, sectors

Audit: Audit, evaluation and reporting

Writers: Guides, procedures, practices

Individual Users

Risk Manager: Implement RM in the organization

Manager: Any decision-maker

Operation Staff: People managing risk in specific area or sector

Auditors: Providing assurance and verification of practices

Developers: People developing procedure
COMMUNICATE & CONSULT

ESTABLISH CONTEXT
- e.g. Internal & external factors/
  Risk Appetite

IDENTIFY RISKS

ANALYSIS RISKS
- Likelihood & impact
  existing controls

EVALUATE RISKS
- prioritise - risk profile

TREAT RISK
- e.g. establish controls

WORKSHOPS

SURVEY/INTERVIEW

WORKSHOPS

CONSULT WITH RISK OWNERS

MONITOR & REVIEW

Picture Credit: https://www.westernsydney.edu.au/ara/audit_and_risk_assessment
Risk
The effect of uncertainty

**Negative Impact**
- Property damage, destruction
- Loss of revenue, loss of money
- Health damage, injury, death
- Liability

**Positive Impact**
- New and safe construction
- Profit, return on investment
- Quality of life, employment
- Opportunities

Picture Credit: www.news.com.au
Risk Owner

Person or entity with the accountability and authority to manage a risk.

**Accountability** = **Authority** + **Resources** (e.g. human, technology, information, finance, partner, etc.) + **Competence** (training)

[Picture Credit: http://www.differencebetween.info/difference-between-authority-and-power]
Risk Assessment Process

Risk identification = process of finding, recognizing & describing risk.

Risk analysis = process to comprehend the nature of risk and to determine the level of risk.

Risk evaluation = process of comparing the results of risk analysis with the risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
Risk Identification

Identification:
Use experience, lessons-learnt, brainstorming, Subject Matter Expertise to identify – Source, Event, Consequences

Dependency:
Consider if risks are inter-related

Examples:
Small Oven 2
Medium Product Line 3
Large Department B
Disaster CEO = (ultimate risk owner)
Risk Source

Element which alone or in combination has the intrinsic potential to give rise to risk.

**TANGIBLE RISK SOURCE:**

- Natural events (e.g. earthquake),
- Stock market crash,
- Rising raw material and energy costs,
- Significant changes in regulation,
- Demographic changes

**INTANGIBLE RISK SOURCE:**

- Organizational culture,
- Culture within a country,
- Cyberattacks,
- Reputational harm,
- Patent infringement,
- Misuse or theft of intellectual property,
- Data stored cloud
Event
Occurrence or change of a particular set of circumstances.

An event can be one or more occurrences, and can have several causes.

An event can consist of something not happening.

An event can sometimes be referred to as an “incident” or “accident”.

An event without consequences can also be referred to as a “near miss”, “incident”, “near hit”, or “close call”.
Risk Analysis

Process to comprehend the nature of risk and to determine the level of risk.

Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Risk analysis includes risk estimation.
Consequences

Outcome of an event that affects objectives.

An event can lead to a range of consequences.

A consequence can be certain or uncertain and can have positive or negative effects on objectives.

Consequences can be expressed qualitatively and quantitatively.

Initial consequences can escalate through knock-on effects.

Picture Credit:
https://www.iconfinder.com/icons/547130/consequence_effect_hit_impact_physics_result_icon
## Likelihood

Chance of something happening.

<table>
<thead>
<tr>
<th>Option A</th>
<th>Option B</th>
<th>Option C</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td></td>
<td>Almost Certain</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>Probable</td>
</tr>
<tr>
<td>3</td>
<td>Likely</td>
<td>Probable</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>Unlikely</td>
</tr>
<tr>
<td>1</td>
<td>Highly Unlikely</td>
<td>Remote</td>
</tr>
</tbody>
</table>
Level of Risk

Magnitude of a risk, expressed in terms of the combination of consequences and their likelihood.

Level of Risk = Likelihood X Consequences

Picture Credit: https://fractionalciso.com/cybersecurity-risk-assessment/
Risk Criteria

Terms of references against which the significance of a risk is evaluated.

Risk criteria are based on organizational objectives, and external and internal context.

Risk criteria can be derived from standards, laws, policies and other requirements.
## Risk Criteria & Level of Risk - Example

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Financial Consequences</th>
<th>Level of Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>&gt;$3mln</td>
<td>Very high</td>
</tr>
<tr>
<td>Certain</td>
<td>$1mln to $3mln</td>
<td>High</td>
</tr>
<tr>
<td>Likely</td>
<td>$250K to $1mln</td>
<td>Medium</td>
</tr>
<tr>
<td>Very unlikely</td>
<td>$250K to $1mln</td>
<td>Low</td>
</tr>
</tbody>
</table>
Risk Appetite

Organization’s approach to assess and eventually pursue, retain, take or turn away from risk.

Consideration Risk Appetite/Attitude of following organizations:
New technology start-up in Silicon Valley
Nuclear power plant
Organization which is owned by dynamic and innovative CEO
Organization in which government owns 90% of shares
Risk Evaluation

Process of comparing the result of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk evaluation assists in the decision about risk treatment
Risk Treatment

Process to modify risk

Risk treatment that deal with the negative consequences are sometimes referred to as

A. Risk mitigation
B. Risk elimination
C. Risk prevention
D. Risk reduction

Risk treatment can create new risks or modify existing risks.
Risk Treatment

Risk control/mitigation

Avoidance
  Removing the risk source

Loss prevention
  Reducing the likelihood

Loss protection/reduction
  Reducing the consequences

Contractual “transfer”
  Transfer of asset or an activity to third party

Tolerate
  Take the risk

Picture Credit: risk-engineering.org
Risk Treatment

Risk Financing

Sharing (not transfer)
- with insurance
- third party contract

Retention (retain the risk)
- generating funds to pay for the loss
Control

- Measures that modify risk
- Any process, policy, device, practice, or other actions which modify risks.
- May NOT always exert the intended or assumed modifying effect

Types of Controls:

A. Physical
B. Procedural
C. Managerial
Residual Risk A.K.A Retained Risk

Risk remaining after risk treatment

Residual risk can contain unidentified risk.

Picture Credit: acamstoday.org
Risk Management - Conclusion

Coordinated activities to direct and control an organization with regard to risk

The risk management process should be

A. An integral part of management
B. Embedded in the culture and practices
C. Tailored to the business processes of the organization

The process comprises following activities:
- Communication and consultation
- Establishing the context
- Risk assessment
- Risk treatment
- Monitoring and review
Contact Information

Fatema Tuz Zohra

Manama, Bahrain

Ph. No.# +973 3350 1828

Fatema.zohra89@gmail.com

LinkedIn: [Link](#)
QUESTIONS?

THANK YOU FOR BEING A WONDERFUL AUDIENCE!