RISK MANAGEMENT: A COMPLETE INTRODUCTION TO MANAGING ENTERPRISE RISK

Global pandemics such as the scale of Covid-19 or the Spanish Flu have an annual occurrence probability that varies between 0.27% and 1.9%. And while organizations with robust enterprise risk functions had identified pandemics as one of their risks, the low probability meant that few had put in place measures to mitigate against the potential occurrence.

Safe to say, we have all been schooled at the moment.

From cyberattacks to air crashes, third party compromise to regulatory changes, employee unrest to economic downturn, the business environment is rife with uncertainties. Having an approach to anticipate and limit the impact should such materialize is critical for any enterprise that wants to remain.

As an organization defines its strategic goals and objectives, a realistic look at threats to success can go a long way in enabling the enterprise to remain on track. Investing in a risk management approach is the mark of mature companies who are well aware that the path to their vision is not always straightforward.

Let's look at some of the key aspects define risk management.

What is risk?

The ISO 31000 standard for risk management guidelines defines a risk as:

The effect of uncertainty on objectives.

The outcome of the uncertainty can swing in either a positive or negative manner. If the risk is negative, then the uncertain outcome results in harm or loss for instance lost customers, regulatory penalties being imposed or reduced business revenue. On the other hand, if the risk is positive, the uncertain outcome can result in benefits if exploited e.g., regulation changes can be favorable in terms of new business opportunities.

Elements of risk

To fully express a risk, one has to consider the following elements:

- **Risk source.** An element which, alone or in combination, has the potential to give rise to risk. Examples here include weather conditions, government agencies, disgruntled employees, etc.
- **Risk event.** The potential occurrence or change of a particular set of circumstances. For example: a cyberattack, flooding of a data center, mass resignation, adverse regulation, etc.
- **Risk consequence.** The outcome of an event affecting objectives. For instance lost revenue, penalties from a regulator, disrupted operations, corrupted data, etc.
- **Risk likelihood.** The chance of something happening—for instance, low or high probability which can be objectively or subjectively computed.

Responding to risk

In order to effectively respond to risks, an approach is required. That's where risk management comes into play.

Defining risk management

ISO 31000 defines risk management as

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

ITIL® 4 outlines the purpose of the risk management practice is to ensure that the organization understands and effectively handles risk to guarantee ongoing sustainability and value co-creation.

Principles for effective risk management, as outlined in ISO 31000 include, ensuring that your risk management practice:

1. Creates and protects value.
2. Is made an integral part of all organizational processes.
3. Is made part of decision making.
4. Explicitly addresses uncertainty.
5. Is systematic, structured, and timely.
6. Is based on the best available information.
7. Is tailored.
8. Takes human and cultural factors into account.

9. Is transparent and inclusive.
10. Is dynamic, iterative, and responsive to change.
11. Facilitates continual improvement of the organization.

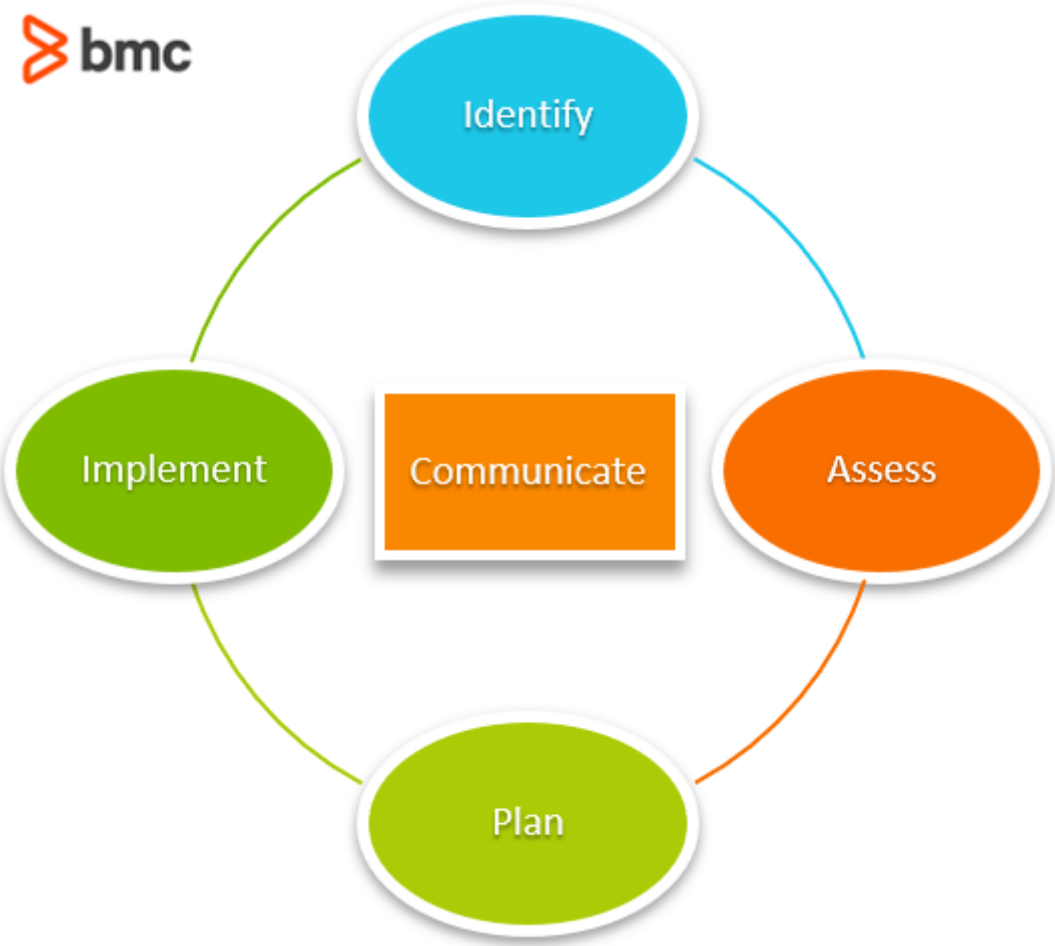
(Learn more about risk management in ITIL 4 & ITIL v3 environments.)

Risk management steps

Let's look at a couple well-known frameworks.

Management of Risk framework

At a high level, the risk management process can be broken down into five iterative steps as outlined by Axelos' Management of Risk (M_o_R) framework:



M_o_R Risk Management Process

1. Identify

The organization identifies its strategic and operational context, and then identifies the risks based on that context. The context leads to a determination of the organization's capacity and tolerance to risks should they materialize. Risks identified are documented in a risk log or register.

2. Assess

The risks identified are then assessed to determine the likelihood and consequence. This then leads to an evaluation of the assessment to rank the risks from a priority perspective, where risks with higher consequence and likelihood are prioritized higher. A risk heat map is a tool that can be used to visualize risk prioritization.

3. Plan

Planning involves identifying and evaluating the appropriate risk response to remove or reduce threats, and to maximize opportunities. Responses can be categorized as follows:

- **Avoid:** Making the uncertainty void by not proceeding with the plan of action where the risk would materialize. For example, not hosting your data on the cloud due to risk of transfer of personal data outside local jurisdiction.
- **Reduce:** Identify actions to reduce the probability and/or consequence should the risk materialize by putting in place mitigation controls. For example, putting policies to prevent senior officials from travelling on same flight or vehicle.
- **Transfer:** Identify a third-party who is willing to take up the risk on behalf of the organization. This option is usually tagged to insurance covers.
- **Share:** Identify a third-party who is willing to take up part of the risk with the organization. This option is usually applied to customers, partners or suppliers.
- **Accept:** Live with the uncertainty and take no action to forestall it.

4. Implement

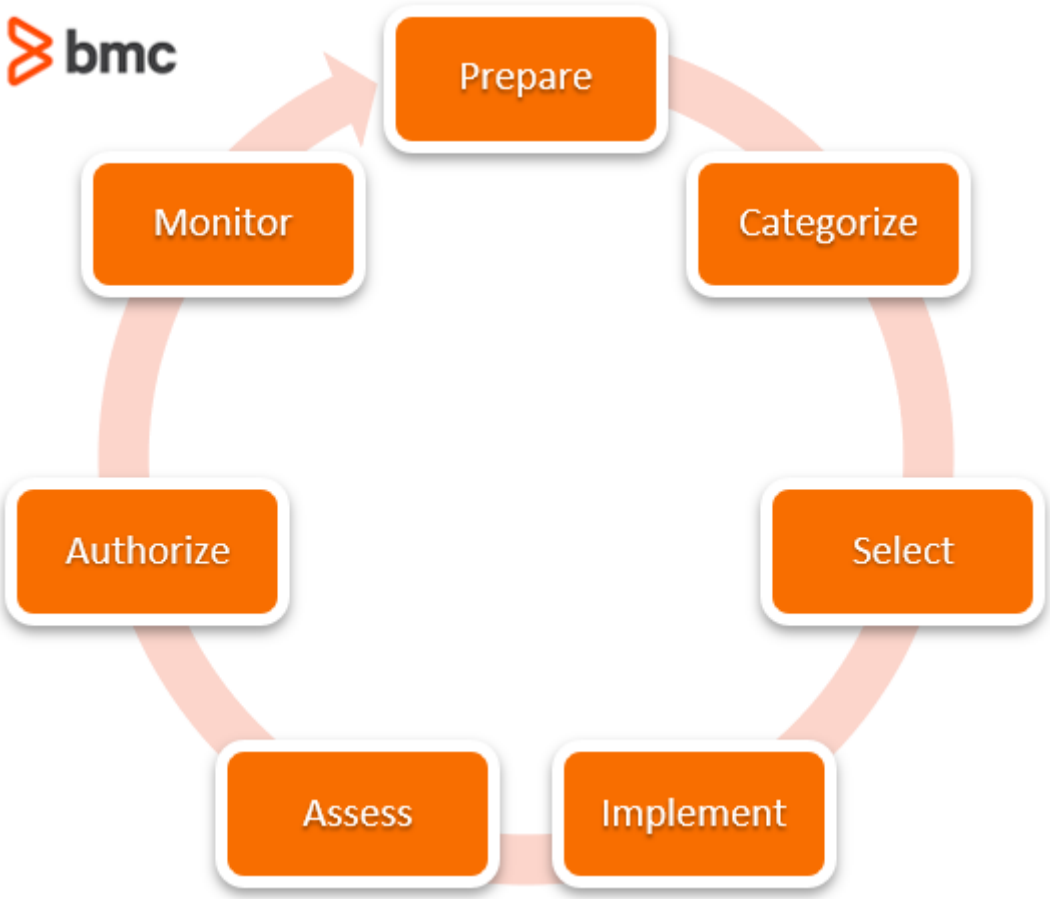
Here the planned risk responses will be actioned, their effectiveness monitored and corrective action taken where responses do not match expectations.

5. Communicate

This is a standalone step that occurs concurrent to the previous four. Risk information and treatment status is reported to key stakeholders based on agreed channels. This step is also very relevant whenever an identified risk materializes.

NIST risk management framework

The NIST risk management framework (RMF) provides a comprehensive, flexible, risk-based process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle through 7 steps outlined below:



NIST RMF Steps

1. **Prepare.** Carry out essential activities to help prepare all levels of the organization to manage its security and privacy risks.
2. **Categorize.** Determine the adverse impact with respect to the loss of confidentiality, integrity, and availability of systems and the information processed, stored, and transmitted by those systems.
3. **Select.** Select, tailor, and document the controls necessary to protect the system and organization commensurate with risk.
4. **Implement.** Implement the controls in the security and privacy plans for the system and organization.
5. **Assess.** Determine if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.
6. **Authorize.** Provide accountability by requiring a senior official to determine if the security and privacy risk based on the operation of a system or the use of common controls, is acceptable.
7. **Monitor.** Maintain ongoing situational awareness about the security and privacy posture of the system and organization to support risk management decisions.

Risk Management Roles

Now that we understand the purpose and steps in any risk management practices, let's look at the people involved. Key roles required for effective risk management in an organization include:

- **Risk Committee.** This is a subset of the organization's board whose mandate is the oversight and approval of the enterprise risk management framework. This includes defining risk

tolerance and appetite, providing resources for risk mitigation, setting governance policies, and evaluating performance of the implemented risk mitigation.
- **Risk Manager.** This role is responsible for coordinating the implementation of the enterprise risk management framework including guiding the rest of the organization in identifying, assessing, mitigating, and monitoring risks. The role will provide reports on the status of the risk management framework and can be elevated to Chief Risk Officer or Head of Risk depending on the size of the organization.
- **Risk Officer.** This role reports to the risk manager and carries out the basic risk management activities and maintains documentation on the same.
- **Risk Owner.** This role is responsible for the management, monitoring, and control of all aspects of a particular risk assigned to them, including the implementation of the selected responses to address the threats or to maximize the opportunities.
- **Risk Actionee.** This role is responsible for implementation of selected risk responses. It can be carried out by the Risk Owner or be outsourced to a third party.

Success factors in risk management

Success in risk management is a chance in itself—that's because you can never plan perfectly (unless you can see the future). However, having a robust yet flexible framework can be the difference between successfully navigating through a challenging risk or seeing your enterprise going under.

Key elements required in successful risk management according to the ITIL 4 practice guide include:

- Establishing governance of risk management
- Nurturing a risk management culture and identifying risks
- Analyzing and evaluating risks
- Treating, monitoring, and reviewing risks

Related reading

- BMC Service Management Blog
- What Is GRC? Governance, Risk, and Compliance Explained
- IT Security Vulnerability vs Threat vs Risk: What are the Differences?
- Risk Assessment vs Vulnerability Assessment: How To Use Both
- Error Budgets Explained: Risk & Reliability in One Metric
- Structured vs Unstructured Data: A Shift in Privacy