**Contents**

[Introduction 2](#_Toc71445244)

[Risk Management Plan Scope 2](#_Toc71445245)

[Research and summarization of compliance laws. 3](#_Toc71445246)

[Roles and Responsibilities of Individuals and Departments 4](#_Toc71445247)

[Proposed Schedule of Risk Management Planning Process 5](#_Toc71445248)

[References 7](#_Toc71445249)

# 

# **Introduction**

The risk management plan is a documented strategy that describes how to cope or deal with specific risks and what actions should be taken to manage the risks. A risk management plan is essential since it provides a guide to team project members to help them identify risks, analyse the risks, respond to the threats accordingly and control the risks. The risk management plan's purpose and goal are to identify all the potential problems before their occurrence and address how to deal with the issues.

# **Risk Management Plan Scope**

This involves identifying specific project risks, goals, tasks, features, and the general cost. It is essential to identify risks to successfully set and define objectives that help control or prevent financial or legal ramifications associated with risks. Examples of risks that a project can face include; the strategic risk of new competitors getting into the market; another risk is regulatory and compliance risk, which means introducing new legislation or new rules; financial risk is another risk faced while working on a project. The last risk is the operational risk. Once the risks are identified, the risks are analysed, and solutions are provided. The answers for our given risks include a strategic risk review, intensive regulation and compliance understanding, financial management of project expenditures, and operational risk controls.

As outlined, the objective of the risk management plan is to identify potential risks likely to occur, assess the outlined risks, and develop risk preventive measures or responses. A risk management plan can or should instead include the approach, milestone, deliverables, and budget boundaries. Defining the outlined boundaries provides smooth execution of the project.

# **Research and summarization of compliance laws.**

Regulatory compliance usually describes the organizations' goals to achieve in their endeavors to ensure they are fully aware of and the various steps taken to comply with the relevant laws, regulations, and policies. There are several compliance laws and rules about the organizations. They include; the Health Insurance Portability and Accountability Act that aims to protect employees' medical information security and privacy.

The next one is the Payment card Industry Data Security Standard. These are set standards regulations developed to ensure the credit card industry is securing and managing the customers' data adequately.

The SOC2 that is systems and organization control, is another compliance law that focuses on the security, confidentiality, privacy, integrity, and availability of customers' data in the cloud.

The SOX is another compliance law about organizations, which means the Sarbanes Oxley Act protects the investors by improving accuracy levels and reliability. The rules of SOX include protection of data, management of electronic records, internal control reports, and executive accountability.

International organization of standardization ISO is another compliance law that helps organizations and companies manage the security of their assets: their financial information, employees' data, and intellectual properties. Also, the ISO regulates the organization's standards to align the business's practices and solve any problem that may come up regarding processes or equipment.

The final compliance law and regulation about the organization is the General data protection regulation (GDPR) that follows the planning step to create plans of owning various key improvements and processes. The next step after planning is the gap analysis step that locates and accounts for any gap found. The next step after the gap analysis step is the remedy gap step; it prioritizes and ranks the key areas to be solved or fixed based on the level of risk. The last step involved in the test of new processes requires assessing the effectiveness of the new procedures put in place.

# **Roles and Responsibilities of Individuals and Departments**

Incorporating risk management roles and responsibilities within the existing job specification, working procedures and policies, committee chatters, and working teams are considered very effective compared to describing every role and responsibility in policy of risk management or framework according to (Sidorenko & Demidenko, 2016). Below are various roles and responsibilities for different individuals and departments.

**The board of directors- their role is to make decisions putting all the risks in mind, and overse**e overall management effectiveness.

CEO –In a risk management framework, there are several assigned roles to individuals about risk management. These roles include authorizing official and designated representative, chief information officer, familiar control provider, control assessor, head of the agency, information owner, risk executive, security architect, system administrator, information system owner, information system officers, and information system security engineer. Each of the roles mentioned above has its responsibilities in the risk management framework, which is the CEO's responsibility to establish and assign the responsibility of designing it. The CEO also makes a decision and allocates business necessary resources with all risks in mind.

**Risk managers and their departments** - from the report done by (Ward, 2001) the risk manager and their departments have the responsibility designing and establishing a combined strategy of risk management and statement policy, establishing and maintaining the strategy of risk management, give guidelines on risk management methods to business units, supervise the processes of risk management, coordinate data delivery and act as conduit for interchanging of the data on risks and their management.

**Other business unit heads** – at this level in the organisation, the involved individuals or working department are responsible for identifying, assessing, and treating risks within their business activities or decision-making. They also allocate resources essential for risk management. They work with the Human Resource group to include the awareness and competencies in risk management of ISO31000 to the new hires under different positions.

# **Proposed Schedule of Risk Management Planning Process**

Risk management planning process involves several elements, which include:-

|  |  |
| --- | --- |
| 1. Risk strategy | Provides the approach to risk management throughout the project. |
| 1. Methodology | It gives out the tools, information sources, and techniques that can be used to carry out risk management on the project. |
| 1. Roles and responsibilities | This gives the information and guidance about who will partake in a specific risk management activity. |
| 1. Timing | It gives the intervals when the risk management process will be performed and enables modification of the risks and inclusion of new threats. |
| 1. Funding | Risk management provides details on how much funding will be used to perform all project risk management activities. |
| 1. Risk categories | It involves all the sources of risks for the project. These risks may be technical, management, commercial or external risks. |
| 1. Stakeholders risk appetite | There are three levels at which the stakeholders are willing to take risks: appetite level, acceptable level, and threshold level. |
| 1. Probability and impact matrix | It is a definition that is used in the project to provide a standard grading among stakeholders. This element of the risk management plan gives a common understanding between high, medium, and low risks. |
| 1. Reporting formats | It gives the information on documentation, analysis, and implementation process of risk management of the project. |
| 1. Tracking | The tracking process involves auditing the risks and keeping records on the risk activities. |

# **References**

Sidorenko, A., & Demidenko, E. (2016). *Guide to effective risk management 3.0*: RISK-ACADEMY.

Ward, S. J. R. m. (2001). Exploring the role of the corporate risk manager. *3*(1), 7-25.