Table of Contents

1. **Purpose** 2
2. **Scope** 2
3. **Risk Management Systems** 2
4. **References** 2
5. **Terminology** 3
6. **Business Impact Analysis and Risk Assessment Instructions** 6
7. **Risk Assessment Matrix** 10
8. **Critical Business Functions** 10
9. **Risk Region Determination: Hazard Analysis** 13
10. **History of Change** 16

1. Purpose

The purpose of this Impact Risk Assessment is to support and complement the company risk management systems to evaluate, control, mitigate, communicate, and review any vulnerability and risk to improve business operations, based on a framework consistent with ICH Q9 and ISO 31000, Risk Management — Principles and Guidelines.

Establish a procedure to perform a risk analysis and mitigation activities related to the company business continuity plan to:

a) Identify and document all possible and potential vulnerabilities, failures, disasters, root causes and actions taken for each business operation, department or area.

b) Based on the potential vulnerabilities, assign the corresponding risks and evaluate how these risks should be minimized as much as possible to an acceptable level.

c) Establish the testing requirements with the associated documentation based on risk, complexity, and novelty as part of a scalable approach that enables to establish and standardize the selection of the appropriate life cycle testing or validation activities for a specific business operation.

d) Determine the corresponding testing environment for each business operation.

2. Scope

This procedure provides advanced instructions, guidance and steps to be followed by the business continuity management team to identify and evaluate the potential risks or failure of the company operations, process, the effect of the same, and the mitigation actions necessary to reduce or eliminate the possibility of occurring.

This plan can be used to assess an organization's ability to meet its own continuity needs and obligations in terms of the following risk management approach.

3. Risk Management Systems

The ICH Guideline ICH Q9 describes a systematic approach to quality risk management intended for general application within the regulated GxP industry. It defines the following two primary principles of quality risk management:

- The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the protection of the patient.
- The level of effort, formality, and documentation of the quality risk management process should be commensurate with the level of risk.

In the context of computerized systems, scientific knowledge is based upon the system specifications and the business process being supported.

Also, the ISO 31000 describes a systematic approach to perform an impact risk analysis that is considered as part of this procedure.

4. References

- ISO 31000, Risk Management — Principles and Guidelines
- ICH Q9 - Quality Risk Management

5. Terminology

Consequence

A consequence is the outcome of an event and affects objectives. A single event can generate a range of consequences that can have both positive and negative effects on objectives. Initial consequences can also escalate through cascading and cumulative effects.

Context

To establish the context means to define the external and internal parameters that organizations must consider when they manage risk. An organization's external context includes its external stakeholders, its local, national, and international environment, as well as any external factors that influence its objectives.

An organization's internal context includes its internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards.

Control

A control is any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk. Risk treatments become controls, or modify existing controls, once they are implemented.

Event

An event could be one occurrence, several occurrences, or even a nonoccurrence (when something doesn't actually happen that should have happened). It can also be a change in circumstances. Events always have causes and usually have consequences. Events without consequences are referred to as near-misses, near-hits, close-calls, or incidents.

External context

An organization's external context includes all of the external environmental parameters and factors that influence how it manages risk and how it tries to achieve its objectives. It includes its external stakeholders, its local, national, and international environment, as well as key drivers and important trends that influence its objectives. It also includes stakeholder values, perceptions, and relationships, as well as its social, cultural, political, legal, regulatory, technological, economic, natural, and competitive environment.

Internal context

An organization's internal context includes all of the internal environmental parameters and factors that influence how it manages risk and tries to achieve objectives. It includes its internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards. Governance includes the organization's structure, policies, objectives, roles, accountabilities, and decision making process, and capabilities include its knowledge and human, technological, capital, and systemic resources.

Level of risk

The level of risk is its magnitude. It is estimated by considering and combining consequences and likelihoods. A level of risk can be assigned to a single risk or to a combination of risks. Common level of risk categories include the following: extreme risk, high risk, moderate risk, and low risk. Of course, you need to define each category so that everyone is using the same terminology in the same way.

Likelihood

Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics).