qualityaustria central asia
Succeed with Quality

Risk Management Policy

RISK MANAGEMENT POLICY

1.0 Overview

QACAPL is committed to excellence and continual improvement, and will continue to encourage innovation whilst maintaining a low-risk profile. Employees are encouraged to adopt a positive approach to risk management, which further strengthens the risk-aware culture of the organization. Risk management is incorporated into the strategic and operational planning and quality processes at all levels within the organization in order to minimize the impact of risk.

2.0 Purpose

The purpose of Risk Management is to ensure effective decision-making that is guided by the organization, ensuring a consistent and effective approach to risk management, formalizing its commitment to the principles of risk management.

3.0 Scope

This policy shall apply to IT activities undertaken within QACAPL.

4.0 Objective

- To provide a common approach to managing IT procedure.
- To provide management with a consistent and repeatable risk analysis, enabling them to effectively manage IT risks.

5.0 Responsibilities

The Business Excellence Audit team shall be responsible for monitoring the IT risks and escalating any risks to the director Technical

All risk owners shall be responsible for the following:

- Maintaining and managing the vulnerabilities and deciding the level of risk that is acceptable.

All asset owners shall be responsible for the following:

- Maintaining the IT Asset sheet, and making changes if they believe it to be inaccurate.
- Monitoring the threats associated with their assets, determining whether their likelihood has changed as a result of corporate, market or legal changes.
- Ensuring that the IT risks associated with their assets are mitigated appropriately or accepted by the relevant risk owner.

6.0 Policy

- A systematic approach to IT risk management is necessary to identify business needs regarding IT requirements.
- IT risk management is a continual process.
- The implementation of the IT risk strategy shall be based on formal methods for risk assessment, risk management, and risk acceptance independent of technology or software.

6.1 Strategy

- An IT Policy shall be developed and maintained to provide management direction and support for IT in accordance with business requirements, relevant laws and regulations and the requirements of interested parties.
- The protection of IT assets and information processing facilities shall be:
    - Based on the security risks identified through a formal, business focused assessment process.
    - Cost effective and justified.
    - Selected by management such that risks are reduced to a level considered acceptable.

6.2 Performing Risk Assessment

QACAPL shall undertake a full risk assessment annually or as needed or as a result of:

- Significant Changes within the Business.
    - New or changed product or service
    - New or changed supplier relationship
    - New or changed resources or technologies.

- Business continuity events

6.3 IT Risks

The following process shall be followed to assess the IT risks:

6.3.1 Asset Identification

- All assets shall be identified that are within the scope of the assessment.
- For each asset group an asset owner shall be identified who shall have the individual responsible for the asset group.

6.3.2 Asset Business Impact Analysis

- The asset owner shall be responsible for valuing each asset group to determine the impact level of an IT breach.

6.3.3 Threat Identification

- QACAPL shall identify and list all the threats which may affect the assets identified.
- For each threat its likelihood shall be determined
- Selection of mitigating controls shall have weighted in terms of the threat impact on the basis of CIA

6.3.4 Vulnerability Identification

QACAPL shall identify specific vulnerabilities in relation to specific IT assets. Vulnerability shall be assessed on a scale of 1 to 3 taking considering of the controls in place:

- their existence & maturity
- the level of documentation supporting them
- their effectiveness
- the level of awareness of them

6.3.5 Risk Evaluation

IT Risk shall be assessed in two stages:

- **Absolute Risk**

  Absolute risk shall be based on the multiple of the Impact value & probability of occurrence assuming no mitigation control are in place. It is this risk level that shall be

considered during major incidents, when a part of a business continuity strategy, IT controls may no longer be in place.

- **Residual Risk**

  Residual risk shall be based on the multiple of the Impact value & probability of occurrence considering the mitigating controls are currently in place. These risks will be acceptable by the management and will have a risk owner assigned respectively.

6.4 Risk Ownership

Risk Owners shall be identified and responsible for determining the course of treatment to be taken to manage any identified risks to an acceptance level.

6.5 Risk Treatment

In determining how the identified risk can be managed, the following options shall be considered by QACAPL.

6.5.1 Modify the level of identified risk by:

Selecting one of the following options:

- Reducing the probability of risk arising
- Reducing the impact upon the assets affected

This can be achieved by

- Improving existing controls
- Introducing new controls

The level of IT risk shall be modified through the selection of controls so that the current risk score can be assessed as being acceptable.

6.5.2 Accept the level of identified risk

The decision on accepting or retaining information risk without further actions shall be taken depending on risk evaluation. If the level of risk meets the acceptance criteria, there shall be no need for implementing additional controls and the risk shall be accepted.

6.5.3 Risk Avoidance

When the identified IT risks are considered above the agreed threshold, or the cost of implementing the risk treatment option exceeds the benefits, a decision could be made to avoid or accept that risk by management.

6.5.4 Risk Transfer

Transferring the risk to third parties to prevent potential loss.

Approved by Rajeev Ral, Director (Technical).

17/10/2023

Next review - 16/10/2024