Issue and Risk Management Framework

Purpose and Objectives

Part of the required activities and documentation for the ISO/IEC 20000-1 certification is a risk management methodology, including risk acceptance criteria and an approach to managing risks. In fact, risk awareness and risk management are a core element of this standard as well as other management system standards.

The relationship and flow between a number of documents and processes, including the Issue Register, the Risk Register and the CSI Register, needs to be clarified and documented in order create an integrated Issue and Risk Management Framework. This document presents that framework and the practical way to deal with the various aspects of it.

**Please consider the environment before printing this document.**

Table of Contents

[1. Introduction 3](#_Toc505346922)

[2. Definitions 3](#_Toc505346923)

[3. Process Description 4](#_Toc505346924)

[3.1 Process Diagram 4](#_Toc505346925)

[3.2 Process Flow 4](#_Toc505346926)

[3.2.1 Issues to Risks and CSI Opportunities 4](#_Toc505346927)

[3.2.2 Operational Risks to Risk Assessment and Risk Controls 5](#_Toc505346928)

[3.2.3 Control of Processes Delivered by Other Parties 5](#_Toc505346929)

[3.2.4 Strengths 6](#_Toc505346930)

[4. Risk Management Methodology 6](#_Toc505346931)

[4.1 Scope 6](#_Toc505346932)

[4.2 Responsibilities 6](#_Toc505346933)

[4.3 Procedure 6](#_Toc505346934)

[5. Acronyms and Abbreviations 9](#_Toc505346935)

[6. References 9](#_Toc505346936)

[7. Revision Log 9](#_Toc505346937)

[8. Document Approval (if cross functional) 9](#_Toc505346938)

[9. Process/Document Owner Approval 9](#_Toc505346939)

# Introduction

For the effective management of issues and risks, there needs to be a logical flow between the existing Internal and External Issues list and the operational Risk and CSI Registers.

# Definitions

The following definitions have been taken from ISO 20000-1 and ISO 27000, if they existed in there. If not, a new definition has been made.

**issue**

a subject or problem that people are thinking and talking about:

*environmental/ethical/personal issues*

*As employers we need to be seen to be addressing (= dealing with) these issues sympathetically.*

*Don't worry about who will do it - that's just a side issue (= not the main problem).*

**risk**

effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

**risk management framework**

set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage risk.

NOTE 2 The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organisation's overall strategic and operational policies and practices.

# Process Description

## Process Flow

### Issues to Risks and CSI Opportunities

ISO 20000-1: “*The organisation shall determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended outcome(s) of its SMS.”*

Issues are collected in the Internal and External Issues Tracker. Issues in here are any items that are deemed important to the organisation, its quality and information security objectives as well as the overall effectiveness of its operations to provide services to the customers.

Examples of issues include staffing needs, new or changed processes, new or changed systems, facility needs, customer requirements, etc.

Issues have the potential to turn into either a risk or a Continual Service Improvement (CSI) opportunity. In those cases, issues listed in the tracker need to be transferred into either the Risk Register or into the [CSI Register](https://onejira.verizon.com/secure/RapidBoard.jspa?rapidView=47444&projectKey=ONVEM).

Examples of when this needs to happen are the following.

1. Personnel needs due to churn have been flagged in the issue tracker for a certain period of time while top management are not making visible progress in handling the additional pressure on remaining staff. The lack of staff is now impacting the operation of the organisation and there is a risk to the quality of the organisation’s deliverables. This issue should now be transferred to the Risk Register and discussed in the Risk Management meeting with top management.
2. A deficiency in an existing process has been listed in the issue tracker. This deficiency is now getting more apparent because new services are more dependent on the missing process step than legacy services. The process needs to be modified, which turns it into a CSI opportunity. The issue is transferred into the CSI Register for handling in the CSI process.

# Risk Management Methodology

## Scope

This risk management framework applies to all risks in [Organisation] and is intended to enable it to pursue and achieve the service management objectives set out in the service management policy.

## Responsibilities

The *[Function]* is responsible for ensuring that the Organisation’s risk management framework meets the requirements of any required legislative or regulatory requirements in terms of risk management.

## Procedure

Risks will be assessed on the basis that each risk item will be valued in terms of the importance of the item in the provisioning of services, and that its value will be the estimated total possible cost of loss that might be experienced if the risk materialises. This valuation will be carried out using an Impact Valuation Scale that has 5 levels: 1=Very Low, 2=Low, 3=Moderate, 4=High, and 5=Very High.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **Impact** | **Low end range ($)** | **High end range ($)** |  |  |  |  |  |  |  |
|  | 5 | 1.000.000 | --- |  |  |  |  |  |  |  |
|  | 4 | 100000 | 999.999 |  |  |  |  |  |  |  |
|  | 3 | 10000 | 99.999 |  |  |  |  |  |  |  |
|  | 2 | 1000 | 9.999 |  |  |  |  |  |  |  |
|  | 1 | 0 | 999 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| The **likelihood** of the impact or loss occurring will be estimated using a 5-Level scale: 1=Very Low, 2=Low, 3=Medium, 4=High, and 5=Very High. |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **Likelihood** | **Threat Exploit Likelihood** |  |  |  |  |  |  |  |
|  | 5 | > 100 times per year |  |  |  |  |  |  |  |
|  | 4 | Between 10 and 100 times per year |  |  |  |  |  |  |  |
|  | 3 | Between 1 and 10 times per year |  |  |  |  |  |  |  |
|  | 2 | Between .1 and 1 times per year |  |  |  |  |  |  |  |
|  | 1 | < .1 times per year (less than once every ten years |  |  |  |  |  |  |  |
| The Risk level will be calculated by multiplying Impact and likelihood, using a multi-level scale that takes account both extent of impact and frequency of occurrence. The risk levels are defined in a risk matrix as follows: |
|  |  |  |  |  |  |  |  |  |  |  |
| **Likelihood** | **5** | 5 | 10 | 15 | 20 | 25 |  |  | VH |  |
| **4** | 4 | 8 | 12 | 16 | 20 |  |  | H |  |
| **3** | 3 | 6 | 9 | 12 | 15 |  |  | M |  |
| **2** | 2 | 4 | 6 | 8 | 10 |  |  | L |  |
| **1** | 1 | 2 | 3 | 4 | 5 |  |  | VL |  |
|  |  | **1** | **2** | **3** | **4** | **5** |  |  |  |  |
|  |  | **Impact** |  |  |  |  |

## Risk Appetite and Risk Acceptance Criteria

Acceptable levels of risk are defined as those that are the same as, or below, the approved acceptable risk level. Acceptable Risk is defined as any risk that falls into level [6] in the risk

matrix calculated via the risk assessment tool by reference to the scales selected by management.

After completion of the risk assessment for any asset, the levels of identified risk are reviewed and compared to the risk acceptance criteria. All risks that are at or below the acceptable level are automatically accepted. Risks that are at a level higher than [6] may be transferred to a third party, such that the residual risk is at or below the accepted level, or must be reduced by implementation of appropriate controls to a level consistent with the risk acceptance criteria.

Where necessary, additional controls may be selected and implemented in order to reduce the residual risk level below the acceptable level. Wherever residual risk remains for any reason above the acceptable risk threshold, management approval must be provided for that level of exposure.

# Acronyms and Abbreviations

|  |  |
| --- | --- |
| CSI | Continual Service Improvement |
| ISO | International Standards Organisation |
| IEC | International Electrotechnical Commission |

# References

|  |
| --- |
| ISO/IEC 20000-1:2018ISO/IEC 27000:2018 |

# Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Amendments**  | **Updated By** |
| 17/7/2019 | 0.1 | Initial Draft |  |
|  |  |  |  |
|  |  |  |  |

# Document Approval (if cross functional)

|  |  |  |
| --- | --- | --- |
| **Date** | **Name of stakeholders** | **Function** |
|  |  |  |

# Process/Document Owner Approval

|  |  |  |
| --- | --- | --- |
| **Date** | **Name**  | **Function** |
|  |  |  |