Risk Management for Digital Service Providers

Guidebook

GB952

Version 1.4

October, 2012

Notice

Direct inquiries to the TM Forum office:

240 Headquarters Plaza,
East Tower – 10th Floor,
Morristown, NJ 07960 USA
Tel No. +1 973 944 5100
Fax No. +1 973 944 5110
TM Forum Web Page: www.tmforum.org

Table of Contents

List of Figures

Executive Summary

This Standard provides guidance to Digital Service Providers on the following areas:

1. Risk Management Guidebook
2. Risk Universe
3. Risk Portfolio

The Risk Management Guidebook presents guidance on how to implement a risk management Guidebook within a Digital Service Provider. The Risk Universe details the portfolio of risks that need to be managed by a Digital Service Provider. The Risk Portfolio details the risks from various stakeholder perspectives.

1. Definitions

This terminology used in this document is consistent with ISO Guide 73 – Risk Management Vocabulary. The exception is that the word “framework” has been replaced with the phrase “Guidebook.” This is to avoid confusion with use of the word “framework” in other TM Forum documents.

For example, ISO Guide 73 – Risk Management states:

“Risk Management Framework: set of components that provide the foundations and organization arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization”

Whereas, this document would use the following consistent terminology:

Risk Management Guidebook instead of the phrase: “Risk Management Framework”.

2. Introduction

A DSP creates value for its stakeholders. It does this by defining a Mission, setting Goals to achieve this Mission, establishing a Strategy, setting Objectives and carrying them out in its Operations. This can be represented diagrammatically as follows:

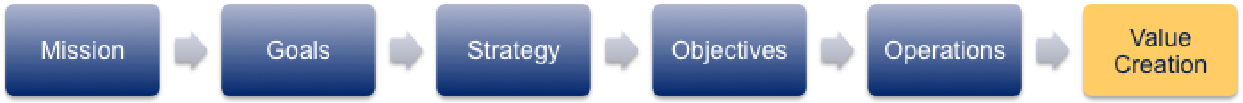

Figure 1: Value Creation

Uncertain events or sets of events (risks), should they occur, will have an effect on the performance of the DSP.

The purpose of Enterprise Risk Management is to maximize and protect the value created by establishing a Guidebook to manage risk effectively, efficiently and coherently across the DSP for those areas of the business that the DSP wants to proactively manage risk.

ERM establishes a Risk Management and Assurance Guidebook to maximize Value Creation:

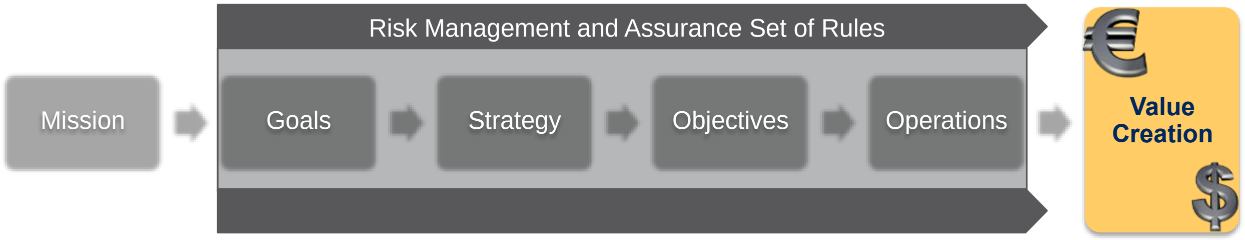

Figure 2: Risk Management and Value Creation

3. Risk Management, Corporate Governance and Internal Control

Risk Management is not a new concept. Indeed risk has always been an inherent feature in any undertaking. Risk is defined as an uncertain event or set of events that, should they occur, will have an effect on the achievement of objectives.

An uncertain event that would have a negative impact on objectives if it occurred is called a threat. An uncertain event that would have a positive impact on objectives if it occurred is called an opportunity. Risk is measured by the combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.

Corporate Governance and Internal Control protect the assets, earning capacity and reputation of organizations.

In recent years a more formal approach to Risk Management has developed due to the increased priority that stakeholders have given to Corporate Governance and Internal Control. Legislation and regulation has increased.

For example, the UK Corporate Governance Code (2010) aimed at companies listed on the London Stock Exchange states, "The Board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The Board should maintain sound risk management and internal control systems and review the effectiveness of these at least annually." Other examples include the United States federal law: Sarbanes-Oxley Act.

Also the UK Guidance for Directors (2005) states that the Board should consider:

- The nature and extent of the risks facing the company
- The extent and categories of risk which it regards as acceptable for the company to bear
- The likelihood of the risks concerned materializing
- The company's ability to reduce the incidence and impact on the business of the risks that do materialize
- The costs of operating particular controls relative to the benefit thereby obtained in managing the related risks

Over the years various cross industry risk management standards have been developed. Some, such as ISO 27011 Information Security Risk Management, have been developed for specific specialisms, others like COSO Enterprise Risk Management, have been developed for the organization as a whole.

Currently ISO 31000:2009 is the recognized international standard for risk management, and many organizations refer to this standard in their Risk Management Policy. The ISO 31000 family of standards provides non-industry specific guidance on Risk Management and a common vocabulary for discussing Risk Management. Specifically:

- ISO 31000 recommends that Risk Management should comply with eleven principles in order to be effective
- ISO 31000 proposes a five stage approach to establishing a Risk Management Guidebook
- ISO 31000 proposes a five stage Risk Management Process
- ISO 31010 provides thirty one risk management techniques
- ISO Guide 73 provides a Risk Management Vocabulary

In addition, the following standards and guidelines are used extensively across industries:

- COSO Enterprise Risk Management: published in three parts, namely: "COSO Executive Summary, Framework and Application Techniques"
- COBIT, Control Objectives for Information and related Technology, provides an enterprise wide, end to end Guidebook addressing governance and management information and related technology

The TM Forum Standard on Enterprise Risk Management Guidebook provides guidance specific to Digital Service Providers and is aligned with the cross industry standards and established best practice.

4. Risk Management Guidebook for DSPs

The purpose of a Risk Management Guidebook is to integrate the process for managing risk into the overall governance, strategy, planning, management, reporting processes, policies, values and culture of the DSP in order to manage risk effectively, efficiently and coherently across the DSP and thereby protect the value created by the DSP.

The Risk Management Guidebook integrates the process for managing risk across the complete set of nested objectives that make up the DSP. Therefore the first step in establishing a Risk Management Guidebook is to identify and understand the hierarchy of objectives that enable the DSP to create value.

Typically the DSP will establish an Enterprise Risk Management team to monitor and report the consolidated risks to the consolidated objectives of the DSP, and the DSP will establish Specialist Risk Management teams to monitor and report the risks at a detailed level. Examples of Specialist Risk Management teams for a DSP are:

- Revenue Assurance
- Fraud Management
- Program Assurance
- Critical Asset Protection
- Business Continuity Management
- Incident and Crisis Management
- Health and Safety Management
- Security Risk Management
- Financial Risk Management
- Environmental Risk Management
- Reputational Risk Management
- Contract Risk Management

The Enterprise Risk Management team will establish the Risk Management Guidebook. This will typically consist of the following six components:

1. Policy and Business Case
2. Risk Portfolios and Reporting
3. Risk Universe and Risk Register
4. Monitoring and Quantification
5. Awareness and Technical Training
6. Maturity Benchmark and Continual Improvement

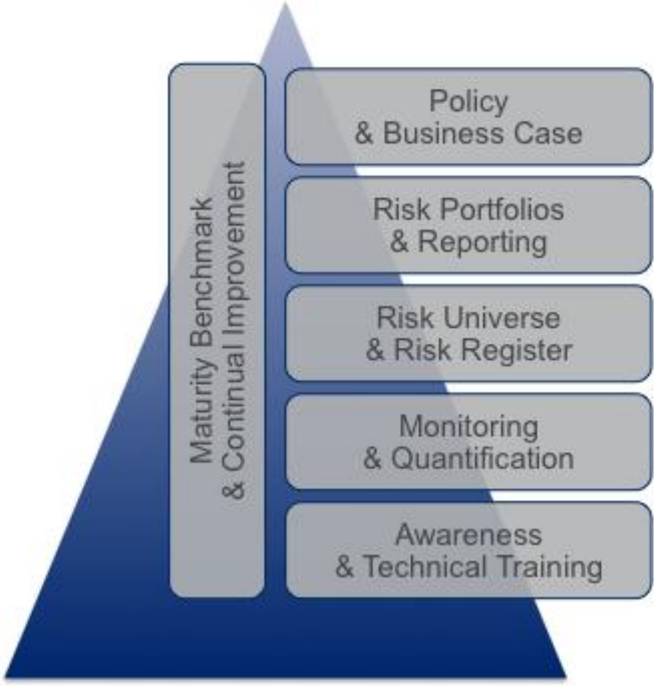

Figure 3: Risk Management Guidebook

The Policy and Business Case establishes a systematic and integrated approach to identifying, managing and monitoring risks supported by a business case mandate.

The Risk Portfolios and Reporting provide appropriate, timely and accurate reporting of risk to the stakeholders that are accountable.

The Risk Universe and Risk Register describe the set of risks, grouped into categories, that the DSP has decided to manage in order to protect and maximize the value that the DSP creates.

The Monitoring and Quantification activities critically observe, measure and report the status of risk exposure and compare it to risk appetite.

The Awareness and Technical Training raises awareness and provides technical competence to the DSP to improve the management of risk.

Maturity Benchmark and Continual Improvement assesses the DSPs current capability, measuring it against best practice, and providing practical recommendations on how to improve.

5. Risk Universe

The Board of the DSP should decide which risks should be proactively managed.

A proactive approach to risk management is likely to make stakeholders more confident about the DSP's ability to manage its affairs. DSPs need to determine which risks should be proactively managed. Typically risks will be proactively managed in order to meet stakeholder expectations and/or where proactive risk management achieves measurable value and delivers a return on investment.

The Risk Universe consists of the set of risks that affect the objectives of the DSP. The Board will choose a subset of these risks will be proactively managed. Because the DSP faces many individual risks, the Risk Universe will typically be presented to stakeholders as a set of categories of risk.

An example of a Risk Universe is presented below, organized into categories:

- Financial—Risks Associated with Items Typically Addressed in the Operator's Income Statements and Balance Sheets
  - **Liquidity & Credit** - Risks that would compromise company's ability to maintain reasonable / healthy cash flows
  - **Capital Structure** - Risks associated with the way company is owned and kept financially (e.g. shareholder / investor group, etc.)
  - **Tax** : Risks associated with Tax legal liabilities
  - **Mergers, Acquisitions & Divestiture**: Risks associated with merger / acquisition / divestiture operations.
- Personnel—Risks Associated with Employees
  - **Code of Ethics** – Risks associated with the composition and management of company's code of ethics to employees, 3rd party contractors & external vendors.
  - **People** – Risks associated with company's management of people – HR, ethnicities, geographies and local community constraints.
- General—Risks Associated with Enterprise-wide Issues
  - **Market** – Risks associated with local and global market place (political, financial, religious, etc.)
  - **Regulatory** – Risks associated with regulatory constraints and implications
  - **Communications and Investor Relations** – Investor / Shareholder perception management risks
  - **Market Dynamics & Commercial** – Business risks associated with local and/or global market scenario.
  - **Major Initiatives –** Risks associated with the execution of major and strategic projects
  - **Planning & Resource Allocation** – Risk and impacts managed by planning and resource management activities.
  - **Governance –** Risks associated with Governance / steering models and structures.
  - **Geopolitical –** Risks associated with the geography where business is operated.
- Technical—Risks Associated with Technology, Systems, Business Geography and Industry
  - **Fraud** - Risks related to exposure to fraudulent activities
  - **Information Technology** – Risks related to technology challenges and complexities of IT systems.

  - **Privacy & Information Security** – Risks associated with exposure of 3rd party confidential data and PII management.
  - **Cyber Security** – risks associated to management and impacts of attacks from WWW.
- Physical—Risks Associated with Tangible Items
  - **Physical Assets** – risks associated with asset management
  - **Hazards** – risks related to exposure to environmental hazards and liabilities
  - **Environment** – risks related to market and business environments
  - **Counterfeit and Tainted Products (Software and Hardware)**—risks associated with revenue loss and brand damage due to third-party incursion on genuine products
- Operations—Risks that are specific to Business functions
  - **Legal** – Risks associated with market's legislations
  - **Accounting & Reporting** – risks associated with the operations of financial accounting and reporting controls.
  - **Revenue Integrity** – risks associated with operators ability to track revenues flowing from all streams (E2E)
  - **Cost Integrity** – risks associated with operator's ability to manage operating cost levels.
  - **Supply Chain** – risks associated with operator's ability to manage the supply/order chain process and groups.
  - **Network Operations** – risks associated with the Operator's management of its network assets and utilization. (SLA's, etc.)
  - **Sales, Marketing and Customer Service** – risks associate with the operation of the Sales, Marketing and CSR's business functions
  - **Programs** – Risks associated with operator's management and execution of enterprise programs.

6. Risk Portfolios for DSPs

Stakeholders will have a subset of the DSP’s objectives that are relevant to them. The risks associated with this subset of DSP’s objectives make up their risk portfolio.

In order to engage effectively with the stakeholder, the ERM team must determine the relevant risk portfolio. This will enable the ERM team to provide relevant information to the stakeholder and receive relevant information from the stakeholder.

Key stakeholder groups for a DSP include:

- Board
- Audit Committee
- Finance & Investment Committee
- Program Office

Key individual stakeholders for a DSP include:

- Chief Executive Officer
- Chief Operating Officer
- Chief Finance Officer
- Chief Technology Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Compliance Officer
- Legal & Regulatory Director
- Head of the Program Office
- Head of Internal Audit
- Head of Revenue Assurance
- Head of Fraud Management
- Head of Security
- Head of Vendor Management

7. Administrative Appendix

This Appendix provides additional background material about the TM Forum and this document.

7.1. About this document

This is a TM Forum Guidebook. The guidebook format is used when:

- The document lays out a 'core' part of TM Forum's approach to automating business processes. Such guidebooks would include the Telecom Operations Map and the Technology Integration Map, but not the detailed specifications that are developed in support of the approach.
- Information about TM Forum policy, or goals or programs is provided, such as the Strategic Plan or Operating Plan.
- Information about the marketplace is provided, as in the report on the size of the OSS market.

7.2. Document History

7.2.1. Version History

Version Number	**Date Modified**	**Modified by:**	**Description of changes**
Version 0.1	1st July 2011	Paul Masters & Peregrine Chard	Initial draft
TEAM Draft	13th September 2011	Paul Masters	Terminology changes
Version 1.0	3rd October 2011	Paul Masters	Mention of SOX
Version 1.1	10th October 2011	Alicja Kawecki	Minor formatting and cosmetic corrections prior to web posting and Member Evaluation
Version 1.2	7th May 2012	Alicja Kawecki	Updated to reflect TM Forum Approved status
Version 1.3	22 October 2012	Mary Amalfitano	Updated for Fx 12.5
Version 1.4	12 November 2012	Alicja Kawecki	Minor formatting and cosmetic corrections prior to web posting and Member Evaluation

7.2.2. Release History

Release Number	Date Modified	Modified by:	Description of changes
1.0	1st July 2011	Paul Masters & Peregrine Chard	Initial release
2.0	22 October 2012	Mary Amalfitano	Updated for Fx 12.5

7.3. Company Contact Details

Company	Team Member Representative
Vodafone Group Services Ltd	*Name: Peregrine Chard* *Title: Global Programme Assurance Lead* *Email: peregrine.chard@vodafone.com*
Ericsson	*Name: Thomas Steagall* *Title: Director EP OSS / BSSManagement* *Email: thomas.steagall@ericsson.com*

7.4. Acknowledgments

This document was prepared by the members of the TM Forum Enterprise Risk Management team.