Revenue Assurance Guidebook

Revenue Assurance Risk Coverage Model

GB941 Addendum E

Version 1.6

April, 2012

Notice

No recipient of this document and code shall in any way interpret this material as representing a position or agreement of TM Forum or its members. This material is draft working material of TM Forum and is provided solely for comments and evaluation. It is not "Forum Approved" and is solely circulated for the purposes of assisting TM Forum in the preparation of final material in furtherance of the aims and mission of TM Forum.

Although it is copyrighted material of TM Forum:

- Members of TM Forum are only granted the limited copyright waiver to distribute this material within their companies and may not make paper or electronic copies for distribution outside of their companies.
- Non-members of the TM Forum are not permitted to make copies (paper or electronic) of this draft material other than for their internal use for the sole purpose of making comments thereon directly to TM Forum.
- If this material forms part of a supply of information in support of an Industry Group Liaison relationship, the document may only be used as part of the work identified in the Liaison and may not be used or further distributed for any other purposes

Any use of this material by the recipient, other than as set forth specifically herein, is at its own risk, and under no circumstances will TM Forum be liable for direct or indirect damages or any costs or losses resulting from the use of this material by the recipient.

This material is governed, and all recipients shall be bound, by all of the terms and conditions of the Intellectual Property Rights Policy of the TM Forum (http://www.tmforum.org/Bylaws/1094/home.html) and may involve a claim of patent rights by one or more TM Forum members or by non-members of TM Forum.

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

Revenue assurance is a rapidly maturing discipline. Over the last decade it has been evolving from a reactive program that investigated revenue leakage after it had occurred and tried to recover those revenues, through the active detection of problems that can be corrected before customers are affected, to the pro-active prevention of revenue leakage before it occurs.

The desire to move away from revenue assurance program being driven solely by problems that have been discovered and reacting to them, to a top-down method of risk identification based upon risk management principles is reflected in the publication of this document.

Risk Management itself is a mature subject area, and many industries and specialisms have their own defined set of controls. In fact, revenue assurance could itself be considered a form of risk management.

In order to provide the industry with the maximum business benefit of this initiative, it is proposed that the Revenue Assurance Controls are aligned to risk management best practice.

If adopted this would provide operators with the ability to:

1. Align their revenue assurance controls with other controls they have in their organization
2. Communicate more easily with existing risk management and audit teams
3. Integrate more readily with existing audit programs
4. Assist conformance with other corporate governance standards
5. Enable formal risk assessment within the context of revenue assurance
6. Quantify the contribution of Revenue Assurance controls on overall risk reduction

The Revenue Assurance Controls and Coverage Model and guidance contained in this publication therefore embraces risk management techniques to provide communication service providers with the ability to identify their revenue leakage risk areas by:

1. Identifying weaknesses in the effectiveness of their revenue assurance controls
2. Establishing the coverage of existing controls
3. Identifying gaps in the coverage of their revenue assurance controls
4. Assessing the business impact of those risks

Consequently, it will help organizations to:

1. Improve the effectiveness of existing controls
2. Identify additional controls that should be implemented

3. Prioritize the implementation of revenue assurance controls based on the relevance and impact to their business
4. Benchmark their level of coverage with their peers

The controls and coverage model are applicable to a wide variety of communications services providers; great effort has been made to provide a straight forward, technology and service neutral model that will provide meaningful results to as wide a segment of the telecommunications industry as possible.

Please note that the full Revenue Assurance Controls and Coverage Model will be released in stages over the coming months. Further details of the release schedule can be found in section 4.

The revenue assurance controls themselves are based on previous work undertaken by the TM Forum, in particular:

- Revenue Leakage Framework and Examples (GB941 Addendum D)
- Revenue Assurance Standard KPIs, RASK (GB941 Addendum C).

1 Introduction

This document recommends a series of controls that operators should consider implementing in order to reduce the risk of revenue assurance related issues and a method of assessing the coverage and effectiveness of those controls.

A Control is defined as one or more Measures that can be implemented to reduce the likelihood of a revenue assurance risk arising or to reduce the impact to the business if the risk did occur.

Revenue assurance risks themselves can be identified assessing the weaknesses of an organization in relation to the business requirements of Confidentiality, Integrity and Availability of both revenue and cost related information.

Please note that communications service providers are likely to operating at different levels of maturity within their various lines of business and consequently, it is recommended that control coverage should be assessed separately for each line of business.

Purpose

The objective of the Revenue Assurance Controls initiative is to develop a simple, technology neutral model, applicable to all types of communication service provider that will:

1. Support the identification, assessment and reduction of revenue assurance risks
2. Provide a method of assessing the level of the effectiveness of implemented controls
3. Identify where additional controls are relevant to an organization
4. Assist operators to create objectives and the priorities for improving revenue coverage of revenue assurance controls
5. Enable benchmarking between communications service providers
6. Quantify the contribution of Revenue Assurance controls to overall risk reduction
7. Prioritize the implementation of missing controls based on risk reduction

Scope

The Revenue Assurance Controls defined here are intended to be applicable to as wide a range of communications services providers as possible, regardless of their lines of business, size, services offered, split of revenues as well as systems and technology employed.

In particular, this model covers, but is not necessarily limited to, the following:

Lines of business	Pre-paid Post-paid Interconnect settlement Roaming clearing Wholesale Content services
Type of operator	Fixed line Mobile CATV Virtual network operator Carrier's carrier
Services	Access Voice/data/fax Messaging Data Streaming media Asset charges Value added services
Key Risk Areas	Product and offer management Order management and provisioning Network and usage management Rating and billing Receivables management Finance and accounting Customer management Partner management

These factors are relevant to understanding the nature and extent of the risks a communication services provider faces in relation to revenue assurance issues and can be used to guide the choice of relevant controls that are required in order to mitigate those risks.

Relationship to Other TM Forum Models

The relationship between this document and other models published by the TM Forum is outlined below.

GB941 Maturity Model	The RA Controls and Coverage Model complements the maturity model by providing guidelines as what revenue assurance should cover.
GB941 RASK (Revenue Assurance Standard KPIs)	The Revenue Assurance Standard KPIs model defines two KPIs related to coverage, however the definition is vague and it is intended to refine this concept in this document.
TR131 Drip-tray Model	This model was used as the basis of establishing the economic impact of placing a control. It is an illustrative model and did not evolve to permit the actual calculations envisaged here and therefore it cannot be used to calculate the importance of each of the checks in the revenue assurance controls coverage model developed here.
GB941 Addendum D – Revenue Leakage Framework and Examples	The document extends the leakage framework defined in GB941 Addendum D and the examples contained therein.

2 Revenue Assurance Controls

The Revenue Assurance Controls themselves are defined in GB941 Addendum E – Revenue Assurance Controls.

This section describes the information provided with the control definitions.

Process Areas

The Revenue Assurance Controls are selected based on the Process Areas defined by the Revenue Leakage Framework defined in GB941 Addendum D.

Weaknesses within in each Process Area can give rise to Revenue Assurance issues and so each is considered within the scope of the Revenue Assurance Controls.

Please note that the choice of processes here are taken from those typically referred to in the RA community and deviate slightly from the Business Process Framework (eTOM) processes. A mapping to Business Process Framework processes is provided. The Mapping to Business Process Framework (eTOM) **processes** covers major but not all **the Business** Process Framework processes that could be impacted by RA issues.

Process general Name	Description	Mapping to Business Process Framework (eTOM) processes
Product and offer management	Commercial issues associated with product conception that may result in the development of unprofitable products and services as well as the timing of product launches and special offers which may be made from time to time, or relates to product mix versus business targets and market dynamics.	Marketing & Offer Management (1.2.1) 1.2.2 Service Development Management 1.2.3 Resource Development

Order management and provisioning	Issues in the process of capturing and fulfilling orders from both domestic subscribers and commercial organizations, including errors in customer contracts, service activation faults or delays that impact revenues and/or costs as well as the coordination of suppliers and third party costs.	Order Handling (1.1.1.5) Resource Provisioning (1.1.3.2) Service Management & Operations (1.1.2)
Network usage management	Issues relating to the accurate accounting of service usage within the network and its recording as well as the management of that information as it is collected from the switching infrastructure to its delivery to the various rating and billing processes.	Service Guiding & Mediation (1.1.2 5) Resource Mediation & Reporting (1.1.36) Customer QoS/SLA Management (1.1.1.7) Resource Data Collection & Distribution (1.1.3.5)
Rating and billing	Issues within the rating and billing processes, from tariff identification, tariff definition, pricing, discounting, charging, billing and invoice production.	Bill Invoice Management (1.1.1.10) Bill Inquiry Handling (1.1.1.12) Charging (1.1.1.13) Manage Billing Events (1.1.1.14) Manage Balances (1.1.1.15) Perform Rating (1.1.1.13.1) Support Charging (1.1.1.1.16) Apply Rate Level Discounts (1.1.1.13.2)

Receivables management	Issues relating to the collections of monies after invoices have been issued, including the cash collection process, debt management and management of bad debt.	Bill Payments & Receivables Management (1.1.1.11)
Finance and accounting	Issues that affect the accurate reporting of the financial performance of an organization, including issues with general ledger mapping from the billing environment, tax payments with government agencies, incomplete processing of information from the billing environment and incorrect posting of entries in the chart of accounts.	Financial Management (1.3.5.1)
Customer management	Issues relating to the on-going relationship with customers, including subscriber identity issues, customer adjustments and rebates, SLA penalty payments, incorrect charging and discounting.	Selling (1.1.1.4) Problem Handling (1.1.1.6) Customer QoS/SLA Management (1.1.1.7) Retention & loyalty (1.1.1.9) Bill Inquiry Handling (1.1.1.12) Authorize Credit (1.1.1.5.2) Analyze & Manage Customer Risk (1.1.1.9.3) Manage Customer Payments (1.1.1.11.2)

Partner management	Issues associated with the management of relationships with third parties, primarily business-to-business interactions with organizations such as content providers, interconnect partners, dealers, roaming partners, wholesale partners and resellers. Examples include under-billing of partners, over-billing by partners, mismanagement of interconnect agreements, route optimization, charging errors, data exchange with external organizations and dealer commission payments.	

Sub Process Area

In order to provide a finer level of Controls are associated with sub-processes within a particular Process Area, as follows:

Product and offer management	Configuration
Order management and provisioning	Order Entry Provisioning Configuration
Network usage management	Event Generation Authentication Quality of Service
Rating and billing	Event Rating Reference Error Management Rating & Billing Calculation Bill Dispersement
Receivables management	To be defined
Finance and accounting	General Ledger Margins Credit management
Customer management	Credit Management Discount Management Customer Care
Partner management	Settlement

Check Type

Indicates the type of check that a Control would implement.

Completeness	Controls that relate to protecting the integrity of information, in particular that no information is missing.
Correctness	Controls that relate to protecting the accuracy of information.
Trend	Identifies issues were current performance deviates from previous, historical performance.
Margin	Controls that relate to the profitability of a product and/or service

GB941_D Reference

A cross reference to GB941 Addendum D – Revenue Leakage Framework and Examples.

For example, a Control could relate to more than one revenue assurance scenario in GB941 Annex D; in which case a list of cross references would be provided as follows:

"C.2 (2.3.2), C.11 (2.3.1) and C12 (2.3.12)"

Title

The name of the Control. This outlines the purpose of the Control, for example:

"Switches generate all required usage records."

Short Description

A brief description of the nature of the Control, for example:

> "Look for missing (or excessive) usage records, for example by counts, aggregated durations, pseudo rating and percentages. Usually by comparing to a reference source, e.g. a SS7 probe, test call generation equipment or other, peer switch."

3 Introduction to Risk Management

This section provides a brief introduction to the risk management techniques employed by the RA Controls and Coverage Model.

Readers who are interested in a more in-depth introduction to this topic should refer to the following publications:

- BS ISO 31000:2009, Risk Management – Principles and Guidelines
- ISO/IEC Guide 73:2009, Risk Management – Vocabulary – Guidelines for use in Standards

Overview

The following diagram illustrates the relationships between the main concepts of risk management as adopted by this model:

Figure 1 – Risk Management Concepts

Risk is assessment of the likelihood and impact to a business of one or more possible threats. This is known as the inherent or gross risk of an organization.

The more threats that could affect an organization, the higher the level of risk within an organization. Threats themselves may be previously identified or unknown.

Threats themselves arise because of vulnerabilities within an organization. Vulnerabilities are weaknesses that can be exploited by one or more threats. Consequently vulnerabilities increase the inherent risk within an organization to a given set of threats.

Ultimately those vulnerabilities expose business processes to those threats. Different business processes will have different levels of importance, or criticality, to an organization. Criticality is normally measured based on key business requirements of those processes; common requirements are Confidentiality, Integrity and Availability.

Therefore, the more critical business processes an organization operates, the higher the inherent risk within the organization.

An assessment of threats and the risk they pose defines the countermeasures or protection requirements that are necessary for an organization to reduce its risk to acceptable levels as defined by an organization's risk appetite, which defines how much risk an organization is ready to bear. These countermeasures are commonly referred to as Controls.

For the purposes of this document Measures are defined as the particular steps or checks that can be undertaken to implement a Control, i.e. Controls are implemented by one or more Measures.

Controls therefore mitigate the risk associated with one or more threats and have the effect of reducing the actual risk, by reducing the likelihood or impact or sometimes both for a given threat, thereby reducing the risk of a threat, often referred to a risk reduction.

The process of risk reduction results in a lower risk state often referred to as residual risk often referred to as net or residual risk.

Please note that full protection against a Threat may require one or more Controls and that a Control may protect against more than one Threat.

An organization's risk treatment plan will define which Controls are necessary for a given level of acceptable risk.

Risk Management Process

The generic risk management process is shown in the following diagram:

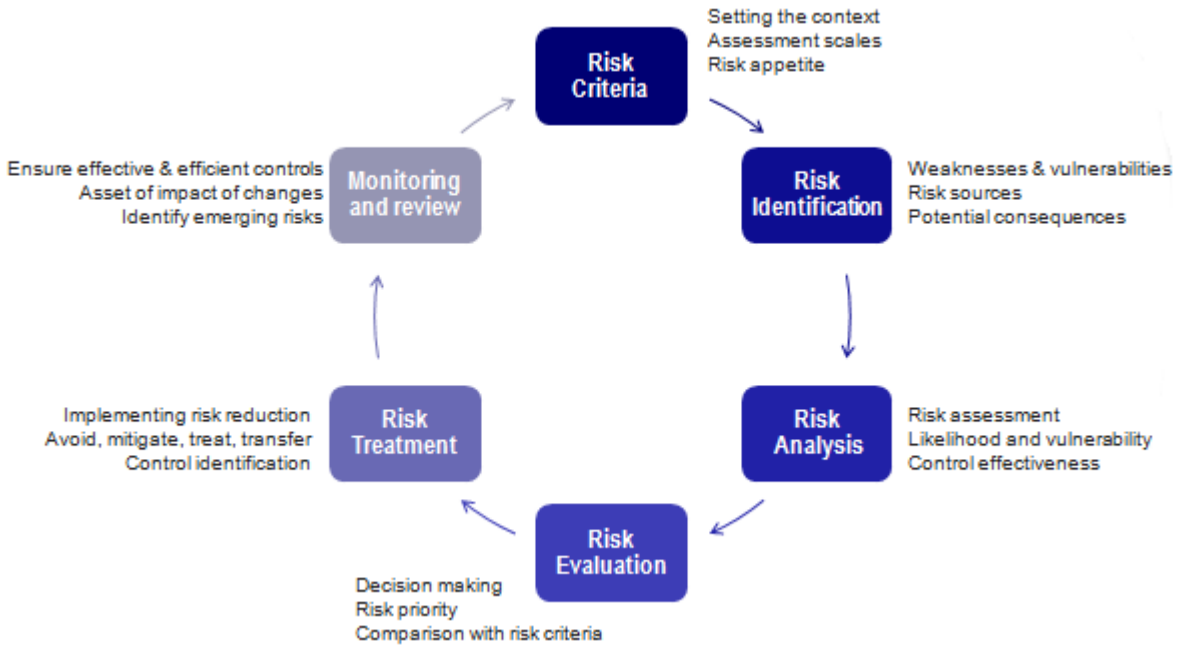


Figure 2 – Risk Management Process

4 Coverage Model

The coverage model provides a method of scoring the completeness and effectiveness of controls designed to protect against cost and revenue affecting risks for a given communications service provider.

Please note that the full Coverage Model is described here, but it will be introduced in phases in accordance with the Release Schedule defined in section 5.

Concepts

The Coverage Model is based on the following concepts:

1. Establishing a coverage score allows benchmarking activities that allow operators to understand how they stand in relation to their peers
2. Weakness and gaps in their coverage should be easily identifiable, from which coverage can be extended and prioritized
3. Controls are implemented through a series of related Measures, so the coverage model needs to operate at the level of these Measures
4. Not all Controls or indeed their Measures have a similar weight in terms of effectiveness of combating a particular risk
5. The Control framework is itself a non-exhaustive list, so an operator could be left with gaps even after the coverage model has been completed.
6. Some controls may overlap in terms of coverage, so they may not necessarily be additive
7. At the control level, two CSPs may perform the same Controls but use different Measures but may still achieve the same level of coverage
8. The Coverage Model must be applied to each line of business independently as coverage can vary between them

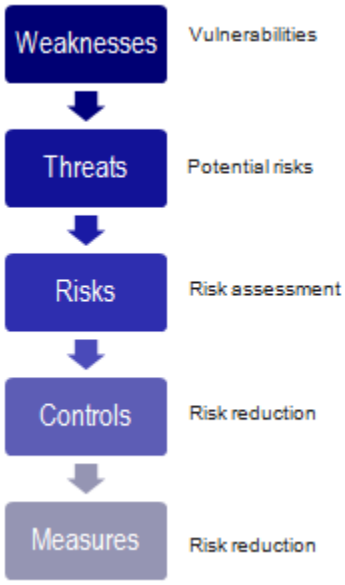
Control Identification

Risks can be identified by assessing the weaknesses of an organization and identifying the Threats that possible based on those Weaknesses.

Once Threats have been identified, Risk Assessments can be performed to determine the maximum level of Risk an organization is exposed to, i.e. the Inherent Risk.

Based on an organization Risk Appetite the target level of risk, or Residual Risk can be determined and the Control and their Measures necessary for the appropriate level of Risk Reduction can be determined.

This process is summarized in the following diagram:



Risk Assessment

The process of risk assessment is to identify relevant Threats and assess their level of Risk to a business in terms of their Likelihood and Impact (see Likelihood Scale and Impact Scale below).

Not all organizations offer the same products or have the same infrastructure, and so the actual risks posed by these threats vary. The actual risk that a threat poses is typically assessed through a risk assessment; by assigning a likelihood and impact for these threats.

A common method of accomplishing this is to assign numeric values for both factors, for example in the range 1-5 (1 is the least likelihood/impact through to 5 which is the highest likelihood/impact).

The Likelihood and Impact can be multiplied together to produce an overall threat level, or Risk Profile Number, for example:

Id	Threat	Likelihood	Impact	Risk Priority Number	Comments
1	Data loss between switches and the mediation system	2	5	10	File sequence number checking implemented between switch and mediation system so chance of missed data file is relatively low, but if it did happen then the impact to the business could be severe
2	Overcharging of interconnect settlement invoices	5	4	20	No ability to cross-check settlement invoices from interconnect partners to ensure that we are not being over charged for terminating traffic
3	Incorrect charging of data usage	0	0	0	All data products charged on subscription, so there is not threat of inaccurate usage based charges
4	Undercharging of SMS terminating traffic	5	1	5	Although few controls are in place for this revenue it accounts for a very small percentage of overall revenues
5	Incomplete TAP-in data files	3	2	6	No control over accuracy of generation of TAP-in files from roaming partners, but overall impact is limited to a small percentage of roaming revenues

A control reduces the likelihood of a threat arising and/or the impact to the business if that threat should materialize.

A threat may have one or more associated controls and a single control may have one or more particular measures that can be taken to mitigate such a risk.

For example, a control might be to ensure the completeness of data transferred between systems. The measures that could be adopted for this control could include: file counts, file sequence number gap checks, block sequence gap check, record sequence gap check, etc. This is summarized below:

Weakness	Poor systems integration
Threat	Data loss
Control	Ensure completeness of data transfers
Measures	File count Block count Record count File sequence gap check Block sequence gap check Record sequence gap check

Please note that any given operator may not necessarily implement all of these Measures, but each Measure that is implemented will reduce the Risk of data loss going unnoticed so that remedial action can be taken before billing is affected.

The application of Controls has the effect of reducing either the Likelihood and/or Impact of Threat, as shown below:

Id	Threat	Likeli-hood	Impact	RPN	Control	Measures	Likelihood Reduction	Impact Reduction
1	Data loss between switches and the mediation system	5	5	25	Ensure no data lost in transfer between systems	File count check File seq no check Block seq no check Record seq no check Local switch archive	-1 -1 -0.5 -0.5 0	0 0 0 0 -2
		-3	-2			Total risk reduction	-3	-2
		2	3	6		Residual risk		

The Likelihood and Impact reductions are adjusted by the Control Effectiveness, i.e. it's Extent and Frequency (see Control Effectiveness), as shown in the following table:

Id	Threat	Likeli-hood	Impact	RPN	Control	Measures	Likelihood Reduction	Impact Reduction	Control Effect-iveness
1	Data loss between switches and the mediatio n system	5	5	25	Ensure no data lost in transfer between systems	File count check File seq no check Block seq no check Record seq no check Local switch archive	-1 -1 -0.5 -0.5 0	0 0 0 0 -2	100% 100% 100% 100% 50%
		-3	-1			Total risk reduction	-3	-1	
		2	4	8		Residual risk			

Please note that individual risk assessments should be performed each line of business separately, as they will be subject to different Threats and Risks.

In this way, the list of Revenue Assurance Controls can be used to:

1. Identify relevant controls for an organization
2. Assess the effectiveness of existing controls
3. Identify missing control
4. Help prioritize the implementation of missing controls

Inherent Risk

The Inherent Risk can be determined by adding up the Risk Profile Numbers for each Risk identified by an organization.

Risk Reduction

The level of Risk Reduction can be determined by adding up the Effective Likelihood and Impact reductions each implemented Control brings to an organization.

Residual Risk

The Residual Risk can be determined by subtracting the Risk Reduction from the Inherent Risk:

Residual Risk = Inherent Risk – Risk Reduction

In-line Controls Versus RA Controls

In order to distinguish the contribution to Risk Reduction made by RA Controls it is import to assess Risk Reduction through existing, typically In-line Controls as well as that through additional RA Controls documented here.

So, when performing Risk Assessments the two sets of Risk Reduction must be identified separately, that is:

$$\text{Risk Reduction} = \text{Risk Reduction}_{(\text{In-line Controls})} + \text{Risk Reduction}_{(\text{RA Controls})}$$

It should be noted that it is unlikely that In-Line Controls will provide the full level of protection required by an organization, hence why they need to be supplemented by additional RA Controls.

Business Requirements

Risks are assessed as the affect on an organization's objectives. For the purposes of this document the following objectives are defined for Revenue Assurance:

	Term	Definition
1	Confidentiality	The measure to which information is accessible by the intended party, and that no unauthorized access is allowed.
2	Integrity	The accuracy and completeness of the information as it relates to the billing and settlement processes within a CSP. If the integrity of charging information is compromised then the accuracy of the billing processes will be affected.
3	Availability	The extent to which information is made available for various business processes i.e. its timeliness. If data is presented late to a billing process it may not be possible to charge for it.

Likelihood Scale

When considering the likelihood of a revenue assurance related threat materializing the following scale is recommended:

	Level	Description
1	**Unlikely**	0-20% probability, characterized by: Automated processes with continuous automated monitoring of controls.
2	**Seldom**	20-40% probability, characterized by: Automated processes with ad hoc monitoring or regular manual inspection of controls.
3	**Likely**	40-60% probability, characterized by: Automated processes with no monitoring of controls or high degree of manual processes.
4	**Very Likely**	60-80% probability, characterized by: Partly automated process with some manual processes little or no monitoring of controls.
5	**Probable**	80-100% probability, characterized by: High degree of manual processes with little or no automation and few automated controls.

Impact Scale

When considering the business impact to an organization of a revenue assurance related threat materializing an impact scale is required to determine the overall risk of the threat. The following Impact Scale is recommended:

	Level	Description
1	**Low**	Less than 0.1% of gross revenues.
2	**Moderate**	Between 0.1% and 0.5% of gross revenues.
3	**High**	Between 0.5% and 1% of gross revenues.
4	**Very High**	Between 1% and 5% of gross revenues.
5	**Severe**	Greater than 5% of gross revenues.

Weaknesses

When considering the vulnerabilities an organization has in relation to revenue assurance risks, the following factors should be taken into consideration:

	Description
1	Poor systems integration
2	Poor processes and procedures
3	High level of manual processes
4	OSS/BSS systems not fit for purpose
5	Out of date business rules
6	Uncontrolled change management
7	Ineffective/incomplete testing strategy
8	Poor reference data management
9	Poor configuration management
10	Poor logistics management
11	Poor quality of service
12	Low level of corporate maturity

Control Effectiveness

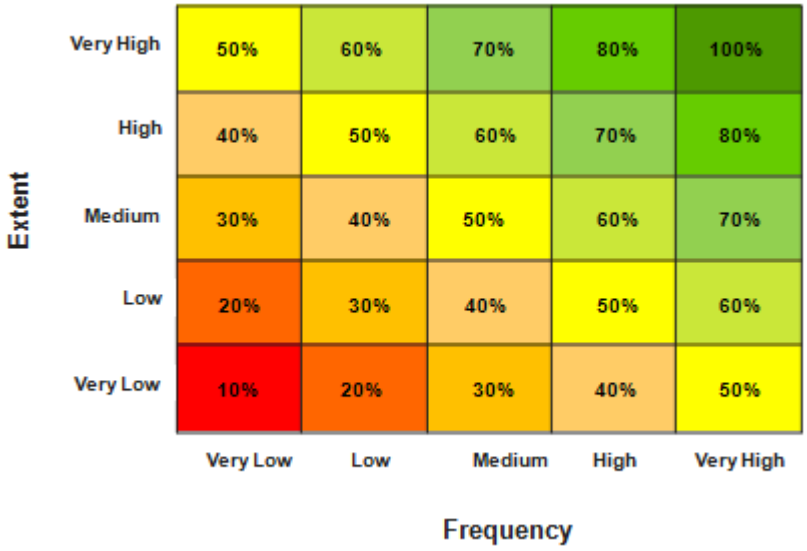
The Effectiveness of a Control, that is, the extent to which the Control implement the theoretical maximum risk reduction, is defined as a function of its Extent and Frequency.

Control Effectiveness = *function* (Extent, Frequency)

The Extent of a Control relates to the amount of data that is within the scope of the Control (see Extent Scale below).

The Frequency of a Control relates to how often the Control is performed (see Frequency Scale below).

Therefore, when considering the Effectiveness, i.e. the effect of its reduction of risk the following table should be used as a scaling factor for the Control's risk reduction:



Extent Scale

When assessing the Extend of a Control the following table should be used:

	Level	Description
1	**Initial**	Very Low. 0-20% of data within the scope of the control, characterized by: Most, if not all, of the data is not verified by the controls
2	**Repeatable**	Low. 20-40% of data within the scope of the control, characterized by: Only a small proportion of the data is verified by the controls which itself may not be a representative sample of the whole data
3	**Defined**	Medium. 40-60% of data within the scope of the control, characterized by: A large proportion of data is verified by the controls, but may not necessarily be a representative sample of the whole data
4	**Managed**	High. 60-80% of data within the scope of the control, characterized by: A large proportion or data is verified by the controls, or if sampling is used it must be representative of the whole data.
5	**Optimizing**	Very High. 80-100% of data within the scope of the control, characterized by: Either all of the data is verified by the control or statistically sound sampling is performed that covers the whole data and that sampling is augmented by "intelligent sample", i.e. • detecting problems with low frequency • re-detecting previous issues

Frequency Scale

When considering the five levels of revenue assurance maturity defined in GB941, the typical characteristics of extent are described here:

	Level	Description
1	**Initial**	Very Low, characterized by: Irregular and seldom, only as a result of an individual initiative, not part of a regular program.
2	**Repeatable**	Low, characterized by: In response to a requirement of internal or external auditors, or when problems are suspected. Normally once a year or less.
3	**Defined**	Medium, characterized by: Controls are performed periodically, with a frequency of once a month or more, although the schedule itself is not formalized. Data and resource availability are the key factors in when the control(s) are performed.
4	**Managed**	High, characterized by: Controls are performed regularly, with a frequency of once a month or more, to a predefined schedule. The actual frequency chosen is determined by business need and resource availability.
5	**Optimizing**	Very High, characterized by: Frequency is set according to business need and is not limited by data or resource availability. All controls are performed at least once a month and with 24 hours of the data becoming available.

Control Correctness

Please note that the correctness of the Control, i.e. its fitness for purposes, is not specifically included in this model.

It is assumed that Controls are fit for purpose and implemented correctly.

Control Gaps

The list of Revenue Assurance Controls can be used to determine whether an organization has implemented all Controls relevant to its circumstances.

Risk Matrix

The results of a risk assessment are often presented in the form of a risk matrix, as illustrated below:

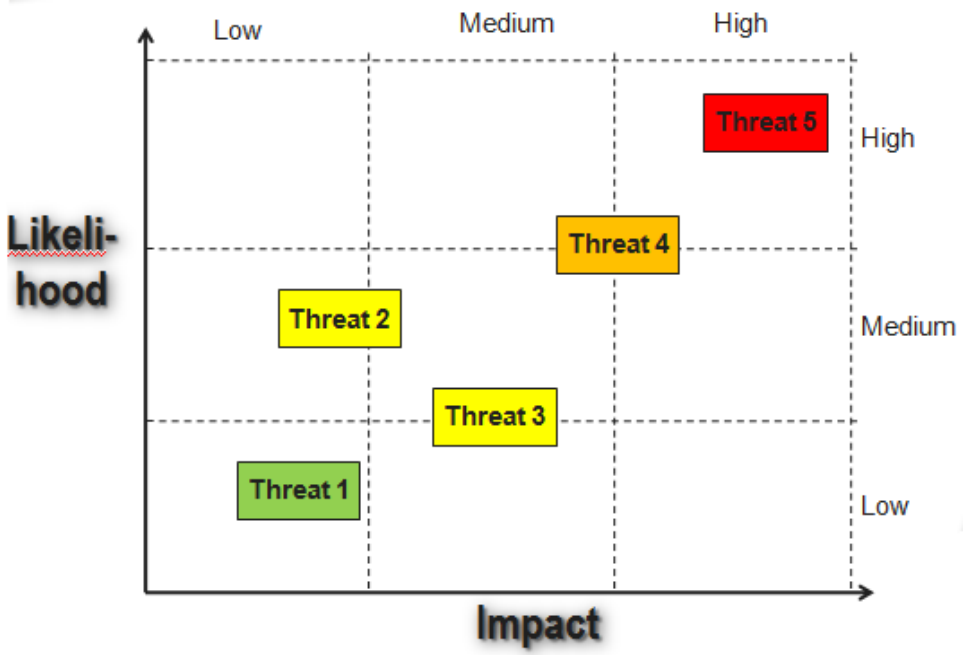


Figure 3 – Risk Matrix

5 Release Schedule

This section contains the expected release schedule for the Revenue Assurance Controls and Coverage Model.

Release 1 – List of Controls

The first release of the Revenue Assurance Controls and Coverage Model covers the following areas

- Introduction of risk management techniques to RA Control identification
- Identification of Controls by Process Area
- Preliminary Coverage scoring model

5.1.1 Controls by Process Area

The associated spreadsheet contains a list of revenue assurance controls by Process Area that are recommended for consideration by revenue assurance teams within the telecommunications industry.

5.1.2 Preliminary Coverage Scoring Model

Release 1 of the coverage model does not include the threats and risk estimation components. We assume that a risk level as per the Likelihood and Impacts scales, in section 4.9 and 4.10, can be used to assess the inherent risk in each Process Area for each Line of Business.

For Release 1 it is intended that this is the Current Risk Level that is assessed taking into consideration the current In-line Controls that are in place; this is considered the Inherent RA Risk level.

In a future release we will identify risk reduction through in-line controls separately from RA Controls. This will allow three risk levels to be identified: the true Inherent Risk (i.e. assuming no controls in place); the RA Risk level (i.e. residual risk after in-controls are taken into consideration and final true Residual Risk, after the additional RA controls have also been taken into consideration.

As an example, an organization's Current Inherent Risk level may be assessed as follows:

Line of Business	Process Area	Likelihood	Impact	Inherent RA Risk
Pre-paid	Product and offer management	4	3	12
Pre-paid	Network usage management	3	4	12

	Inherent RA Risk (Pre-paid)			**24**
Post-paid	Product and offer management	2	2	4
Post-Paid	Network usage management	2	2	4
	Inherent RA Risk (Post-paid)			**8**
	Total Inherent RA Risk			**32**

For each Line of Business and Process Area we have a set of relevant RA Controls and Measures, that may or may not have been implemented.

The Maximum Risk Reduction for each RA Control can be calculated as its reduction on Likelihood and Impact, as follows:

RA Control	Line of Business	Process Area	Likelihood	Impact	Maximum Risk Reduction
Control 1	Pre-paid	Product and offer management	1	2	2
Control 2	Pre-paid	Network usage management	2	3	6
		Maximum Risk Reduction (Pre-paid)			**8**

In the first release of this model, the effectiveness of all RA Controls for a Process Area within a Line Of Business can then be calculated as the average reduction ignoring the weighting of the RA Controls.

Firstly, the average Inherent RA Risk needs to be calculated, as follows:

$$\text{Average Inherent RA Risk} = \frac{\text{Inherent RA Risk}}{\text{Number of Risks}}$$

From the above example:

$$\text{Average Inherent RA Risk} = \frac{24}{2} = 12$$

Secondly, the average effectiveness of RA Controls, this is the RA Coverage for RA Controls for a give Process Area within a Line Of Business.

The effectiveness of each of the relevant RA Measures can be determined by using the matrix in section 4.12 to adjust the effectiveness of that Measure based on its Extent and Frequency.

For example assume that for "Product and offer management "in LOB "Pre-paid" we have 3 possible RA Controls, with effectiveness of 50%, 40%, and 60%, as shown in the following table:

RA Control	**Line of Business**	**Process Area**	**Likeli-hood**	**Impact**	**Maximum Risk Reduction**	**Effective-ness**	**Actual Risk Reduction**
RA Control 1	Pre-paid	Product and offer management	1	2	2	40%	0.8
RA Control 2	Pre-paid	Product and offer management	2	3	6	50%	3
RA Control 3	Pre-paid	Product and offer management	3	1	3	60%	1.8
		Risk Reduction			**8**		**5.6**

The average effectiveness is 50%, and therefore the average coverage of RA Control for "Product and offer management "in LOB "Pre-paid" is 0.5.

The impact of the RA Controls on a Process Area within a Line Of Business will be the associated with the Average Inherent RA Risk multiplied by the coverage. To convert the result into a scale of 1 to 5 it must be divided by 5. In our example:

$$\text{RA Control Risk Reduction} = \frac{\text{Average Inherent RA Risk x Average Control Effectiveness}}{5}$$

$$= \frac{12}{5} \times 0.5$$

$$= 1.2$$

These calculations are summarized in the following formulae:

$$Coverage_{i,k} = \frac{\sum_{j=1}^{j \le MaxControls_i} \begin{cases} Extent_{i,j} = NR \text{ or } Frequency_{i,j} = NR & 0 \\ else & Extent_{i,j} * Frequency_{i,j}/5 \end{cases}}{\sum_{j=1}^{j \le MaxControls_i} \begin{cases} Extent_{i,j} = NR \text{ or } Frequency_{i,j} = NR & 0 \\ else & 1 \end{cases}}$$

Where:

$$RRisk_{i,k} = RRisk_{i,k} * Coverage_{i,k}/5$$

and

$$\max_{k=1..7} \left(\begin{cases} Irisk_k \neq NR & Irisk_k \\ else & 0 \end{cases} \right)$$

and

NR = Not Relevant (control is not relevant for the Line Of Business)

Please note that in future releases the Risk Reduction will be calculated using Actual Risk Reduction.

Release 2 – List of Measures

The second release of the Revenue Assurance Controls and Coverage Model covers the following areas

- Identification of Measures related to each Control
- Extended Coverage scoring model at the Measure level

5.1.3 Measures

The range of Measures by which a Control can be implemented will be included in the model.

5.1.4 Extended Coverage Scoring Model

The Coverage Model will be extended to cater for risk reduction for Measures and also to distinguish between risk reduction due to existing in-line Controls and those introduced specifically for the purposes of revenue assurance risk reduction.

Release 3 – Full Model

The final release of the Revenue Assurance Controls and Coverage Model covers the following areas

- Identification of Weaknesses and Threats
- Mapping of Controls to Threats
- Final Coverage Model
- Control Correctness
- Risk Matrix

5.1.5 Identification of Weaknesses and Threats

This version of the model will relate Threats to the underlying root causes, or Weaknesses, that allow the Threats to present a Risk to an organization.

5.1.6 Mapping of Controls to Threats

Controls will also be related to Threats, so that it is clear which Threats are mitigated by which Controls.

Please note that a particular Threat may be mitigated by one or more Controls, and that a Control may mitigate one of more Threats.

5.1.7 Final Coverage Scoring Model

The final Coverage Model will be made available in this release.

5.1.8 Control Correctness

The concept of Control Correctness will be explored and published in this release of the model.

It stems from the fact that just because a Control is identified and implemented does not mean that it is the correct control for the risk nor even if it is, that it is operating correctly.

Advice and guidance will be provided to identify Control Correctness.

5.1.9 Risk Matrix

Guidance will be provided on how risks may be visualized in the form of a Risk Matrix.

Release Schedule

The proposed release schedule for the Revenue Assurance Controls and Coverage Model is shown below:

Release	Description	Date
1	Preliminary Release	Q4 2010
2	Extended Release	Q2 2011
3	Final Release	Q4 2011

6 Glossary of Terms

Terms which are used in RA Controls and Coverage Model and have a specific meaning are defined here.

Most of the terms defined here are based on ISO Guide 73, but please note that some new terms are defined here.

Term	Definition
Control	Something that is modifying risk. Note 1: Controls include any process, policy, device, practice or other actions which modify risk. Note 2: Controls may not always exert the intended or assumed modifying effect. (ISO Guide 73:2009)
Control Effectiveness	An assessment of the actual of risk reduction based on its Extent and Frequency.
Extent	An assessment of the effectiveness of the control based on the percentage of the overall data that is subject to a Control.
Frequency	An assessment of the effectiveness of the control based on how often the control is performed.
Impact	The consequences of a threat normally measured as the impact to one or more objectives of an organization.
Inherent risk	The level of risk in an organization assuming that no mitigating factors, i.e. controls, are in place.
Likelihood	The chance of something happening (ISO Guide 73:2009) Note: Likelihood is used here specific as it relates to possibility of a revenue assurance threat materializing.
Measure	A technique that reduces risk. Controls are implemented by one or more Measures.
Risk	Coordinated activities to direct and control an organization with regard to risk (ISO Guide 73:2009)

Term	Definition
Risk appetite	The level of risk an organization is willing to bear in pursuit of its objectives
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk management	Coordinated activities to direct and control an organization with regard to risk (ISO Guide 73:2009)
Residual risk	Risk remaining after risk treatment. Sometimes referred to as “retained risk” or “net risk”.
Risk treatment	The process to modify risk, which can involve: - Avoidance of the risk - Increasing risk - Removing the risk - Changing the likelihood of the risk - Changing the impact of the risk - Sharing the risk - Retaining the risk
Vulnerability	See Weakness.
Weakness	A vulnerability within an organization that allows one or more Threats to pose a Risk to that organization.

7 Administrative Appendix

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

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.

Document History

7.1.1 Version History

Version Number	Date Modified	Modified by:	Description of changes
1.0	8th November 2011	Geoff Ibbett	First draft, for comment
1.1	29th April 2011	Alicja Kawecki	Updated Notice and footer, minor cosmetic corrections made prior to web posting and ME for inclusion in Release 3.0 of the GB941 Solution Suite
1.2	16th September 2011	Alicja Kawecki	Updated to reflect TM Forum Approved status
1.3	14th October 2011	Alicja Kawecki	Revised document title to align with change noted in Section 3.1 of Release Notes for Release 3.5
1.4	13th April 2012	Alicja Kawecki	Updated to reflect TM Forum Approved status (for R3.5)

1.5	20th March 2012	Gadi Solotorevsky	Updated to use Frameworx nomenclature
1.6	13th April 2012	Alicja Kawecki	Notice, minor cosmetic corrections and version history updated to align with correct versioning prior to web posting and Member Evaluation

7.1.2 Release History

Release Number	Date Modified	Modified by:	Description of changes
3.6	20th March 2012	Gadi Solotorevsky	Updated to use Frameworx nomenclature

Company Contact Details

Company	Team Member Representative
cVidya Networks	*Name* Gadi Solotorevsky *Title* Chief Scientist *Email* gadi.solotorevsky@cvidya.com *Phone* +972 52 556 5218
rrmSolutions	*Name* Geoff Ibbett *Title* Senior Consultant *Email* geoff.ibbett@btopenworld.com *Phone* +44 7977 449832
Telefonica International	*Name* Gabriela Sobral-Gil *Title* Revenue Assurance Director *Email* gabriela.sobral@telefonica.com *Phone*
Swisscom	*Name* Rose Moura *Title* *Head Business Assurance* *Email* *Rose.Moura@swisscom.com* *Phone*
China Telecom	*Name* Elvis He *Title* *Email* herl@sttri.com.cn *Phone*

Company	Team Member Representative
Portugal Telecom	*Name* Carlos Duarte *Title* Head of Prevention & Projects *Email* carlos-m-duarte@telecom.pt *Phone*
China Unicom	*Name* Haoyang Lu *Title* *Email* LUHY@chinaunicom.cn *Phone*
Huawei	*Name* Adrian Long *Title* Senior Marketing Manager *Email* huiminlong@huawei.com *Phone*
Quantellia	*Name* Mark Zangari, *Title* Co-Founder *Email* mark.zangari@quantellia.com *Phone*
Ericsson	*Name* Igor Damjanovic *Title* Strategic Business Solution Manager, Revenue Assurance, BSS/OSS *Email* igor.damjanovic@ericsson.com *Phone*

Acknowledgments

This document was prepared by the members of the TM Forum Revenue Assurance Working Group team:

- Gadi Solotorevsky, cVidya Networks, RA Working Group Team Leader
- Geoff Ibbett, rrmSolutions, Editor
- Moshe Zolotov, cVidya

The document is a direct result of the work performed by the RA Coverage Model Catalyst team

- Gadi Solotorevsky, cVidya
- Amir Gefen, cVidya
- Gabriela Sobral-Gil, Telefonica
- Rose Moura, Swisscom
- Elvis He Ren Long, China Telecom
- Idalina Vilela, Portugal Telecom
- Carlos Duarte, Portugal Telecom
- Antonio Rosa, Portugal Telecom
- Haoyang Lu, China Unicom
- Dr. Chen, China Unicom

- Zhibin Guo, China Unicom
- Adrian Long, Huawei
- Helen Zang, Huawei
- Prabhudatta Mishra, Huawei
- Mark Zangari, Quantellia
- Lorien Pratt, Quantellia
- Igor Damjanovic , Ericsson
- Manuel Cabanas, Ericsson

Additional input was provided by the following people:

- Eric Priezkalns, Qtel ,Revenue Protect Limited
- John Brooks, Subex
- Geoff Ibbett, rrmSolutions
- Paul Masters, Ericsson
- John Karanikolas, Synaptitude Consulting
- Yoel Arditi, IBM
- Anandan Jayaraman, Connectiva
- Amitava Maulik, Connectiva
- Itay Gan, cVidya
- Robert Szekely, cVidya