

Revenue Assurance RFX Guidelines

GB941-C

Version 0.10



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

Notice.....	2
Table of Contents	3
List of Figures	4
List of Tables.....	5
Executive Summary	6
1 Introduction	7
1.1 Purpose	7
1.2 General.....	7
2 What to ask for in an RFx	8
2.1 Phased Solution.....	8
2.2 A solution description rather than a product description.....	8
2.3 Growth Potential	8
2.4 System interactions	9
2.5 TM Forum Standard Compliance	9
Information to be included in the RFx.....	10
2.6 Business Environment.....	10
2.7 The Intent behind the RFx.....	10
2.8 Existing Revenue Assurance operation	11
2.9 Revenue Assurance desired solution scope.....	11
2.10 Description of the IT policy in the organization.....	11
2.11 Data Sources/flows for the Revenue Assurance solution	12
3 Sanity Check.....	13
3.1 Data Volume	13
3.2 Data Storage Costs	13
3.3 Data Transmission.....	13
3.4 Timeliness	14
3.5 Ability to support execution.....	14
3.6 Data Access	14
4 Sample RFx structure	15
5 Functional Decomposition	18
6 Deployment Strategy.....	19
7 Administrative Appendix	20
7.1 About this document.....	20
7.2 Document History	20
7.2.1 Version History	20
7.2.2 Release History.....	21
7.3 Acknowledgments	21

List of Figures

Figure 1 Revenue Assurance within the Business Process Framework (eTOM) 6

List of Tables

Table 1 Deployment Strategy

19

Executive Summary

In today's environment where service providers are monitoring and watching over all expenses with extra care and caution we see an increase in the demand for Revenue Assurance tools and implementations as part of the above process. Revenue Assurance is being positioned now days as a strategic solution for operators. They realize that by implementing such a solution they will be able to increase their bottom line results and account for any lost revenues.

During recent years Revenue Assurance has been identified as an essential component of the TM Forum's overall solution Framework (Business Process Framework, Information Framework). These important frameworks have been complimented with a comprehensive Revenue Assurance framework that provides practical advice on how to tackle the challenges of revenue assurance. The guidebooks and supporting addenda provide a common understanding and definition of the problem space which enable service providers to better manage and improve their revenue processes.

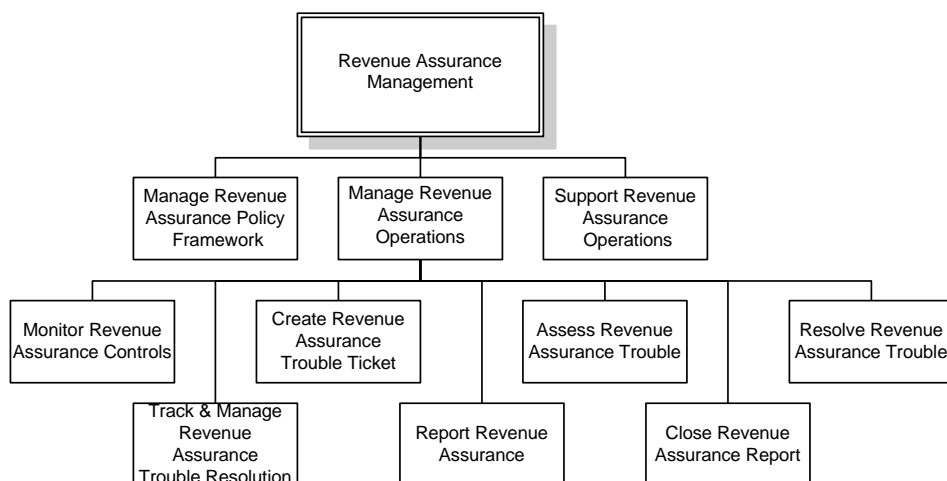


Figure 1 Revenue Assurance within the Business Process Framework (eTOM)

The growing need for Revenue Assurance solution brings with it also a growing number of Request for Proposal and Request for Inquiry (hereafter referred to as "RFX") documents issued by different companies to ISV's, system integrators and consulting companies looking for upgrading or introducing a new Revenue Assurance solution. The complexity of the business problem, the extent of systems involved, standards and frameworks available, and the number of industry solutions available can elongate the overall process. Poorly crafted RFX documents can result in inconsistent responses making it difficult to properly evaluate the best solution.

This Revenue Assurance Guidebook Addendum C tries to gather the most important foundations of the guidelines and requirements for a Revenue Assurance RFX to assist service providers to ask relevant questions and objectively evaluate responses to procure the solution that meets its needs.

1 Introduction

1.1 Purpose

The purpose of this document is to provide Service Providers with assisting guidelines for issuing RFx's for Revenue Assurance solutions. Each Service Provider will be able to add his specific requirements on top of this document.

1.2 General

The RFx Guideline covers the following aspects of the RFI / RFP:

- How to form the RFx in a way that would allow the Service Provider to effectively benchmark competing replies / bids
- The information that should be provided within the RFx so that the vendors would be able to relate to the specific characteristics and requirements of the Service Provider
- How to perform a sanity check for the request and over the replies / proposals.
- A proposed format / template of an RFP/RFI.

2 What to ask for in an RFx

2.1 Phased Solution

Implementing a full blown Revenue Assurance solution that covers the whole functionality and each and every relevant location in the organization, the network and the supporting systems is practically impossible to do and even harder to maintain once done. On the other hand – aiming for the complete solution is a desirable strategy. The solution this dissonance lies in the form of a phased approach solution.

Realistic division into well defined phases turns the project into a manageable and is much easier to implement, integrate, comprehend and assimilate. The role of the Service Provider in this 'phasing' approach is to set the framework for each of the phases. The dimensions of this framework span across functionality (e.g. monitoring, problem examination, root cause analysis, problem resolution, etc.); business processes (ordering, provisioning, service delivery, billing, etc.); systems (CRM, billing system, Network Management, DWH, etc.); services (e.g. voice, messaging, data access, etc.); and service elements (by geography, customer types, network equipment types, number of controls, etc.).

2.2 A solution description rather than a product description

When RFx documents contains a set of requirements, vendors often reply with a generic product description, which highlights the benefits of the product, leaving it to the Service Provider to figure out how the product features are mapped to the requirements stated in the RFx. A better way is to structure the RFx to demand the responses to describe the specific solution rather than the generic product, and there are two main reasons for this:

- As a threshold mechanism – it is not enough that a vendor has the most glamorous software product. The vendor should be able to implement the product according to the Service Provider's specific requirements and preferences.
- As a basis for benchmarking – a good benchmarking is done by comparing 'apples to apples'. The requirements, or the statement of issues to be solved, serve as a standard ruler, on the basis of which each of the replies / proposals needs to be mapped and scored. Once there is a score, benchmarking is very simple to do, technically, hence – a great tool to assist the decision making.

2.3 Growth Potential

The growth potential in a Revenue Assurance project has three aspects.

Transition between project phases

The first aspect is merely the mechanism of moving from one phase of the project to the next. The Service Provider has to state the ground rules for such a transition, and the vendors have to relate to these ground rules and explain how they are going to demonstrate the fulfillment of these rules.

Enhancing capabilities against dynamic requirements

As the Service Provider keeps evolving, the technology, the market and the opportunities keep on changing, the vendor should demonstrate its ability to enhance the capabilities of the solution accordingly. This type of enhancements may be in the form of adding phases to the project (without explicitly define the characteristics of these phases, as they are not known at the time of the RFX creation) or as an enhancement within the already established phases, for example – when referring to the amount of customers or volume of data to be analyzed in a specific region. The vendor should explain how the offered solution is going to address this type of growth / dynamic requirements.

Maturity Enhancement

Each Revenue Assurance organization should have a roadmap, according to the TM Forum Revenue Assurance maturity model. Each of the maturity levels requires a set of capabilities and operation that imply a discontinuous improvement. Implementing discontinuous improvements where a specific system is in production is far from being trivial, and the vendor should provide a description of how to handle this type of requirement leap based upon the offered solution. This type of enhancement is, in a way, similar to the previous one (the enhancing capabilities), but the difference is that in the previous case – the requirements are changing incrementally and in relatively small steps, and when the change is in the maturity – the implication is much more ‘revolutionary’.

2.4 System interactions

For the cases in which the Service Provider has, or plan to have Revenue Assurance products of more than one vendor (which may be relevant when ‘best of breed’ strategy is in place), very important requirement is that each of the offered solutions would be able to interface with other Revenue Assurance solutions. These interfaces can be achieved in many ways, and the vendor should state the mechanism that supports them. The interaction of each Revenue Assurance system with others can be southbound (collecting or receiving information from other systems) and/or northbound (sending / providing information to other systems). The Service Provider should require the type of interaction that fits the strategic approach to the implementation of Revenue Assurance. The vendor response should provide a description not only of the data that it can acquire from other Revenue Assurance systems and share with other Revenue Assurance systems, but also the supported interface technology – protocols, structures, formats, etc.

2.5 TM Forum Standard Compliance

The TM Forum has published several recommendations that became de-facto standard in the Revenue Assurance industry in particular, and in the Telecom BSS/OSS industry in general. These standards include:

- The Revenue Assurance Technical Report (TR131)
- The Revenue Assurance Guidebook (GB941)
 - Standard KPI (GB941a)
 - Revenue Assurance Maturity Model (GB941b)
 - Revenue Assurance RFX Guidelines (GB941c)
 - Control Leakage Points (GB941d)
- Business Process Framework (eTOM (GB921))
- Information Framework (SID (GB922))
- Application Map (GB929)

Information to be included in the RFx

The more concrete information the vendor has the more accurate and focused the response can be. When the vendor understands the environment, the specific needs and the preferences of the Service Provider, they are able to provide a better response -- making it much easier for the Service Provider to compare responses to each other.

2.6 Business Environment

The Service Provider has to provide a description of the business environment in which the solution is required to operate. This description should include:

- The type of the Service Provider – technology and services wise
- Macro parameters:
 - Relevant regulations (e.g. SOX, privacy, etc.)
 - Currencies involved – in the case that the Service Provider is multi-national, or involved in commercial relationship with value chain parties that use other currency
- Commercial parameters:
 - Market share and growth potential
 - Customer types and quantitative segmentation
 - Service value chain description
 - Description of the existing environment VS. the future environment for the next 2 years

2.7 The Intent behind the RFx

The Service Provider must state the main benefit expected from the Revenue Assurance and/or cost assurance solution. This statement dictates the focus of the solution. It is not necessarily a dichotomy, but definitely a statement of priorities. Basically, there are several options here:

- Assuring company revenues. The need for having an accurate inventory for both incoming and outgoing revenues.
- **Revenue leakage detection** – The basic need from a Revenue Assurance system is to detect revenue leakage. This would usually be the intention of an organization making its first steps in Revenue Assurance operation. The system would be geared, in its first stages, to collect the 'low hanging fruit', that is – the leakage that is apparent due to lack of data and process integrity, and help the Service Provider to investigate and understand the reasons for the detected leakage.
- **Revenue Leakage Prevention**
- **Active Revenue Assurance** – this intent drives a focus on high performance of the offered solution. The Service Provider should define what it means by granularity of seconds, minutes, hours, etc. The Service Provider should also notice that in many cases there is a tradeoff between the time granularity and costs, and that the answer may vary between the different controls/ systems. The requirement will also cover the corrective measures needed in order to prevent the revenue losses Reference to TR131
- **Support regulatory compliance (e.g. SOX) and internal auditing requirements** – These requirements mainly refer to the ability of the system to demonstrate internal integrity, to report the results in a way that would allow the Service Provider to use it within other mandatory reports and to allow external parties (systems or people) to probe into the control structure and the historical data maintained by the Revenue Assurance system.
- **Other Goals e.g. margin management, stock control, accruals etc.**

2.8 Existing Revenue Assurance operation

Behind every IT need there are people, processes and information. If the solution does not address all of these – it becomes useless. In order to provide the context of the intended solution, the Service Provider must first describe the existing operation of Revenue Assurance in the organization. This description should include, at least, the following:

- Revenue Assurance organization:
 - Existence
 - Size (how many people)
 - Modus operandi – Geographic and organization-wise position (centralized / distributed); Time scale (Alert / Research); Interactions with other sub-organizations
- Maturity level with regards to the TM Forum (Reference) Revenue Assurance Maturity Model
- Scope of Revenue Assurance within the company and the processes included (e.g. collection, credit control etc.)
- Solution strategy – The preferred approach of the organization to IT solutions, internal development and support vs. product procurement vs. 3rd party tailor-made software development projects

2.9 Revenue Assurance desired solution scope

The Revenue Assurance discipline spans across several functionality domains and different vendors may have different expertise. The Service Provider has to indicate which domains should be covered or excluded by the offered solution:

- Switch to Bill
- Lead to cash
- Usage
- Configuration
- Rating & Billing
- Interconnect
- Etc...

The Service Provider should keep in mind that there is a trade-off between the granularity of the control points and the cost (both in terms of data analysis, as well as in the energy that should be invested in maintaining the control points). The above should be mentioned as a requirement for the RFX and 2 years to the future.

2.10 Description of the IT policy in the organization

Another aspect of the context in which the Revenue Assurance solution is needed is the system environment. Clear, concise statements will enable the vendors to gain a more thorough understanding of the requirements and the types of parameters that may affect the offered solution significantly:

- System architecture approach:
 - Does the organization have an IT policy management system? Is there a common guideline or is it of the prerogative of every department / division to decide how to orchestrate its IT policies?

- Is the overall architecture derived from any industry standards? Is there a common infrastructure to which all the systems should interface (e.g. EAI / SOA bus / CORBA / Web Services)
- System characteristics:
 - Approved/Unapproved hardware
 - Approved/Unapproved OS
 - Approved/Unapproved Database

2.11 Data Sources/flows for the Revenue Assurance solution

Many of the solution aspects are heavily dependent on the way in which the source data arrives at the Revenue Assurance system. When the vendor knows the format and the context of the data that the Revenue Assurance system requires, the proposed solution will be more suitable to the Service Provider's needs.

The Service Provider, in order to achieve this level of solution adequacy, should provide the following details within the request:

- For each of the candidate source systems:
 - Type of the relevant data – static / transactions / logs etc.
 - Type of protocol per source
 - Volume of the source data
 - Rate of data creation / submission – near real time / batch
- The distribution of the data in terms of systems layout as well as in terms of geography and localization (possible diversity of languages, metrics, time zones, etc.)
- Data Warehouse as a data source:
 - Data Warehouse is NOT a recommended Revenue Assurance source. But where the service provider makes this choice, the following should be included in the RFx:
 - Description of the available data (fields and context)
 - Level of data cleansing before arrival to the Data Warehouse. The data cleansing process itself can create a perception of high-quality data leaving the 'bad' data out, without cleaning it from the operational system. Consequently, the operational data is 'bad', but the Revenue Assurance system is not aware of it due to the intermediation of the data warehouse.
- For each of the systems that are candidate to become data sources, including network devices, the following information may affect the offered solution:
 - System type (e.g. Billing, Inventory, NMS, Switch, etc)
 - System vendor: in many cases, the Revenue Assurance vendor may have a ready-made interface to other systems, as a part of an alliance between the two or past projects at other Service Providers.
 - Current data retrieval mechanism / protocol: direct access to database, data extracts in files, API calls, interface layer (e.g. EAI)

It is advisable for the Service Provider to check the ability of providing incremental data and/or introduce changes to the existing data sources

3 Sanity Check

The sanity check includes 2 main phases. First, the Service Provider should perform a sanity check over the RFX before issuing it to the vendors, to make sure that the request is internally consistent and that it is feasible with respect to technical, organizational and legal restrictions (**pre-submission** sanity check, hereafter). The second check takes place after receiving the vendor replies. Its purpose is to make sure that the bid is reasonable and with internal integrity (**bid** sanity check, hereafter).

3.1 Data Volume

In the pre-submission sanity check – the purpose is to make sure that the data volumes that are mentioned in the request are consistent with the size of the organization, the number and the types of the customers and the services.

In the bid sanity check, the Service Provider is to check the data volumes that are supposedly derived from the source data volumes stated by the Service Provider in the RFX.

Sometimes we find larger numbers in the bid compared to the request, as some of the data needs to go through stages of enrichment, and to be kept for the purpose of reconciliation and analysis. However, the Service Provider can check to what extent the numbers are larger and to make sure that each such difference in the data volume statements has a good explanation.

3.2 Data Storage Costs

This section is significance only as part of the bid sanity check. The Service Provider can get a figure of the costs of data storage, either by deriving it from the information in the various bids, or from external sources, and reconcile each of the proposals against this figure.

3.3 Data Transmission

This section should be considered in the context of the distribution level of the data sources and of the Revenue Assurance operation. In the case of high distribution – the Service Provider has to make sure that the physical and logical network infrastructure is sufficient to transfer the amount of data required to perform the requested Revenue Assurance tasks, and in the case of a centralized operation, the Service Provider has to make sure that all the data that is required for the Revenue Assurance tasks fulfillment has a way of getting to the Revenue Assurance system(s).

On the other hand, in the bid sanity check, the Service Provider can refer to the data transmission requirements derived from the architecture and the model of the offered solution and to assess whether these requirements are sufficient, feasible, proportional to the actual data, or if there is a way to reduce these requirements (every KB of information transferred from one system to another consumes costly resources).

3.4 Timeliness

In the pre-submission stage, the Service Provider has to check two things. First, and most important, the timeliness of source data creation (record files, data mart updates, etc.) puts a limit to the frequency of data processing. It is of no benefit to process the data in a higher frequency than that of the source data update. Thus, the requested data processing rate should take into account this limit.

The second aspect is the cost of data processing, both in terms of computing power as well as in terms of required storage and means of storage.

The Service Provider has to consider, as part of the pre-submission sanity check, whether there are places in which the requested data process frequency can be reduced, to eliminate unnecessary costly computing resources. There are basically two ways of reducing the required level of computing in this aspect – one is to require batch processing as opposed to near-real-time processing, and the other is to require statistical sampled processing as opposed to processing of all of the source data. In the bid sanity check, the Service Provider should look for the same kind of restrictions that the source systems put on the timeliness

3.5 Ability to support execution

In the pre-submission sanity check stage, the Service Provider needs to make sure that all the supporting capabilities are taken into account. For example, a requirement to place control points in every possible place within a process has to be supported by resources to maintain the control point, get the source data and make sure that the Revenue Assurance system adjusts itself (most probably, with the help of human Service Providers) with the changes in the data source.

In the bid sanity check, the Service Provider should examine what supporting resources the offered solution requires and to what extent the support is feasible and proportional to the projected benefits to be achieved by the solution.

3.6 Data Access

The Service Provider will conduct a pre submission check for the ability to access the data with all aspects in mind:

- Technical feasibility – is the required interfaces of the source system in place?
- Required support – is there documentation or a reference person that can provide the context of the data and the guidelines to access it?
- Internal politics - are there foreseen obstacles that may interfere with the access to the data due to personal or departmental interests?
- Regulations and laws – is there a legal permission to use the data? Privacy regulations and customer protection regulations can create a substantial obstacle on the way to acquire the data.

A bid sanity will be able to adjust the access requirements based on received results and validate that all data sources have been considered.

4 Sample RFx structure

The RFP would include the following parts:

- Introduction
 - Background - this will include 'intention statement' and the background / context and the motivation for the RFx
 - General – this will include a clarification of the main terms that will be in use throughout the RFx. Here is the place for definition of terms such as reactive, active and proactive Revenue Assurance, the Revenue Assurance ABEs, and other standard terms, but also for definitions of terms that can get different interpretation in different companies. (E.g. types of customers such as residential, business, corporate, etc.)
 - RFx structure should include one sentence about each of the chapters / annexes, information about the documents that construct the RFx together, the requirements, the templates for reply, the required form of cross reference indication between the chapters / annexes / documents.
- Guidelines for the response:
 - Instructions – administrative and legal. Here is where non-technical terms, conditions and processes related to the RFx are defined. The requirements for the structure of the response, priorities (e.g., the Service Provider may indicate that different requirements have different priorities, so that some of them would be mandatory, some important, some preferable and some 'nice to have'). Other indications that may find its representation here are the description of the process (e.g. – distribution of the RFx, getting the replies, Q&As, short list announcements, presentations, etc.)
 - Contact persons – names, titles and contact details
- Technical Environment, subject to information security considerations
 - A description of the services which should be covered under the scope of the RFx
 - For each service – a description of the role of each participating network, IN / AIN elements and relevant OSS/BSS. For example, when describing a premium SMS service – describe the service architecture with all the SMSCs, gateways, MSCs, service nodes with relevant information and other network equipment, as well as which specific provisioning system is involved in the subscription process, and which service relevant data is flowing between the systems.
 - OSS and BSS architecture: here is the place to sketch an overview diagram of the existing OSS / BSS existing deployment that is relevant to the services covered under the scope of the RFx. It should contain as much as possible information about the types of systems (e.g. Billing, CRM, and Provisioning), the vendors and the number of systems of each type.
 - A description of relevant business processes – this will usually include the products/services fulfillment and billing processes. It would help if the description would be accompanied by a UML collaboration diagram showing that various systems and the information flowing between the systems.
 - Special physical environment parameters, if applicable
 - Electricity
 - IT – network, specific relevant software licenses (OS, databases, etc.)
 - Distributed system considerations
- Organizational environment
 - Characteristics of the system users – here is the place to categorize the users of the required system (RA analyst, RA manager, business user external to the RA staff, administrator, etc.).
 - Interfaces between the relevant organization groups: Revenue Assurance is, at the end of the day, a vehicle to improve the accuracy of processes and the coherence between different systems. These systems are typically operated by different sub organization of the Service Provider (e.g. finance, operations, marketing, sales, etc.). The organizational formal interfaces can provide the vendors with better understanding of where to focus in order to find discrepancies or revenue leakage.

- Functional Requirements
 - General
 - An introduction to the chapter, explaining the structure and the 'way to read' the chapter. This may be used particularly in the case of using a template for each requirement.
 - User interface
 - Dashboards
 - Which dashboards are desired, describe what the user wants to see upon starting the application, how flexible the dashboards are, etc.
 - Alarms panel
 - Alarm status and severity levels – here the Service Provider may define the status indications (active, close, resolved, etc.) and the severity levels (minor, major, critical, warning or any other set) or to ask for the severity levels and status indications that the vendor suggests.
 - Structure: here the vendor may be asked for the structure of an alert record, and about the capabilities resulting from the structure (dealing with multiple alarms, search capabilities, historical queries, etc.)
 - Revenue Assurance Trouble Tickets management
 - Structure: here is the place to query about the fields included in the Revenue Assurance Trouble Ticket. This is particularly relevant for the case in which the Trouble Ticket is to be injected to other systems for further treatment or for the purpose of correlating it with trouble tickets coming from other systems. Here is also the place for the Service Provider to require mandatory fields.
 - Workflows: A trouble ticket may be transformed from one state to another and from one user to another. The Service Provider may query the suggested flows or to define one or more business flows that should be supported by the offered system. In addition, the Service Provider may require flexibility in defining the workflows.
 - Pre-defined reports
 - Structure – what are the fields that should be included in a report and the level of flexibility
 - Indicators (Gauges, Graphs, etc.)
 - Types – which types of indicators are available and to what extent the user can configure them
 - Drill down capabilities
 - To which level – which aggregation levels are , raw data
 - Within what time frames
 - Self configuration capabilities:
 - Ease of configuration and adaptation to new services: here the Service Provider may want to know which services are supported by the provided system and to which extent, and to query or require ease of configuration of the system in order to adapt new services and new features in existing services.
 - Offline testing of the self configuration
 - Administration
 - User management
 - Roles management
 - Security
 - System management
 - Advanced user interface (if applicable)
 - KPI Management
 - KPI modeling

- Types of KPIs
- Expected reporting output of the Revenue Assurance solution
 - The desired modus operandi of the Revenue Assurance solution may vary in the dimensions of scope and timeliness. Basically, there are four options:
 - Analyze all of the data all of the time – apply the Revenue Assurance reconciliation rules on each and every piece of data as the event that creates the data occurs.
 - Analyze all of the data part of the time – apply the Revenue Assurance reconciliation rules on data aggregated over time periods, and drill down when there is a suspicious outcome, as part of the root cause analysis process.
 - Analyze part of the data all of the time – define a sampling criteria, and apply the Revenue Assurance reconciliation rules on all the data that applies to the selection criteria at the moment that this data is introduced to the Revenue Assurance system.
 - Analyze part of the data part of the time – analyze and apply Revenue Assurance reconciliation rules on selected data, which is aggregated over a time period, with the ability to drill down to the single data item for root cause analysis purposes.

The Service Provider should state whether a specific modus operandi is required. It is also possible, but should be stated as such, that the decision upon the modus operandi would be based upon the vendor's recommendation.

- Data collection
 - A list of the data sources (if known)
 - Supported Protocols – FTP, SOAP, JMS, etc.
 - Data structures within each data source (if known) – xDRs, inventory records, customer data records, etc.
 - Time considerations
 - Time resolution of the data
 - Desired collection periods (if relevant) – e.g. during night time
- Data export (northbound)
 - Business processes for which data export is required, e.g. charging and collection, problem escalation, executive reports, etc.
- Regulatory compliance
- Security
 - Confidentiality
 - Securing information along the flow
 - Integrity
 - Data will remain intact along the flow
 - Availability
 - Information will be available to other system
- Storage
 - The RFx should inquire about the approach to storing any level of information:
 - Raw data (raw files and raw extractions from databases)
 - Formatted and enriched data
 - Aggregated and summary data
 - Reconciliation results
 - Alerts
 - Trouble Tickets and their history
 - Reports
 - Approach to storage can be defined as 'for <such and such time> the <relevant information> will be held in a granularity of <...>

5 Functional Decomposition

The RFX should define the expectations or to ask for the system architecture, at least on the top level functional decomposition. This is characterized by the availability of distinct products geared towards a specific functionality. A basic list of these functional components includes:

- Test call generation
- Data collection modules
- Reconciliation for usage data
- Reconciliation for non-usage data
- KPIs handling
- Front end (dashboards etc.)

6 Deployment Strategy

The recommendation is to require a staged deployment approach. The Service Provider has to decide, based upon business priorities, existing and foreseen services and network environment, the stages of the functional and technological implementation of the system.

The Service Provider may define here the conditions that determine the transition from one phase to another (time, achievements, resources, etc.)

The staging can be represented by a table such as the following:

	Service A	Service B	Service C
Order	Phase I	Phase III	...
Provisioning	Phase II	Phase I	...
Service Delivery	Phase III
Mediation	Phase I
Rating	Phase II
Billing	Phase II

Table 1 Deployment Strategy

And so forth.

In addition, requirements for KPIs and reconciliation rules should be represented with separation to the various phases. As the priorities of the KPI implementation has to do with a deep business acquaintance with the Service Provider's internal goals and processes, it would make sense to ask the vendors to state the number of KPIs they can create at each stage, but not for the named list of these KPIs.

7 Administrative Appendix

This Appendix provides additional background material about the TM Forum and this document. In general, the sections may be included or omitted as desired, however a Document History must always be included.

7.1 About this document

GB941c is an addendum to the GB941 Revenue Assurance Guide Book.

7.2 Document History

7.2.1 Version History

Version Number	Date Modified	Modified by:	Description of changes
0.1	DD/MMM/YY	Doron Avidar	Initial draft
0.2		Assaf Landau	Updates, corrections and additions
0.3	23/07/2008	Assaf Landau	Formatted to current template
0.4	03/09/2008	Gadi Solotorevsky	Corrected Acknowledgements
0.5	11/11/2008	D.F. Burkett	Edits in preparation for Approval Committee review
0.6	23/Jan/2009	Alicja Kawecki	Minor corrections
0.7	20/Nov/2009	Alicja Kawecki	Updated cover page, notice, footer, and version history to reflect TM Forum Approved status
0.8	10/May/2011	Alicja Kawecki	Removed "Release 1.2" from cover page per CD to align with R3.0 guidelines
0.9	26/February/2012	Gadi Solotorevsky	Updated to use Framework nomenclature
0.10	13/April/2012	Alicja Kawecki	Notice, minor formatting and cosmetic corrections prior to web posting and Member

			Evaluation
--	--	--	------------

7.2.2 Release History

<This section records the changes between this and the previous Official document release>

Release Number	Date Modified	Modified by:	Description of changes
	DD/MMM/YY	<<name>>	Description e.g. first issue of document
3.6	26/February/2012	Gadi Solotorevsky	Updated to use Frameworkx nomenclature

7.3 Acknowledgments

This document was prepared by the members of the TM Forum Revenue Assurance team and is a genuinely collaborative effort. The TM Forum would like to thank the following people for contributing their time and expertise to the production of this document.

Assaf Landau, Editor, cVidya

Gadi Solotorevsky, Team leader, cVidya

Edwin Hanke, BT

Kenny Dickson, BT

Doron Avidar, cVidya

Dmitry Kirsanov, Ernst & Young (CIS) B.V.

Elena Ustyugova, Ernst & Young (CIS) B.V.

B.J. Taylor, Stevens Institute

Vinoo Jacob, Subex Azure Ltd.

Kathryn Dunham, The Billing College

Debbie Burkett, TM Forum