Revenue Assurance Overview

TR131

Version 2.3

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

This document contains the TM Forum's technical overview of revenue assurance. The original technical overview was written in 2004 and broke new ground by being the first cross-industry collaboration to achieve a consensus definition of the purpose and reasons for revenue assurance. This version contains a number of significant updates that reflect the evolution in the subject that has taken place since. This overview explains what revenue assurance is, its scope and the reasons why it is needed. The TM Forum has also produced a companion publication, the GB941 Guidebook. The GB941 guidebook gives practical advice on how to tackle the challenges of revenue assurance. This publication retains a strict focus on the reasons why revenue assurance is needed.

The overview begins at the beginning, by identifying the forces that give rise to leakage within modern electronic communications businesses, and have hence created a need for a discipline dedicated to revenue assurance. To avoid confusion, the term "revenue assurance" is given an unambiguous definition as the combination of data quality and process improvement methods to deliver improved financial returns without stimulating an increase in sales. This definition is based on actual observation of how the phrase is used in practice, and is supported by an internet survey which has been updated for this second edition of the overview. Errors occur due to the complexity of modern electronic communications businesses. The combination of rapid change necessary to remain competitive with different technical challenges in correctly implementing transactional data flows from point of sale to point of billing, charging, accounting and cash collection across multiple product types and pricing models leads to an increased propensity for error. These errors may directly impact the bottom line through lost revenues and increased costs, or indirectly impact the bottom line through customer dissatisfaction if they have been incorrectly billed. Some errors may be particularly damaging because they remain undetected for prolonged periods of time. It is possible to identify factors that lead to discrepant data in typical voice and data products, but the exact approach undertaken by revenue assurance will always need to be tailored to the circumstances of the specific business.

Calculating the value added by revenue assurance in general, and by individual revenue assurance activities in particular, is problematic. We have included the "justification" of revenue assurance as it seeks to prevent problems before they occur, or resolve them as quickly as possible after they occur. This limits the data available to draw inferences. Nevertheless, the overwhelming conclusion from practice is that revenue assurance generates a positive ROI for businesses that have adopted the discipline. To give a degree of consistency and precision to the calculation of revenue assurance benefits, a "drip tray" model is described which expands upon the metaphor of revenue leakage and discusses the ways to quantify and attribute the value of either stopping leaks before they occur or catching leaks and recovering the value that would otherwise be lost.

There are many connections between revenue assurance and laws and regulations intended to protect the interests of shareholders and customers. The integrity of charging for products and services is vital for the delivery of reliable accounts and also for ensuring customers are not overcharged. In contrast, service providers are at risk of fraud from a number of quarters. The relationship and boundaries between

revenue assurance and fraud detection and prevention needs to be explored and determined in each service provider, in order to avoid gaps that may be exploited by the fraudster.

When establishing the priorities for revenue assurance in each business, it is also worth identifying the strategic approach. The three complementary layers of the Proactive-Active-Reactive (PAR) strategy gives the best safeguard of assurance, though in establishing revenue assurance for the first time it will likely be necessary to put initial efforts into a reactive approach and then seek to gradually augment this with active and proactive controls. In addition there is a decision to be made about striking the correct balance between data-oriented and process-oriented techniques in each business. However, the two techniques are ultimately complementary, and a business with a mature approach to revenue assurance will seek to combine the two to get the best overall results.

1. Introduction

1.1. Document Structure

This document has four major parts: a problem statement, a justification case study, a solutions analysis and a mapping of the revenue assurance discipline onto the eTOM and SID. The document is structured as:

Section 1 Executive Summary

Section 2 **The Problem**: Identifies the issue of Revenue Assurance as a vital aspect of a service provider's business process.

Section 3 **Justifications**: Describes an actual cost benefit analysis of a revenue assurance study undertaken by a service provider. It seeks to highlight how and why such justifications can be made.

Section 4 RA and Regulation

Section 5 RA and Fraud

Section 6 **Solution Approaches**: Identifies areas, methods and lifecycles encountered when tackling revenue assurance.

1.1.1. Appendices

Appendix A Terminology, acronyms and abbreviations

Appendix B References

Appendix C Worked Examples

Appendix D Draft Vendor Standards

Administrative Appendix provides document revision history, acknowledgements for work completed and information about the TM Forum.

2. The Problem

Revenue Assurance evolved from independent efforts to resolve specific problems in a variety of communication providers. Although specific, the problems all related to lost revenues and reduced profitability as a consequence of process flaws. Over time it became increasingly apparent that the seemingly disparate problems of different communication providers shared many similarities. Typically all the problems stemmed from the same kinds of root cause. It also became apparent that without a conscious ongoing effort to tackle the root causes, any communications provider should expect to suffer significant revenue loss.

During the rapid business expansion in the 1990s, some communications providers experienced difficulty in keeping up with the evolution of back office systems. Increased competition and time-to-market pressures forced many to cut process corners and make temporary fixes to legacy systems to accommodate emerging market opportunities. Over time the back office evolved into a highly complex environment characterized by largely disparate systems, manual interventions and out-of-sync databases. Back-office support requires cross-departmental activities and many of those were never fully automated. Frequently automated systems were supported by entirely manual processes, increasing the risk of processing bottlenecks and errors. This outcome created significant potential obstacles for providers wanting to lower cost structures, integrate automated processes and optimize network utilization. Telecom technology is developing continuously. Radical and rapid industry changes, though competition and dynamism, and un-predicted market needs ensure that the speed of change remains high and time to market low. The market demands new services, which require mass deployment and demand more systems and processes to manage them efficiently.

These three factors - the economy slowdown, the continuously developing technologies and demand for new services - forced telecom service providers to reevaluate their business focus in order to survive the downturn.

The large-scale service providers realized that in order to carry on in this period of time and remain profitable, they had to examine their internal business processes, and restructure their organization according to the new business targets and priorities. A new discipline, organizational goal, and even an organizational unit emerged as a reaction: Revenue Assurance.

Revenue Assurance has become a significant "soft spot" within service providers, who significantly empower internal Revenue Assurance departments to further accelerate efforts to identify and fix malfunctioned processes in their existing networks, OSS/BSS architecture, and business-processes.

Revenue Assurance has experienced a fundamental transformation. It has turned from a temporary tactical fix into a holistic process for optimizing the usage of existing service providers' assets to maximize their revenues and profits. Although industry expansion and downturn highlighted the need for Revenue Assurance, mature businesses recognize that the dangers of revenue loss persist even in the best of circumstances.

The Subex Azure Report from September 17, 2007 reports leakage in the global telecom industry increased from 12.1% to 13.6%. While many have made great strides in the area of Revenue Assurance, the report attributes most of the increase in

leakage to external, internal and other types of fraud. The leakage in this area grew from 2.9% to 4.5% with more emphasis in the mobile telecom industry. Further studies revealed that smaller telecom companies (those with 100,000-1,000,000 customers) suffer the highest losses from leakage.

Revenue leakage is considered a cost of doing business in the telecom industry. Revenues are lost due to several reasons such as network provisioning, mediation and CDR errors, billing and interconnect inconsistencies, loss of data and corrupted files, fragmented support systems and manual or fuzzy business processes. When a product increases in its importance and popularity, margin leakage also increases. The main question for any business is how much leakage is acceptable and how to improve the operations and systems in such a way that minimizes those leakages.

Effective RA process must ensure the data integrity and synchronization across all the disparate systems and the network itself, in order to ensure operational and financial efficiency. Such process provide analysis of the relationship between network resources, services, customers, and generated revenue, and will enable the service provider to detect revenue leakage (e.g. un-billed customers, mis-billed customers), stranded assets, and operational inefficiencies.

In addition, a process management layer is required to allow RA managers and Financial Directors to enjoy the benefits of their achievements, track the revenue leakage identification, quantification and reclamation processes and easily report the results. A big challenge for RA and communications business in general is to gradually move the focus of process management away from resolving and reacting to problems that repeatedly occur, and towards the prevention of problems before they occur.

Currently there is no industry accepted cross processes Revenue Assurance methodology which will enable the deployment of an effective Revenue Assurance processes across the various activities, processes, systems and network technologies.

2.2. Definition of Revenue Assurance

The Team has adopted the definition for revenue assurance as “Data quality and process improvement methods that improve profits, revenues and cash flows without influencing demand.”

The basis of this definition is discussed below.

Until year 2004 there was a degree of confusion about the scope of revenue assurance. Many different parties have suggested their own definitions for revenue assurance, and these frequently contradict each other. There are several reasons for this confusion:

Revenue assurance emerged as a reaction to specific business problems in individual businesses; hence the usage of the phrase tends to reflect differing objectives and experiences of each business;

Revenue assurance has a potentially broad remit but in practice revenue assurance evolves within businesses from a variety of different organizational units including Finance Controls, Network Operations, Billing and Internal Audit, each of which bring a differing sense of perspective and priorities to the same subject area;

By 2004 term has entered the catalogue of industry "buzz words", hence it is sometimes over-used or used indiscriminately; and

Until 2004 no organization has emerged as a credible industry leader for revenue assurance practitioners.

The definition deliberately avoids a strict specification of what are the boundaries to the scope of Revenue Assurance. Whilst all seem to agree that the main driver of Revenue Assurance is an enhancement of financial performance, there is considerable disagreement about which financial KPIs are relevant. For this reason, the definition has focused on the common methods employed in Revenue Assurance, leaving the choice of relevant financial metrics open so they can be tailored to different business models. In this way, a "stepped" model of activities is enabled, starting with those where there is a very high degree of consensus that they belong within the scope, but able to move through and explore the relationships with activities that may considered as secondary or subsequent developments of a maturing Revenue Assurance discipline within a business, or alternatively are thought of as related activities but which remain outside of the scope of a strictly defined Revenue Assurance.

2.3. Highlighting the Challenges

The specific problems dealt with by Revenue Assurance are often particular to a kind of technology, product, and business model. However, Revenue Assurance has emerged as a recognizable discipline applicable to all communications providers because the root causes of many the problems they face tend to be the same. This section seeks to summarize collective industry experience of what are the most common factors giving rise to the need for Revenue Assurance.

2.3.1. The Core Challenges as Derived from Telephony

Revenue Assurance largely emerged as a response to problems within businesses focused on telephony. The bulk of RA practitioner work continues to relate to telephony but the boundaries of scope have since expanded to the many other services offered by modern electronic communications firms. There is no defined limit to what kinds of services might be subject to RA; ambitious practitioners see value in translating the telecommunications experience to other business sectors. However, telephony continues to be the best-explored example of the challenges addressed by RA in general.

Given the complexity of a modern electronic communications provider's operations, effective RA strategies must rely on technology, people and processes to accomplish its goals. RA programs span complex network technologies, sophisticated IT infrastructures and complicated business processes. Identifying data discrepancies and prioritizing the correction efforts is a daunting task, and can only be carried out with software support. The challenge of RA is to:

- Identify where there is the potential for problems that will damage the bottom line;
- Implement mechanisms to detect and measure the severity of actual problems;
- Continually detect integrity problems in a large, complex and constantly changing body of multi-sourced data;

- Prioritize those problems according to their impact on the business;
- Correct the highest priority problems quickly;
- Prevent historic problems from recurring;
- Anticipate the potential for future problems; and
- Implement improvements to prevent future problems.

In order to address an effective RA approach, it is required to see the business operations as a whole, with the network and the engineering systems in one edge and billing and accounting systems on the other edge. . From a RA point of view, managers are required to define and implement revenue assurance tools, methods and metrics that allow seeing the network infrastructure, its elements and services from a business and cost effective perspective. Today's networks are required to be seen from a profitability standpoint, focusing on the costs and revenues the network services yield.

At the other edge of the service provider's infrastructure stand the billing systems. Billing is a complex set of processes and integrated systems that begin with the collection and accounting of call detailed records, its correct rating, billing and discounting, invoice generation and verification of the payment collection.

A traditional approach to revenue assurance leads towards performing an audit process once a year and to try and identify the problems, quantify them and create or change existing procedures. The cost of such method is that there is a huge delay between the occurrences of a revenue leak to the time it is fixed, which means that the money lost cannot be reclaimed. When using an automated ongoing approach, the continuous checks and audits performed enable the carrier to react immediately to block the leak e.g. if an error occurred in the billing process, and if identified before the invoices were issued, a corrective action can be taken without the customer being aware of it.

RA systems should be designed to support data acquisitions from network elements, provisioning systems, mediation platforms, billing systems, etc. without being obtrusive to business operations and mission-critical support systems. The following picture depicts Yankee Group’s key characteristics of revenue assurance functions and processes.

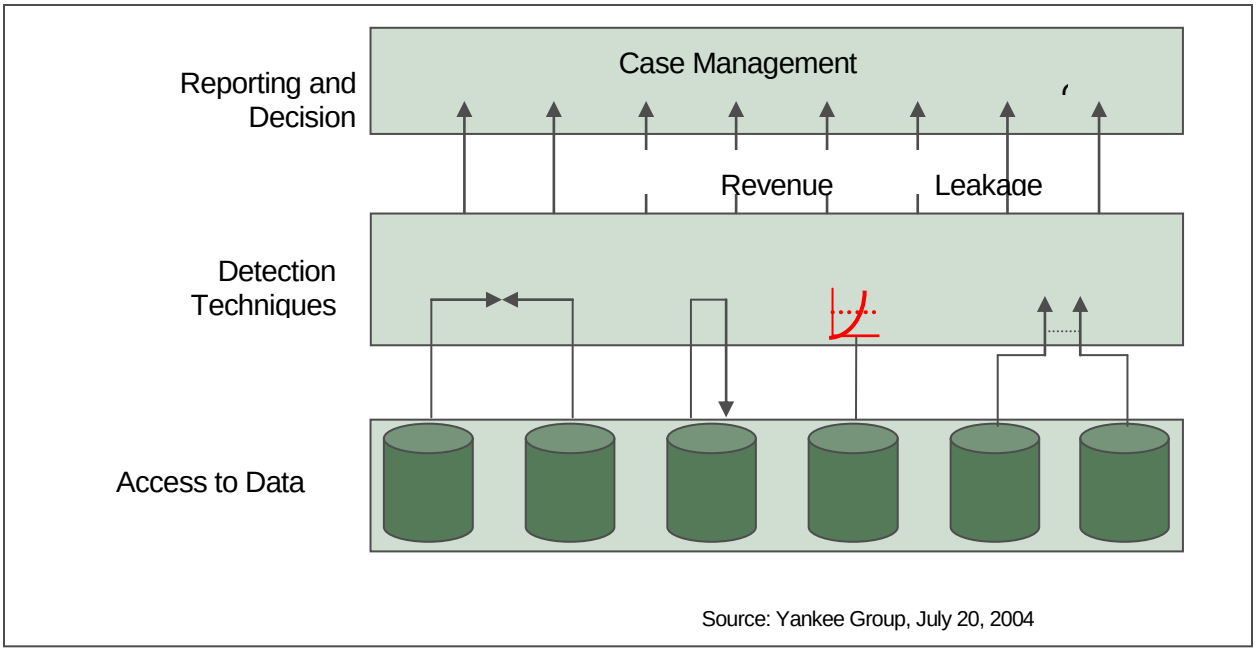


Figure 2-1 Characteristics of Revenue Assurance Detection and Monitoring

Comprehensive RA is a long-range strategic objective that should be approached incrementally, addressing the low hanging fruit first. The scope and depth of RA initiatives are largely dependent on the organizational readiness of businesses to execute such programs as well as the maturity of the communications markets they serve. As communications providers mature in their RA efforts and accumulate experience, they tend to move from a reactive mode to proactive methods. This is normally manifest as follows:

- The ability to identify the potential for problems improves, leading to an improved understanding of the scope of Revenue Assurance and spawning activities to address causes of leakage that had gone unnoticed in previous waves of deployment;
- Mechanisms to detect and measure the severity of actual problems become more sophisticated, robust, precise and comprehensive.
- The time taken to exercise the feedback loop from problem occurrence, through detection and prioritization to resolution shortens.
- Prioritization of problems becomes more sophisticated and better reflects the overall business priorities.
- Root cause analysis of problems identified is conducted more thoroughly and intelligently, and fixes shift from operational through tactical to strategic, reducing the number of problems that recur.
- Knowledge is retained, the awareness of Revenue Assurance improves across the business and hence the ability to anticipate the potential for future problems increases.
- Business buy-in for improvements to prevent future problems is attained more readily, resistance to activities to stimulate continuous improvement recedes, and

the need to build-in integrity is automatically recognized during the consideration of any major process or system change.

While detecting data discrepancies is the starting point for RA in most providers, to realize benefits it is necessary to correct the errors found and prevent them from recurring. Errors may be trivial, or they may be difficult and challenging to deal with because of the interdependencies of multiple systems and processes involved in enabling the service. Once data discrepancies are detected, a series of activities may be required to pinpoint how, what, where and when to correct the error.

One method of dealing with revenue assurance issues is to fix them at the event, or "ticket" level, i.e. to correct each event or each discrepancy and reclaim the lost revenues. This approach brings results, but is not necessarily the most efficient one, since hundreds of thousands of cases should be maintained all the time. Buy implementing intelligent techniques into the revenue assurance process, the root cause of the discrepancies can be identified and then fixed at once e.g. when a large group of customers are configured in the network for a bronze service, while all of them ordered a platinum service, it is quite clear that somewhere in the provisioning processes a faulty process or system is generating the leakages. By examining and analyzing the provisioning processes, the flow of information between the systems and the configuration of the various systems involved in this process the root cause can be detected. In our example an activation system might have been wrongly configured to translate a platinum service into a set of bronze service activation tasks.

A RA methodology is not only limited to the discovery, estimation, control and minimization of the exposure points in the revenue chain where a possibility of revenue leakage exists. The holy grail of RA managers is to compose a holistic set of routines, controls and metrics designed to maximize revenues, increase profitability and strengthen corporate integrity.

Some communications providers find they get "stuck" at a certain level of RA maturity. They may conduct one-off audits year after year; each time successfully recovering revenue that would otherwise have been lost, but fail to move towards timelier automated monitoring that would recover a higher proportion of the revenue at risk. They may have automated monitoring and a robust mechanism for fixing the errors found, but fail to identify or act on the root causes of errors so that the same number of errors are found by monitoring each and every month, when it would have been more efficient to take steps to prevent errors recurring. A commitment to continuous improvement is the lynchpin of successful RA. At the time of writing, no business has claimed to have been so successful at RA that there is no longer a commercial incentive to look for new ways to further reduce their leakage. With communications providers continuing along an evolutionary path of more complicated technology, more sophisticated charging models, more advanced products, shortening time to market and all with leaner operations and fewer staff, it may be unrealistic to suppose that RA will ever fully catch up with the latest causes of leakage. This places the onus on RA to act as the conscience of the business, remembering past mistakes and continually finding a way to anticipate and mitigate future risks.

2.3.2. Challenges in IP and Data

The successful penetration of broadband services happened so rapidly that the entire data services market suffered a focus shift. Even traditional services such as Frame Relay, leased lines and ATM connections are included in this technology evolution.

IP and Data Services are seeing a strong growth in demand for these services. As reported in PCWorld magazine in February 2008, expected growth should reach worldwide US$4.6 trillion in 2011.

With the demand, these services will impact directly on back office activities and engineering tasks that begin in the ordering process through the service provisioning and finishing in the accurate invoicing. These tasks involve cross-departmental activities many of those not fully automated or even handled entirely manually. The entire scenario becomes even more complex if we consider the fact that service changes, upgrades and cancellations are common and rollback activities have to be done. Any minor failure in the system interfaces, errors in the data or probable death-end paths in the business procedures causes not only delays in the business process as a first step but it opens the way to system discrepancies and revenue leakage.

Billing is typically broken into separate systems according to customer segments (corporate and residential customers) or according to the lines of business (voice, IP etc.). In addition, enterprise and other external demands are also leveraging the complexity required to support complex account hierarchies. These systems originally implemented to address billing of voice services, have been modified to cope with the dynamism of data and IP services, which makes the billing process even more complicated. Those changes in the system and their interface with others have to be aligned with the service provider's business processes; otherwise it causes as a result exposure of unattended areas and leakage of unnecessary costs and non-recovered revenues.

Data and IP services also contribute to the evolution of the new concept of “content services” although those types of services are known also in the voice related world as SMS services or Premium numbers, the access to those services was controlled mainly by the telecommunication company. In the IP environment the content becomes a separate “product” with its own life, not necessarily related to the communication which provider, which assists in delivering the content to the end customer, but in no means is the only channel available for the customer.

This separation expedites the introduction of new business models where this separation was translated to partnership agreements between the bearer carrier (either fixed or mobile), the content provider and sometimes the content aggregation service. This required enhancing the inter carrier types of agreements into a new level of partners management, with business agreements between the communication carrier and the content providers.

In the Service provider system environment, most of the provider's systems from the network and operations side as of the billing and customer care counterparts are key elements and important data sources for Revenue Assurance activities; information derived from every system of the OSS and BSS infrastructure is relevant to be included in the RA methodology. The introduction of systems and business

procedures that support IP and data services and the increasingly complex logic that exists between them creates, as a result, a much more challenging arena.

Broadband and data services differ in many aspects from traditional voice and other Service provider service offerings; those services have a different nature and level of complexity in business processes and the OSS and BSS infrastructure that supports them. Similarly, RA methodologies for switched networks do not properly fit into the IP and Data services spectrum. Data service networks require a different approach.

Even though many of the services are charged flat, and not usage based as in telephony, an important question to answer in data services fields is; is the service configured the same service that it is billed? The roots of this question points to the fact that the integration between billing and provisioning is loose since there is no obvious connection between the business and the network domains. It is also important to consider that standards for IP-based events are not generally accepted.

Revenue assurance techniques developed in the voice world do not fit into the data services world, since they are not designed to synchronize billing information with the network's complex dynamic topology. The best way to assure a broadband service, from a business-wise and revenue assurance perspective is by having a single and common view of the service, the network and the subscribers.

Provisioned IP and data services are not limited to a single network technology; they may cross several network architectures and protocols, based on different technologies, network elements and management systems. From a network management perspective, it is organized in network layers, which are operated by different skilled personnel and dedicated systems. Consider as an example an enterprise with several buildings and remote users connected to the corporate network via VPN access. The combination of network technologies is many (broadband, leased lines, ATM connections, etc.). From a revenue assurance perspective, the service is a logical business entity that relies on several technologies that should not be divided.

At today's carrier environment the systems supporting the business, operation and network aspects are different not only in the processes they carry but also in their customer modeling, service and products entities (a customer to the network is not necessarily the customer to the billing, resource using entities are not equal to the legally contracted entities). Although some effort has been made to create a cross carrier product catalogue, in general it is correct to state that those initiatives did not fulfill requirements, mainly because the creation of a catalogue detailed enough to serve those processes is extremely complicated. The RA methodology requires that information derived from marketing supporting systems, has to be uniquely correlated with its network counterpart, giving as a result a cross-domain entity that possess the completeness required for the RA methodology.

To cope with the dynamism of the changes in the IP and data scenario, the RA methodology shall consider business logic time parameters and time offsets that are inherent in the operational systems. Synchronizing data from different sources is not enough, it may even result confusing due the fact that data is not time-aligned all over the organization. Synchronization issues and time delays in business processes and data updating cannot be ignored.

Considering the facts that data and IP services provisioning is a much more complex process that involves many systems, and since many of those services does not rely on continuous usage processing, in many cases once a service was established the notification process between the systems is the only event that creates a connection between the OSS and the BSS systems. Once this notification fails or for some reason deliver the wrong information, no process is in charge to make sure that the information is synchronized (e.g. no CDR is moving along the revenue chain and can indicate that something is wrong).

3. Justification

3.1. Project Method

Assumptions have been stated explicitly in order to aid their analysis. As far as reasonably possible, analysis is always based on empirical data and not hypothetical, anecdotal or "common sense" arguments. Comparative data from differing sources has been used to either corroborate findings or highlight discrepancies that need further investigation. The project method included a holistic view of costs and benefits. Costs and benefits to both supplier and customer are considered. Consumer protection is taken to be a motivating factor in implementing accuracy controls, but in general no ethical dimension has been included in the analysis. The project objectively analyzed the best information available on the economics of the scheme without any moral bias.

Most of the empirical data was obtained from actual business activities, though publicly available sources were also used. The service provider that conducted the project should not be considered any more representative than any other. To broaden the analysis, data relating to other businesses has been included wherever possible. As such, the project characterized an alternative service provider, called Service provider X, in order to exemplify how accuracy and compliance may vary in practice. Service provider X is not based on any single company, but is drawn from real life examples. The contrast helps to illustrate differences in the way assurance may be undertaken and the benefits that might be realized.

3.1.1. A Project to Analyze Costs and Benefits

The analysis given here is the output of a specific project to assess costs and benefits at a service provider. The basis of the conclusions has been anonymized and generalized to aid in the comparison amongst communications providers.

3.1.2. Project Remit

This chapter represents the conclusions of a project to analyze the net benefits that accrue from improvements in the completeness, accuracy and validity of metering and billing as driven by

- Commercially driven activities; and
- Incremental activities to deliver regulatory obligations.

The potential economic benefits of improved conversion of amounts billed to cash collected; Reductions in cost; Better utilization of assets; and Increased sales because of improved realization of sales opportunities; were excluded from scope. Completeness, accuracy and validity of metering and billing may be considered a core aspect of revenue assurance. Limiting the scope of the analysis helped to reduce complexity.

3.1.3. Notation and Interpretation

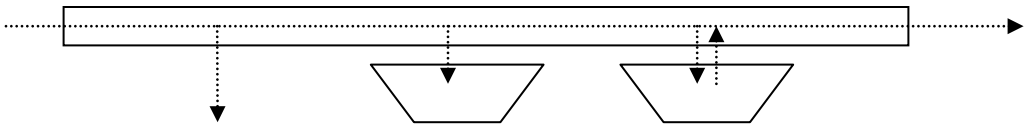
Definitions of terms are labeled with a number prefixed by "D".

Hypotheses and assumptions are labeled with a number prefixed by "H".

Definitions and hypotheses are numbered in a sequence that reflects the order in which they were formally accepted by the project.

Negations of hypotheses and assumptions are labeled "NH" and have the corresponding number to the hypothesis they negate.

The word "accuracy" is used variously to collectively refer to what is more properly described by the phrase "completeness, accuracy and validity", and also in its strict sense. Where used in the former sense, it will always be prefixed with the words

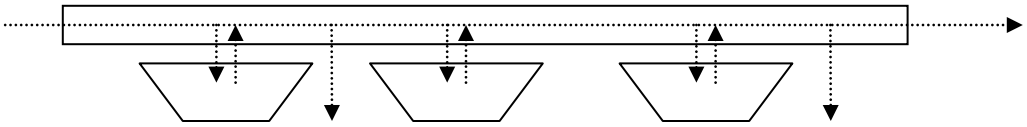


"end-to-end" to avoid confusion whilst aiding readability.

3.2. "Drip-Tray" Model of Accuracy Controls

A common metaphor for describing the effect of errors in processing charges is that of "leakage". The metaphor is apt because the loss of water from a pipe exhibits similar properties to the loss or corruption of data as it is processed from one system to the next. The amount of water lost by the pipe could be measured by comparing what goes in to what comes out. Though simplistic, the comparison of ins and outs lies at the heart of activities intended to monitor, diagnose, prevent and measure the extent of error. In assessing cost-effectiveness and benefits obtained from such activities, it may be tempting to view such activities as "drip trays" that capture errors and so capture or prevent "leakage". Where there is no drip tray, the leakage continues unabated.

Figure 3-1 Leakage and Drip Trays



The idea of a drip tray can be further refined. Some drip trays will lead to the capture of errors, some will lead to their capture and resolution. Capturing errors without resolution means that errors are measured but still take place. Capturing and resolving errors means measurement of errors that would have gone unresolved without the drip tray. A drip tray that captures errors without leading to resolution has a cost, but no clear attributable economic benefit. The ideas of capture and resolution might be represented diagrammatically as follows.

Figure 3-2 Uncaptured, Captured and Resolved Errors

The costs and benefits of each drip tray should hence be quantifiable as follows:

-
- benefits of the drip tray activity are measured by the improvement in the ratio of in : out for the whole pipe
- set-up costs of the drip tray activity are amortized over its useful life
- ongoing costs of running the drip tray activity are related to the period in which they are incurred.
- So, the net benefits of any activity over its life would be the benefits as measured in terms of improved in/out ratio less the costs to set-up and operate the activity.

The project concluded that most practitioners, in some cases unwittingly, perceived the costs and benefits of accuracy using a model equivalent to the drip tray model. In effect, they recognized that such activities added value, but that value is measured in terms of the overall improvement in results for the end-to-end process. The ironic implication is that costs can be associated in a straightforward way with the individual activity, but that the benefits are not. As a result the difficulty in evaluating and enabling the best end-to-end results for all parties is equivalent to any problem where individuals must be motivated to meet the cost of attaining a common or public good.

3.2.1. Weaknesses of the Drip Tray Model

Although the drip tray model of evaluating costs and benefits conformed to the expectations of those involved in instigating and arguing for the merits of accuracy control activities, there was general recognition of a number of flaws in using this model. Discussion of the flaws was hampered by:

- a lack of practical examples drawn from the real-world that would have been of use to illustrate the ideas expressed;
- a poor understanding of how to perform a cost benefit analysis for a drip tray activity because of a lack of practical experience; and
- novelty as a topic of discussion.
- Some respondents to the project noted that
    -
    - although costs and benefits were frequently addressed in discussions, presentations and the like, these tended to be specific to individual projects; and
    - there was a scarcity of systematic and consistent methodical analysis of how to assess costs and benefits in general or for projects where this would be difficult.;

No alternative model had been proposed to the knowledge of the project. As appears to be the issue with similar problems involving the public goods, some of the difficulties in using the drip tray model were related to the fact that cost-benefit analyses in general tend to be used to conclude whether an incremental activity generates a net *positive* contribution; but the benefit of this kind of activity is understood in terms of *avoiding something undesirable*.

A metaphor for the organizational ill of charging error is the public ill of pollution. Some pollution may be inevitable as a consequence of the desirable activities of industrial production or transport, but harm is caused to the public in relation to the total quantity of pollution. An increased likelihood of error is a natural consequence of change and development of new products and technologies but the business suffers overall in relation to the extent of unresolved error. A drip tray activity prevents a negative contribution in the way a catalytic converter prevents pollution. On a simple level, preventing a "loss" may be seen as equivalent to generating a benefit, but this obscures complications that hinder use of the approach in real-life analyses of costs and benefits.

3.2.2. Weaknesses in Determining the In/Out Ratio

In a water pipe, an amount of water enters one end, and an amount exits the other. The ratio of volume in to volume out determines precisely how much is lost during transmission. This is true because of two properties of piping water that do not apply to the chain of processing charging data. All water is equivalent; any given molecule is a perfect substitute for any other. All transmission problems in a water pipe occur one way only. The assumption is that water may leak, but that it does not enter from another source.

Unlike water molecules, any datum necessary to charge a customer is unique and cannot be substituted. From the point of view of the business, it is tempting to think of data as a general flow, but that obscures the fact the correctness of each individual datum is essential for charges to be correct. Corrupting data has much the same implication as stopping the flow of data in that the *correct* charge will not flow through to the customer. For the correct charge to be rendered processing has to be correct from beginning to end.

From an overall perspective there is a temptation to judge the severity of the error by the net effect on the value of the bill. This may obscure the fact that the severity of the outcome may bear no relationship to the severity of the flaw that lead to the error. The size of an identified error may not be a good indicator of the seriousness of the risk of error. For example, if a tariff rate is manually keyed to a system, and a typographical mistake goes unchecked, the nature of the mistake is the same whether it alters the most significant or least significant digit in the number.

In a water pipe, some of the water that enters one end may not leave the other because of leaks along the way. We might say that the water output from the desired end is incomplete. In end-to-end accuracy of charging there are three kinds of errors:

- an error of completeness is due to loss of data along the way;
- an error of validity is due to additional bogus data being introduced along the way; and
- an accuracy error (in the strict sense) is not due to valid data being lost or invalid data being introduced but a corruption of what was valid data.

The consequence of the above is that, unlike the water pipe, errors in charging may occur in two directions:

- an error of completeness is in the customer's favor because there is a failure to render what would have been a genuine charge;

- an error of validity is in the supplier's favor because a charge is rendered that should not have been;
- an accuracy error may be in either direction.

In determining the actual extent of error, errors that net should not be netted. This means that a single in/out ratio is not possible. At the very least a separate ratio is needed for errors in each separate direction.

It follows from all of the above that calculating the value of the input is no simple matter. Measuring the value of the input, in monetary terms, is exactly what the metering and billing process chain is designed to do. Calculating and delivering the end charge is the very purpose of the processing chain that is subject to scrutiny. It follows that the task of correctly calculating the value of inputs in order to gauge the extent of errors in a process, or the benefits of drip trays capturing errors in a process, will be as complicated as the process under scrutiny. It may be possible to devise checksums and proofs in total and the purpose of these is to expend very little effort in obtaining a high degree of confidence. These will not, however, guarantee perfect accuracy, as there will always be some risk of errors or combinations of errors that are not identified using techniques like these.

Where an error takes place in the processing chain will determine how many processing steps still need to be performed in order to definitively value the error. This means that it is easier to put a precise value to errors that occur late in the chain of processing. Though it is easier to put a value to such errors that does not mean these errors are of greater value. Not valuing an error that occurs in the chain of processing may lead to confusion if these errors are considered to be of no or negligible value. There is an accounting principle that the difficulty of estimating a value is unrelated to what that value is. This means difficulty in evaluating an error should not be considered a good reason to treat its value as nil.

3.2.3. Attributing Benefit to Each Drip-Tray

Benefit was considered the improvement in the in/out ratio, but the improvement will relate to many factors, including:

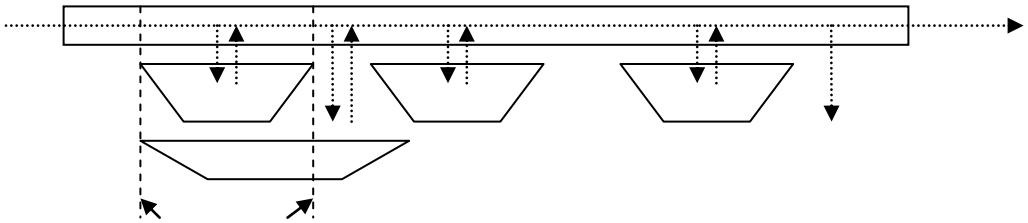
- changes over time in the overall volumes and value of data flow; and
- the relationship between the drip tray and other drip trays

The former should not be difficult to understand, as the important thing is to understand not just the absolute values billed but also the types of charges affected by an error and so the proportion of errors prevented or corrected by a drip tray.

A situation where multiple drip trays could potentially resolve the same error is more difficult to evaluate. It may seem obvious to credit the benefits to the activity that "actually" captures the problem and leads to its resolution. However, taking this approach to its logical conclusion implies there are no benefits from having redundancy. In particular, this would imply that the economically rational course of action would be to avoid intersections in the coverage of drip trays, but intersection may help to identify weaknesses or limitations in one or other drip tray that might not otherwise come to light.

It is possible to implement drip trays with wider or narrower span, so that a wide-span drip tray may represent some overlap with another narrower-span drip tray. For

example, during the development of a product, a formal review of the integrity of the charging/billing process would be a very wide-span drip tray, designed to proactively identify issues and potential issues before the product goes live. However, it would



be unrealistic to assume that such a control would always capture every error, so there is every reason to also implement adequate monitoring processes when the product goes live. By definition, the two drip tray activities of development review and live monitoring will overlap in that either might equally well identify some kinds of error. The overlap gives confidence that errors missed by the earlier activity may still eventually be caught. The overlap also means that the individual net benefits attributed to either or both drip tray activities are diminished.

Overlaps may make it difficult to predict the long-term value of a drip tray. For example, if an overlapping drip tray highlights a weakness in another drip tray, circumstances will dictate whether it is more cost-effective to:

- resolve the identified weakness in the first drip tray; or
- leave the weakness in the first drip tray and continue to rely on the overlapping second drip tray to capture errors.

Figure 3-3 Overlapping drip trays

3.2.4. Determining the Lifetime of Benefits Arising From a Drip Tray Activity

From an economic point of view, the benefits of an activity relate to the improvement in the in/out ratio. However the ascribable "lifetime" of benefits may not be clear. For example, consider a monitoring activity that captures an error resulting from a bug. By capturing the error, the activity leads to the identification of the bug. The bug is fixed as a consequence, and no more errors take place. Does the benefit lifetime of the activity run:

- until the bug is fixed, because the there are no more errors of that type after the bug is fixed? or
- for as long as the process which was fixed is used in practice, because the fix has eliminated errors, and so delivered the benefits of a bug-free process for as long as the process is in effect? or
- for some time between the time of fix and the time the fixed process ends, because if the errors were not identified by the activity, they would still probably be identified at some time as a result of another activity?

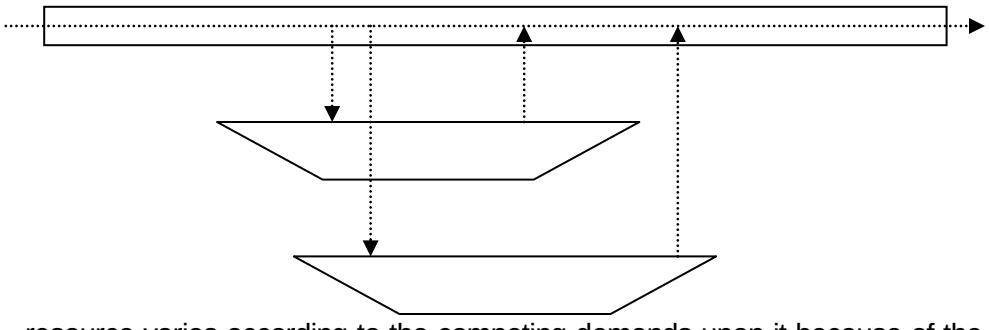
Figure 3-4 Overlaps mitigate weaknesses of drip trays

There appears to be no good basis to consider any of these three theoretical lifetimes as inherently superior. If the problem will never be identified without the drip tray, there is an argument for ascribing the benefit to the drip tray indefinitely. Any judgment as to what would have happened if the problem had not been found using the drip tray would always be essentially speculative. This may suggest that the best approach is to ascribe benefit only until the bug is fixed. This approach would only attribute the most conservative and least disputable benefits to the drip tray, but in so doing ascribes no ongoing value to the benefit incurred by prompting a fix.

3.2.5. Determining the Benefits of Capturing Errors without Resolution

It was stated above that there are no attributable benefits to a drip tray activity that captures errors that are not resolved. This makes sense because the conception of benefit was an improvement in the in/out ratio. However, we can conceive of a drip tray that is used to "trigger" resolutions according to a step function: only errors of a certain magnitude are resolved. In practice, the trigger point may not be well defined, which further complicates any analysis of the benefits arising. Many real monitoring activities can be thought of this way. This is true because setting the trigger point for resolution may be thought of as an academic activity. In reality, management will monitor performance and deploy available resources according to priorities, meaning that the trigger point for resolving an error will vary according to fluctuations in supply and demand of limited resources. In such circumstances, it is unlikely that sufficient analysis will be performed to get a robust assessment of the costs and benefits of the monitoring activity.

A further complication in such cases is that it will take some resource to resolve an error once the drip tray has triggered resolution. Thus the net benefits are the improvement in the in/out ratio less the costs of the drip tray and the costs of the resource used for the resolution. From the above, it follows that the cost of the



resource varies according to the competing demands upon it because of the varying costs of opportunities foregone elsewhere.

For these reasons, it is unlikely that economic benefit will be attributed to an activity intended to capture errors but which only leads to a resolution on a sporadic basis.

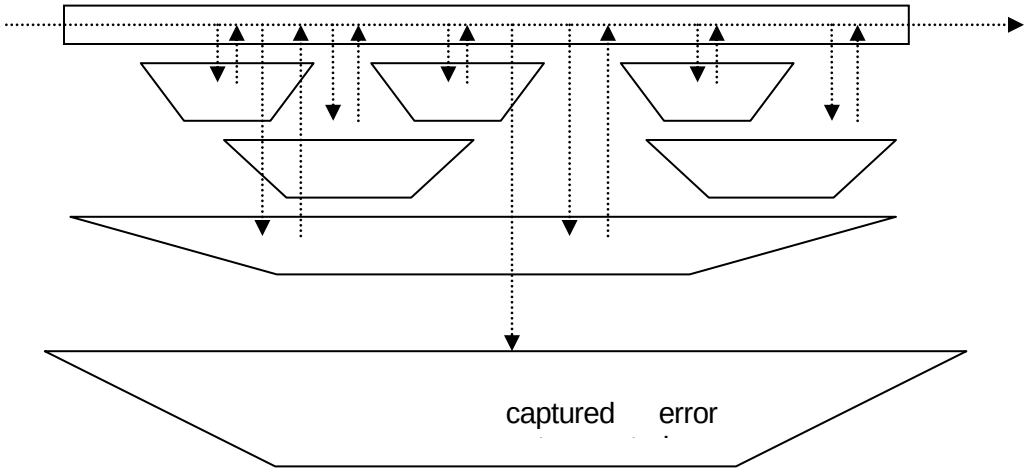


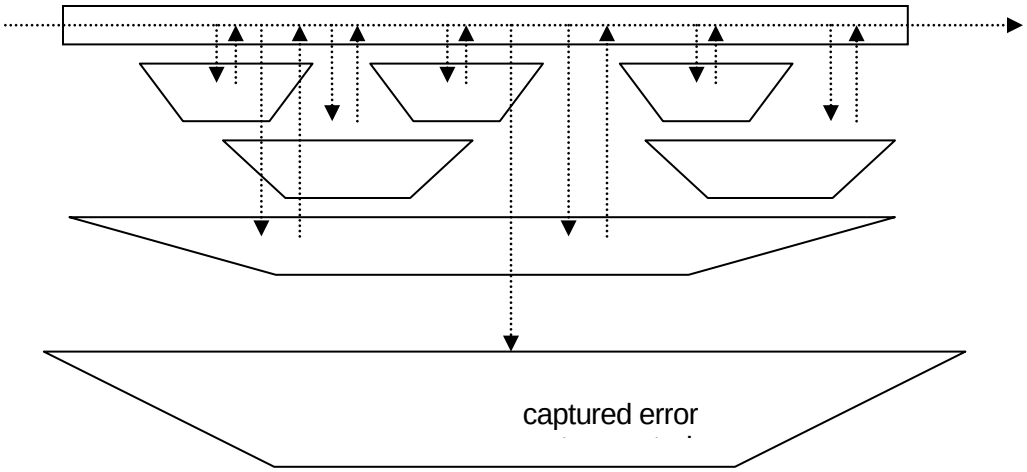
Figure 3-5 Drip Tray View of End-to-End Accuracy Objective

3.2.6. Using the Drip Tray Model to Describe Objectives

The requirement for end-to-end accuracy to be consistently within a certain tolerance of perfection means that drip trays should be implemented so that the in/out ratio can never fall outside of tolerance. In other words, the uncaptured error must be less than the error tolerance at all times.

This model may obscure a key fact: the “in” is only known by reference to the “out” plus items which fall into drip trays which are not corrected. This means precisely evaluating uncaptured error, though seemingly an obvious goal is not possible. For certainty over the “in”, and hence for certainty over the in/out ratio it is necessary to have a comprehensive collection of drip trays, so that any possible error is captured (even if not corrected). This also means that the arrangement of drip trays must be failsafe. If there is a gap in the coverage of the drip trays, there is always the risk that some error is not captured and so the total extent of error is underestimated.

Figure 3.2.6: Comprehensive Drip Tray Coverage to Measure All Error



The following points about measuring error follow from the drip tray model:

- Complete measurement of accuracy is equivalent to having a drip tray for all errors that are not corrected or at least a means of estimating the total error from representative samples.
- An error that is not captured by any drip tray is not reported, which leads to under-reporting of the total value of all errors.
- Drip trays must be totally comprehensive in order to keep real error rates low and to ensure all errors are measured.

When considering using drip trays to measure error, one key issue is span. A few wide-span drip trays may be more comprehensive than many narrow-span drip trays. There is a danger that the teams responsible for implementing drip trays or for assessing their coverage place too much faith in their own ability to diagnose or categorize all possible errors and so mistakenly believe their measures are complete although they have not implemented a genuinely failsafe or foolproof deployment of drip trays.

Wide-span drip trays may be less effective for commercial objectives, because they are slow in effect or make it difficult to diagnose problems, but narrow-span drip trays will always leave the risk of uncaptured errors. There is hence a balance to be reached between wide-span and narrow-span activities, but overlap may be a desirable property.

Another key feature of design for reporting and measuring error with drip trays is timeliness. Whereas commercial goals would favor early capture of problems, this increases the risk that the drip tray will fail to capture all problems. This is because it may not be possible to diagnose all errors from either a subjective design review or from unsophisticated checks of data. Drip trays are more likely to be comprehensive if designed to capture errors as late as possible because there is less complexity in interpreting data and evaluating the implications of errors if the data has been more completely processed. Comprehensiveness of measurement is of greatest importance in protecting customers from overcharging, but again there is a trade-off between activities that can realistic resolve problems before a customer is affected, and those that give comprehensive assurance but may take longer to execute.

3.3. The Commercial Benefits of End-To-End Charging Accuracy

Care is taken in the following sections to distinguish economic benefits as enjoyed by the electronic communications provider from those enjoyed by its customers.

3.3.1. The Kinds of Benefit to the Provider Expressible in Economic Terms

The economic benefits, to the electronic communications provider, of bill accuracy could be categorized as either recovery or ongoing benefits.

D1: Recovery is the benefit resulting from corrective action taken to bill what had previously not been billed or correctly bill what had previously been incorrectly billed.

D2: Ongoing benefit is the benefit resulting from activities to correct or prevent future errors.

H1: Total gross benefits from activities to improve bill accuracy = recovery + ongoing benefits.

Because recovery is correction of an historical error, but ongoing benefit is about benefits relating to possible future errors, H1 should be correct by definition. Either an error in the past is found, and corrected, or an error in the future is not permitted to have an impact by virtue of a preventative or mitigating activity. It may be argued that some of the activities that realize an ongoing benefit are reactive in nature, and hence work by recovering revenue. A monitoring activity might be of this type. For the sake of a consistent definition, recovery is only assumed to take place when a new or one-off activity is performed that enables correction of historical errors that would not otherwise have been corrected. Established activities that permit errors but then correct them are considered to have an ongoing benefit from the point that the activity becomes established. In other words, two similar corrections will be categorized as recovery or ongoing benefit depending on whether the correction stem from an ad hoc activity or an established control.

No benefit is assumed to accrue from activities to improve bill accuracy by virtue of improved customer satisfaction or reduced complaints. This is discussed in further detail below. There is no good evidence of a correlation between sales and customer satisfaction and between customer satisfaction and bill accuracy. What evidence of a connection that has been identified is too anecdotal to provide a basis for estimating the economic benefit following from the improvement in customer satisfaction? The project hypothesized that

- although some customers may churn because of dissatisfaction with inaccurate billing;
- the likelihood of churn relates to how sensitively and promptly the error is handled once the customer raises it to the service provider's attention; and
- it was not reliable to assume that all customers that do churn and state bill accuracy as the reason for churn actually did so because of that reason and were justified in their belief.

This was based on the following conclusions arrived after detailed analysis of the service provider's complaints data:

- most bill accuracy complaints are not justified;

- most bill accuracy complaints are resolved through providing more information to the customer without any bill correction and without issuing a credit;
- most complainants in this category who threaten to disconnect do not subsequently disconnect.

Some independent evidence to support these conclusions has been generated within the industry since the original project was completed. A report presented by a service provider to an open meeting hosted by the UK communications regulator reached similar conclusions that most complaints about accuracy were resolved by providing the customer with more information.

3.3.2. Benefits of Revenue Assurance Accuracy Controls

The Revenue Assurance (RA) Department had monitored the benefits obtained for the business from their activities under three headings:

- recovered
- prevented
- generated

The RA department had found that a high degree of estimation was needed to calculate the benefits in the all cases except recovery. Even in recovery, it was found that there was often a need to use assumptions in order to calculate the attributable benefit. The matter had been subject to significant discussion, and in general RA sought to employ a conservative approach in order to ensure all figures reported to senior management could be justified. RA found that it was not possible to apply any single technique or set of assumptions when calculating benefits. In particular, the period of time over which benefits are realized for preventative gains was impossible to estimate, so largely arbitrary estimates were used in each specific case according to the judgment of the individuals involved in diagnosis and resolution. Because of the difficulty of estimating and extrapolating benefits, such benefits were only calculated when they resulted from the clear remedy of a problem of significant value. As such, no value was attributed to the majority of ongoing activities simply because the approach adopted was not suited to the level of granularity appropriate to capture the benefits arising from them. The project concurred that no method known to the project would enable such benefits to be valued. In addition, the project agreed to the following assumption:

H2: The economic benefits accruing from an activity to correct or prevent future error cannot be assumed to continue to accrue at the same rate for all time.

Instead, the project decided that specific judgment would be needed over the lifetime for any benefit arising from a preventative activity.

The RA department had not sought to capture its costs and the costs incurred by other departments in supporting it. The project analyzed the costs of RA on the basis of:

- payroll costs of RA staff
- costs of equipment

- estimated payroll costs in relation to time spent by other departments to support RA

Dividing total benefits by total costs for the last year indicated that the benefits of RA greatly outweighed the costs even using conservative assumptions about benefits accrued. The project also concluded that:

-
- "generated" revenue relates to changes of business policy and so is unrelated to accuracy per se;
- some of the recovered revenue included improvements resulting in new opportunities to sell and charge for services, so again should be considered unrelated to accuracy;
- generation of revenues through business policy changes and through improved realization of sales opportunities tended to give much bigger one-off benefits than improvements to accuracy; but
    - it was generally harder to estimate the benefit of changes designed to generate revenue or from improved realization of opportunities then it is to determine the benefits of improvement in accuracy; so
    - it was hence reasonable to continue to limit the project scope to questions of benefits accrued from improved accuracy, and not to extend scope to other kinds of commercial benefits.

Preventative benefits of improvements in accuracy had been calculated by the RA team through extrapolation of current error rates for a period of 6 or 3 months past the date of resolution. The choice of period was governed by whether the RA team judged that the discovery was mostly due to RA's work or that of other parts of the business. These timescales appear arbitrary, though the project has no data to suggest an alternative. Their rationale was based on RA's judgment as to how long it would have taken for the matter to be resolved without RA's involvement. The project considered the timescales to be very conservative, as it is speculative that many of the matters would even have been identified with RA's role as a monitoring function. It was reasonable to note that several of the problems identified and corrected had existed unidentified for a period of years rather than months. Preventative benefits all related to identifiable and specific issues, so no benefit was assumed to relate to general improvements in controls and avoidance of errors. This contradicted RA's own analysis of error rates, which suggested that systematic errors had fallen over the period monitored. This is evidence that monitoring leads to smaller improvements that cannot be readily separated out and tracked, but which do have a genuine benefit although no method for calculating these has been devised. Non-systematic errors had observed a more volatile pattern of behavior, but the volume of data was too small to form any meaningful trend analysis. This was as expected, as these errors were categorized as resulting from specific changes.

Although RA did monitor and report on errors in the business' favor, as well as is the customer's favor, the value of these were trivial in comparison to both the costs of the department and the benefits of resolving errors in the customer's favor. Detailed analysis of individual drivers of benefits confirmed that none stemmed from additional monitoring or auditing necessitated by accuracy regulation. This was as expected, because the results also corroborated RA's anecdotal expectation that errors are greater for immature products and technologies. In contrast, regulatory monitoring

and auditing had been focused on the most material and most mature revenue streams, as relevant to most customers.

Data prior to the last year was considered too piecemeal to give a meaningful analysis of trends. Though error rates had been monitored, the basis for estimating benefits had not been consistent and it was impractical to re-estimate the benefits that had been obtained.

3.3.3. Benefits of the Billing Department's Accuracy Controls

The Billing department had not assessed the benefits they obtain for the business in the same manner as RA. However, a number of their quality control activities would improve the accuracy of billing. This is most apparent by analyzing the trends in errors as identified and resolved by the Billing Department. The data on errors captured by the Billing Department show that the value of errors they found were in the customer's favor by a ratio of around 3.25 : 1, but that the value of these errors were trivial in comparison to the errors identified and resolved by RA. This appears to underestimate the true extent of the benefits of the controls implemented by the Billing Department, particularly as they regularly propose changes to ensure that errors once found do not recur, even if the errors are small. The department's control activities is also considered to have an intangible benefit as an ultimate "backstop" should other control activities fail to identify issues at an earlier stage.

3.3.4. Combined Benefits of Accuracy Controls of Revenue Assurance and Billing

Combining the costs and benefits of Revenue Assurance and Billing, as described above, shows that, for the service provider reviewed, the benefits of accuracy outweigh the costs. Even on the highly prudent comparison of only amounts recovered to all costs, there is a clear net benefit. Including a conservative assessment of ongoing benefits significantly improves the assumed net benefit. The calculations of total net benefit are highly sensitive to the assumption of the period over which ongoing benefits is enjoyed. This means it would be misleading to quote a definitive ratio of benefits to costs, because the most significant variable is the assumption of how long ongoing benefits last. This in turn, is a highly speculative judgment. However, as benefits outweigh costs even if no ongoing benefits are assumed, the improvements in billing accuracy conclusively justify the investment in controls.

3.3.5. Understanding Benefits to the Supplier in the Context of the Customer

Neither RA nor Billing sought to value the benefit of their activities for customers. The project reviewed the matter and decided that the following assumption was appropriate:

H4: Errors are symmetrical in the costs and benefits for suppliers and customers. Any benefit that arises from an error is exactly equal to the cost to the other. A model based solely on inaccuracy of billing made by a supplier to a customer will approximate to a zero-sum game.

The implications of this hypothesis are discussed further below. This hypothesis, however, is not at odds with the belief held by RA that reducing overall error is in the

business' favor. This was because their observations were consistent with the following hypothesis.

H7: More error is in the customer's favor than the supplier's favor.

It has become an industry truism that H7 is correct, though the project was unable to identify any instance where it had been subjected to serious analysis. The faith in H7 is predicated on two sources:

- the actual experience of service providers, vendors, consultants etc; and
- a theoretical explanation of why incompleteness is a particular problem for telecommunications.

Many of the arguments from experience had merit, but the project concluded that these were not, ultimately, reliable. This was because the individuals that made the arguments from experience would have reason to give a biased assessment. In short, they were either made by:

- consultants promoting the benefits of their skills and approach;
- vendors promoting the benefits of their products; or
- employees of communications providers with specific responsibility explaining the results they had obtained in activities or projects intended to generate commercial benefits.

Although there may have been a lot of truth in their reports, the concern was that the experiences related would always be positive. In short, it would be difficult to envisage a scenario where the results presented showed that the projected benefits were not subsequently attained.

The theoretical argument that errors are more likely to be in the customer's favor was thought to be robust. Errors of completeness are always in the customer's favor, errors of validity in the supplier's favor. Other errors may be to the benefit of either party, so may reasonably be assumed to have an equally likely impact either way unless subject to biased controls. This means that if errors of completeness are more likely than errors of validity, then errors in the customer's favor are more likely than errors in the supplier's favor. It follows from the way that data is produced and transmitted that errors of validity should be unlikely. A new data record is unlikely to be written for no reason. Even when an invalid record is written, the likeliest cause is duplication of an existing record, which means that a relatively straightforward, and hence universal, approach of checking for and eliminating duplicates eliminates virtually all errors of validity. In contrast, errors of completeness may occur either because of a failure to write a record, or because the error is not correctly transmitted from one point to the next. These may seem more probable as causes of errors, though the project did not consider that they would be evidently far more likely. Practical experience suggested the following:

- systems may be configured under extreme loads to continue to work by suspending activities to write or transmit records;
- where processes depend on the input of data from several sources, they may fail to work when any one source fails or is corrupt;
- failure to write a data record may be difficult to detect or reproduce.

The likelihood of errors being in the customer's favor hence relates to common design decisions, which permit a certain risk of failure to write or transmit a record, combined with the difficulty of detecting such failures. Though the argument is supposedly theoretical, it was accepted that its truth was still largely based on experience. Nevertheless, were such circumstances only rarely true, it would imply that all reports of benefits outweighing costs for accuracy projects would have been exaggerated. Though the argument was not considered wholly satisfactory, the hypothesis was hence adopted because of the lack of contradictory evidence.

This suggests that RA's belief is correct that

H8: There is a normal commercial incentive to prevent errors in the customer's favor.

If H7 is correct, then regulation to reduce error rates will benefit the supplier. But if the supplier is rational, H8 already means they have a commercial incentive to avoid errors without the need for regulation. This remains true whether the supplier is sales maximizing or profit maximizing. Because telecommunications infrastructure costs are largely fixed or stepped, a reduction in the total figure billed to customers will reduce both sales and profits.

3.3.6. Assessing Benefits According to the Timing of Drip Tray Activities

The trend observed from RA and Billing information was that controls that are "earlier" in diagnosing problems tend to give the greatest return for the outlay. This is as expected; if early controls are successfully capturing problems there should be fewer problems left that could be caught by later controls. It was considered flawed, however, to judge whether later controls were themselves uneconomic for the following reasons.

Earlier controls are themselves improved by the identification of flaws implied in any capture of errors at later stages, so later controls are a necessary means of improving the effectiveness of earlier controls;

The apparent returns of early controls are easy to estimate in comparison to both later controls and very early controls. The benefit of these controls is most likely to be in early diagnosis and resolution of real and potential problems even though the impact is trivial or nil in terms of value. Although this project has inadequate resources to form an estimate, this does not imply that there is no material benefit. Rather, the cost of estimating the benefit is too great to justify the activity at present.

Very early controls, such as proactive reviews of designs prior to implementation, were not ascribed any economic value. The rationale was that any error captured by such a control is entirely notional. Because of the control, no actual error takes place. This is another instance where no benefit is attributed because of the difficulty of estimating the benefit rather than there being no evidence of any benefit.

3.3.7. Drip Tray Controls Identified During This Project

The costs of the following activities have been factored into the analysis of commercially driven costs and benefits given above for:

- operation of a re-rating tool;

- detailed expert analysis of risks and weaknesses for proposed system changes and product launches;
- analysis of implementation needs to increase visibility/checks in relation to system or product changes;
- daily analysis and reconciliation of volumes of usage records processed through each element;
- reconciliation of sample SS7 data to usage records;
- detailed walkthroughs of business processes by controls experts;
- manual check of circa 1000 bills per month;
- reconciliation of standing customer data between network and billing systems;
- the process and database to control and track tariff plan changes;
- controls and reconciliations of data exchanged for billing purposes with other parties;
- irregular one-off projects to review areas perceived to be at high risk due to previous problems or issues raised through other monitoring;
- regular reporting of results and incidents to senior management.

The costs of the following controls were not factored into the analysis above as they were driven by regulatory compliance. They are hence included in the calculation of the additional costs created through regulatory compliance.

- test call generation;
- operation of a secondary sample-based usage reconciliation engine between multiple elements;
- external audit for the purposes of determining regulatory compliance;
- activities to support the regulatory audit through communication, planning, information gathering, additional documentation etc.;
- collating, calculating and reporting of regulatory compliance measures.

The costs of the following controls were not factored into the analysis above because they fell outside of the remit of either RA or Billing and the project was not able to readily assess the relative costs to benefits of these activities.

- numerous standing data reconciliations between elements;
- the Legal department's review of the accuracy of statements made in tariff documents issued to customers;
- reviews and audits by Internal Audit;
- manual bill checks performed in response to customer queries;

The Customer Services process to capture complaints data and escalate justified complaints to an appropriate system or human process resolution to prevent recurrence.

4. Revenue Assurance, Quality Assurance and Regulation

The discipline of Revenue Assurance by its nature addresses a number of topics that are subject to a variety of international and statutory regulations.

Diverse regulations, each having its unique focus, can be aligned into two major groups of industry-neutral, and industry-specific regulations. Examples of the former include European Union's "8th Directive" and the United States' Sarbanes-Oxley Act (SOX), which is often considered the most significant and illustrative regulation with respect to its rigorous compliance rules. Examples of the latter group, with regard to telecommunication industry, include a wide range of guidelines and standards, covering billing accuracy, network and service availability, settlements between CSPs, customer relationship management, privacy of customer data, revenue booking and recognition and many other telecom issues.

The objective of this chapter is to provide an overview and guidance on some of the regulatory requirements that could be partly or fully addressed by a comprehensive Revenue Assurance function.

4.1. Sarbanes Oxley

The Sarbanes Oxley Act of 2002 was enacted largely in response to a number of major corporate and accounting scandals involving some of the most prominent companies in the Unites States. These scandals have resulted in loss of public trust in reporting practices and corporate accounting. The objective of the SOX Act is to restore investor confidence in public markets and enhance penalties for corporate wrongdoing. The SOX Act has entitled the PCAOB (Public Company Accounting Oversight Board) to oversee compliance with relevant provisions of the Act.

4.1.1. Relevant Sections of SOX

While SOX is an extensive regulation encompassing all transactions related to financial reporting for Organizations, from a regulatory compliance perspective telecom CSPs need to focus primarily on the Act's following most important sections:

Section 302 – Accuracy of Financial Statements

The signatories to the Financial Statements are responsible for

- Designing, Establishing & Maintaining the Disclosure Controls
- Evaluating the effectiveness of Disclosure Controls
- Presenting Conclusions
- Fraud, Deficiencies & Significant changes in the Disclosure Controls should be disclosed

Section 404 – Internal Controls

- Management accepts responsibility for establishing & maintaining Internal Controls
- Management is responsible for assessing the effectiveness of Internal Controls
- External Auditor attests management's assessment of Internal Control

4.1.2. Interplay between SOX and Revenue Assurance

Revenue Assurance is essentially a set of activities involving detailed data monitoring, analysis and control, aimed primarily at minimization of financial losses. It holistically encompasses the Service provider's entire workflow from service provisioning to billing, to payment allocations, and beyond. RA should perform a thorough evaluation of Service provider's every domain to ensure there are no leakages at a process as well as technology level. Revenue Assurance is also about risk assessment and risk management with respect to processes that support revenue management chain and collateral areas.

Evidence resulting from in-depth Revenue Assurance activities in the form of monitoring reports, investigation results, reconciliation, and synchronization procedures helps responsible management to gain assurance of data completeness and accuracy, as well as to assess the internal control environment over respective processes. Integration of SOX compliance initiatives into Revenue Assurance function creates a functional tool in the hands of financial and operational departments to properly monitor as well as control a great number of risks that are subject to financial reporting compliance. In absence of a comprehensive Revenue Assurance function, the financial institutions would have to delve into the intricacies of individual functions to analyze specific risks. SOX compliance requirements can serve not only as one of the key drivers, but also as the point of alignment, for many different risk management initiatives undertaken within organization.

Key elements of NGOSS framework, namely eTOM and SID, referred to in the Chapter 2 of this Guidebook, and could be successfully used as an efficient basis for the development of diverse risk management functions, including Revenue Assurance, Regulatory Compliance and others. This idea is illustrated by the below diagram:

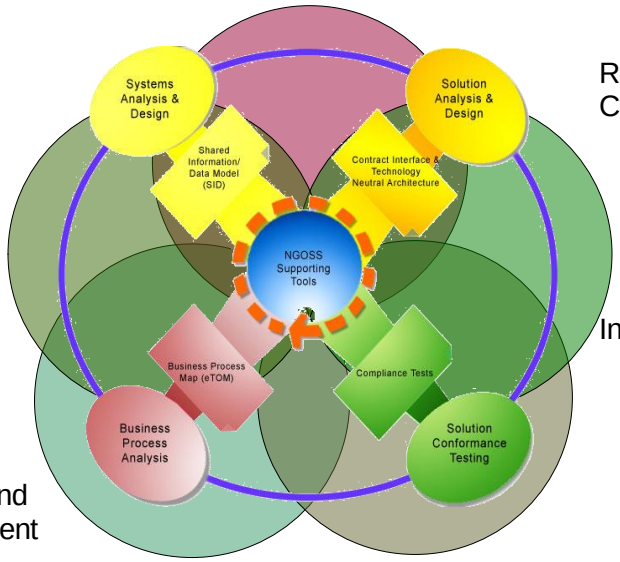


Figure 4-1 SOX, RA and Management

The objectives and focus areas of each of the above risk management functions are different:

- Revenue Assurance: data quality and process improvement aimed at prevention and management of revenue leakages or instances of fraud, caused by subscriber, external party or a Company's employee.
- SOX Compliance: maintenance and enhancement of an adequate system of internal controls over financial reporting through the period of compliance.
- Internal Audit: independent assurance of compliance with Company's internal policies and procedures.
- Business Risk Management: alignment of risk management with strategy, people, business processes and related technology.
- IT Governance: alignment of IT processes with business requirements to meet organizational objectives.

4.1.3. Linkage between SOX and eTOM processes

Linkage between Revenue Assurance and SOX can be realized at Level 2 of eTOM. Figure 8 below represents processes in Operations area that are subject to SOX compliance in terms of internal control for financial reporting that could be considered part of "Enterprise Risk Management" or "Stakeholders & External Relations Management" at Level 2 within Enterprise Management area.

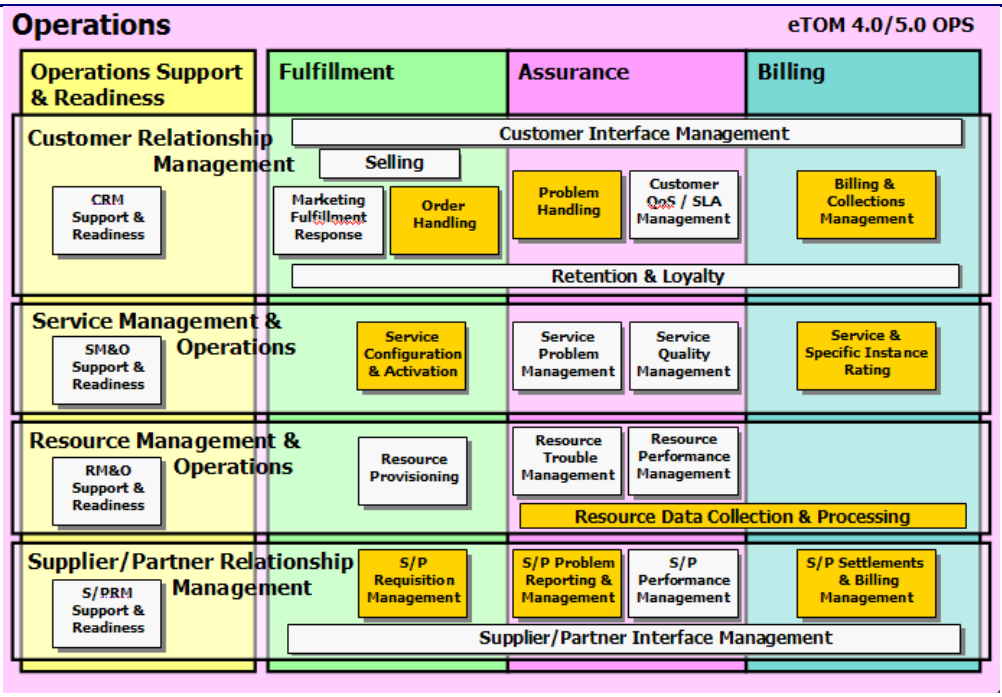


Figure 4-2 SOX related eTOM processes

4.1.4. Key Requirements for Revenue Assurance Activities to Enable SOX Compliance

From SOX perspective, any Control Framework developed within the Company should explicitly show the following sections:

- Monitoring
- Information and Communication
- Control Activities
- Risk Assessment
- Control Environment

The above layers are defined by COSO (The Committee of Sponsoring Organizations of the Treadway Commission) integrated control framework that is adopted by PCAOB (Public Company Accounting Oversight Board) as the most relevant for use from compliance perspective. COSO is a voluntary private sector organization dedicated to the improvement of the quality of financial reporting through business ethics, effective internal controls, and corporate governance. COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative that studied the causal factors that can lead to fraudulent financial reporting, and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

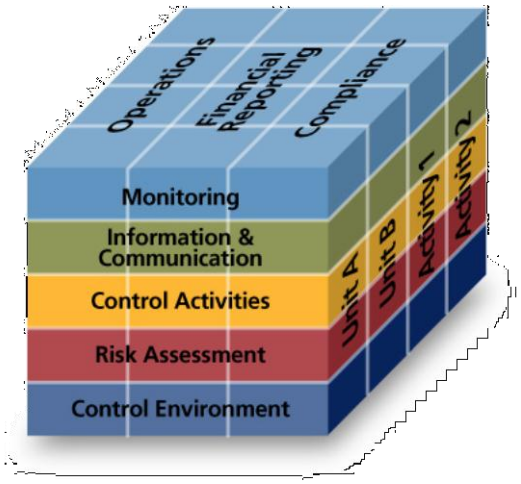


Figure 4-3 COSO Internal Control Framework

Control Environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people. This includes risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

Risk Assessment includes risk analysis, assessment of a risk's likelihood and potential impact, as a basis for determination how those risks should be managed. Risks are assessed on an inherent and a residual basis.

Control Activities represent policies and procedures that, when established and implemented, help to ensure that responses to risks are effectively carried out.

Information and Communication ensures that relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

Monitoring ensures that internal controls are monitored and modified as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Control activities have to be properly documented to enable regular assessment of their design and operational effectiveness. The usefulness of the above framework is in that internal control system, designed according to the definitions of the framework layers, could be successfully used for different risk management objectives, e.g. the ones formulated in the areas of operational efficiency, compliance or financial reporting.

4.1.5. Illustrations of Interplay between SOX and Revenue Assurance

An integrated Revenue Assurance function could provide facilitation for the following sample list of control objectives mandated for telecom service providers by the Sarbanes Oxley legislation:

- Ensure that all collected events are processed according to established filtering rules.
- Ensure that duplicated records are identified, labeled and analyzed.
- Ensure that Customer information items stored in different internal data sources are synchronized or regularly reconciled.
- Ensure that all payments made and received for telecom services are properly allocated to Customer or Service Partner accounts within proper period.
- Ensure that external Customer information is regularly verified against internal customer information.
- Ensure that usage records are obtained from each Service Partner and reconciled with internal records whenever applicable to verify accuracy of Service Partner invoice.
- Ensure that all billable usage records from Service Partner are processed and billed according to the billing rules consistent with existing contracts.
- Ensure accuracy of service fees and charges classification to enable proper matching of revenues and expenses.
    - Benefits for SOX Compliance Derived from Revenue Assurance
    - RA enables risk assessment across revenue management chain and collateral processes
- RA ensures data integrity for financial reporting purposes
- RA detects leakages at system integration points
- RA provides evidence for internal control evaluation and documentation

In summary, Revenue Assurance and SOX Compliance are two tightly inter-mingled functions that not only have a number of overlapping business critical objectives, but also have a strong dependence upon each other.

4.2. Europe & UK specific linkages

4.2.1. Introduction:

This section is aimed at providing a broader view of European telecom regulation, which is structured around the concept of “Promoting competition to the maximum benefit of users, contribute to the development of the internal market and promote the interests of EU citizens.”

It should be noted at the onset that within Europe the European Parliament and Council provide directions and guidelines around the Regulatory Framework. The implementation of this is left to the NRA’s (National Regulatory Authorities). As a result there is a vast disparity on the maturity, implementation and monitoring of the Regulatory requirements within EU members.

4.2.2. Implementation of the new European regulatory framework

The European Parliament and Council set a legal deadline of 24 July 2003 for the transposition of the main provisions of a new framework.

The "Framework Directive" forms part of the "Telecommunications Package designed to recast the existing regulatory framework for telecommunications in order to make the electronic communications sector more competitive. This new regulatory framework consists of this Directive plus four specific Directives, namely the:

- Directive on the authorization of electronic communications networks and services (the " Authorization Directive");
- Directive on access to, and interconnection of, electronic communications networks and associated facilities (the “Access Directive");
- Directive on the universal service (the "Universal Service Directive");
- Directive concerning the processing of personal data (the "Directive on Privacy and Electronic Communication”).

As of 1 November 2003, only eight countries had taken action to incorporate these into national law. These countries are: Denmark, Spain, Ireland, Italy, Austria, Finland, Sweden and the United Kingdom.

In some cases, secondary legislation is still required to ensure full transposition. Of those Member States that have not yet notified the Commission of transposition measures, there is particular concern that the passage of drafts through the legislative process is likely to be lengthy (Germany, France); that political uncertainties are causing delays (Belgium); or simply that despite the existence of drafts the legislative process has not yet been completed (Greece, Luxembourg, the Netherlands, Portugal).

4.2.3. Scope, Aims and Definitions

The objective of this Directive is to establish a harmonized framework for the regulation of electronic communications networks and services. It lays the foundation in the form of horizontal provisions serving the other measures: the scope and general principles, basic definitions, general provisions on the national regulatory authorities, the new concept of significant market power, and rules for granting certain indispensable resources such as radio frequencies, numbers or rights of way.

In response to convergence of technologies and the need for horizontal regulation of all infrastructure elements, the new framework is no longer limited to telecommunications networks and services but covers all electronic communications networks and services. This includes, for example, fixed and mobile telecommunications networks, cable or satellite television networks and electricity networks, where they are used for electronic communications services. On the other hand, the content of services delivered over electronic communications networks, such as broadcasting content or financial services, is excluded, as is telecommunications terminal equipment.

The Directive defines a series of terms related to electronic communications, including:

- "**Electronic communications networks**" means transmission systems which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, networks used for radio and television broadcasting and cable television networks;

- "**Electronic communications service**" means a service, normally provided for remuneration, which consists in the conveyance of signals on electronic communications networks. Services providing, or exercising editorial control over, content transmitted using electronic communications networks and services are excluded;
- **"Associated facilities"** means the facilities associated with an electronic communications network or service which enables the provision of this service via that network or service. This includes conditional access systems - any technical measure whereby access to a protected radio or television service is made conditional upon subscript ion or other form of prior authorization - and electronic program guides.
-

4.2.4. Structure - National Regulatory Authorities

Independence

Member States must guarantee the independence of national regulatory authorities by ensuring that NRA's are legally distinct from and functionally independent of all organizations providing electronic communications networks, equipment or services.

Right of Appeal

At national level effective mechanisms must allow any user or undertaking providing electronic communications networks or services the right of appeal to an independent appeal body in the event of any disputes with a national regulatory authority.

Impartiality and transparency

Member States must ensure that national regulatory authorities exercise their powers impartially and transparently. They must also ensure that the national regulatory authorities make arrangements for consultation of the interested parties if they intend to take measures, which could have a significant impact on the market.

4.2.5. Obligations and Tasks of National Regulatory Authorities

To promote competition in the provision of electronic communications networks and services, the primary tasks for the national regulatory authorities are:

- Ensuring that users derive maximum benefit in terms of choice, price and quality;
- Encouraging investment in infrastructure and promoting innovation;
- Encouraging efficient use and management of radio frequencies and numbering resources.

The national regulatory authorities must also contribute to development of the internal market by, *inter alia*:

- Encouraging the establishment and development of trans-European networks and the interoperability of pan-European services;
- Ensuring that there is no discrimination in the treatment of undertakings providing electronic communications networks and services;

- Cooperating with each other and with the European Commission to ensure the development of consistent regulatory practice and consistent application of the new regulatory framework for the telecommunications sector.

The final task of the national regulatory authorities is to promote the interests of the citizens of Europe by, *inter alia*:

- Ensuring that all citizens have access to a universal service, as specified in Directive;
- Ensuring the availability of simple and inexpensive dispute resolution procedures;
- Contributing to ensuring a high level of protection of personal data and privacy ("Directive on Privacy and Electronic Communications".)

4.2.6. Maturity Status of National Regulatory Authorities

It is quite apparent that the maturity status of regulatory requirements varies according to the maturity of the country's NRA and this could vary significantly as is apparent in above.

Taking this fact into consideration there is a need to map an Organization's Revenue Assurance functions to its obligations towards the Telecom Regulatory Requirements.

4.2.7. Regulatory Requirements v/s Revenue Assurance

One of the major constraints on revenue assurance evolution is the need to overcome senior management skepticism about its benefits. Skepticism about the merits of revenue assurance is due to:

- Doubt over the magnitude of benefits that can be earned from implementing fixes and improvements that arguably could and should have been made unnecessary had systems and processes been initially implemented correctly;
- The difficulty of quantifying the unknown (the "iceberg" paradox); and
- The immaturity of revenue assurance as professional discipline.

But when regulatory requirements come into play, the scenario is changing. Depending on the regulatory requirements some form of Revenue Assurance functions may need to be addressed. And if, whilst doing this, benefits to both the Business and customer perceptions are realized, management skepticism, to a certain extent can be mitigated.

The issues at this stage are two-fold:

- Regulatory requirements imposed by NRA on Business can be costly to address and provide only minimum benefit from the business standpoint (An example of this includes an instance in which an service provider was required by NRA to set up test call generators for all of the service provider's switches,);
- The Business could get complacent about effectiveness of its Revenue Assurance function by assuming that meeting the Regulatory requirements is sufficient for Revenue Assurance needs.

It can hence be stated that compliance with regulatory requirements should not be deemed to address the completeness of Revenue Assurance. On the other hand a

mature Revenue Assurance function should be able to address the Regulatory Requirements.

5. Revenue Assurance and Fraud

5.1. Introduction

Traditionally, most CSPs identified fraud management as a priority in the early days of operations. The early focus and implementation of systems contributed to the development and maturity of fraud management practices and systems. Although there is a clear relationship between fraud management and revenue assurance, fraud management has evolved as a separate function, often under different department and sponsorship within the organization. Industry-wide, there is consistency in the approach and system functionalities for fraud management.

However, revenue assurance is still an immature activity for many CSPs. Revenue assurance activities in most of the CSPs are independent of their fraud management practices. As new issues and systems come into place, there is an increasing need to look at both fraud management and revenue assurance together due to the nature of the leakages and the solutions and practices to identify these.

The purpose of this section is to demonstrate the relationship between fraud management and revenue assurance and recommend different options for CSPs to effectively tackle revenue assurance issues.

5.2. Revenue Leakage – Differentiating Fraud and Revenue Assurance Issues

Revenue leakage in any CSP's operations can be grouped into three categories, namely, Fraud, Revenue Assurance and Bad Debt. Revenue Assurance problems are mainly due to the operational inefficiency in the systems or processes. Fraud represents the deliberate intention to avoid payment and Bad Debt is the combination of un-intentionable and intentionable revenue loss.

An example of this segmentation is a new bundle offer from a service provider may cause leakage due to illegal use of services and network or non-payment of the dues by the customer. Other leakages such as the customer not being billed properly as in the case of under billing or over-billing and issues such as the order not being provisioned are due to inefficiency in the system.

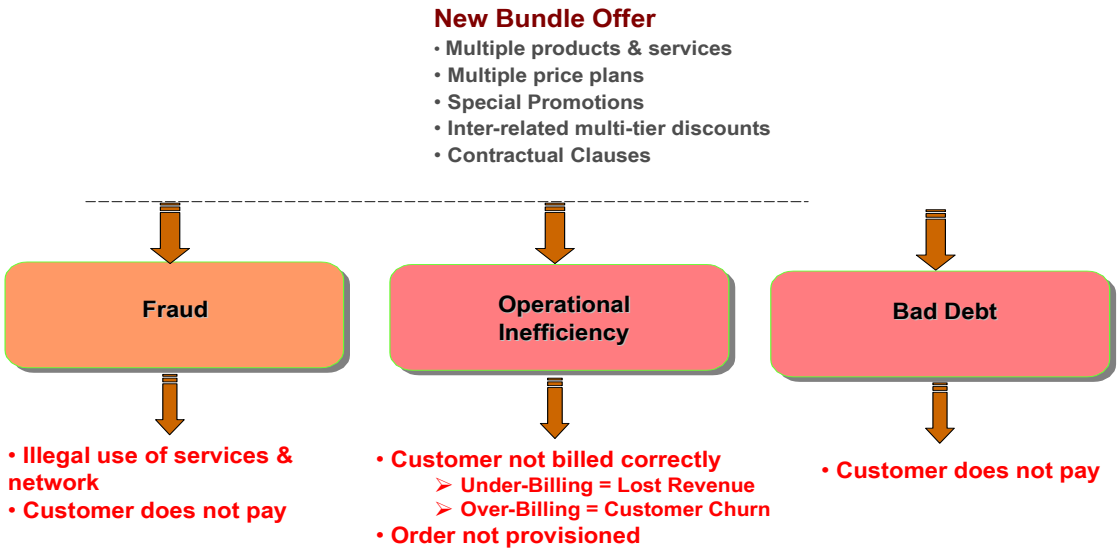


Figure 5-1 Categories of Revenue Leakages

It may not be possible to have a clear segmentation and resolution for the following reasons:

- Differentiating factor is very thin: The root cause of fraud and revenue assurance can be the same. Intent and root cause are the differentiating factors. Incorrect provisioning of service at the switch without provisioning at the billing system causes revenue leakage, as the service usage cannot be billed for. The root cause could be a shortfall of the provisioning process or an intentionally performed activity. In the former case, this is a revenue assurance problem and in the latter case, it is an internal fraud.
- In case of most of the problems, since the data analyzed is the same, it would be reflected on multiple tools and systems. This trend is likely to continue and become more significant in case of IP and event records.

5.2.1. Case 1

Service is not provisioned for a particular subscriber in the billing system, but the subscriber is using the service. The subscriber is provisioned in the network element. This scenario can be interpreted in the following way:

- The subscriber has been illegally provisioned in the network element
- The subscriber was genuine, but because of a process error or error in provisioning system, only network element was provisioned.

5.2.2. Case 2

A sudden increase in the number of CDRs generated for a subscriber could be interpreted as three different scenarios

- Increased call pattern that is detected by the fraud management system as a potential fraud;
- Increased number of records that may be due to malfunctioning of switch causing multiple records or incorrect guiding of records
- Genuine increase in usage of the subscriber that could be potentially new revenue opportunities for the service provider.

5.2.3. Case 3

A sudden increase in traffic is detected from a trunk configured for national calls from an interconnect service provider. This scenario can be interpreted as:

- Incorrect trunk configuration causing other traffic (such as international traffic) to be routed through the trunk;
- A third company is illegally routing its calls through the trunk using devices such as gateway SIMs
- There is a genuine increase in traffic. This calls for a renegotiation of the existing contracts and tariffs.

5.3. Relationship between Fraud and Revenue Assurance

The relationship between the two domains is illustrated below:

- Revenue Assurance issues that may be exploited for fraud:
- Certain frauds, especially internal frauds are caused when fraudsters are able to exploit data integrity issues or process loopholes. New systems, services, and equipments are potential vulnerable areas that can be used by fraudsters. Test phones or a SIMs can also be a target for such misuse. Some of the common examples of these frauds are in the following areas:
- New product development;
- System configurations;
- Test configurations and equipment.
- Fraud scenarios that can cause revenue leakage
- Certain fraud scenarios result in revenue loss for subscribers not related to the fraud. This loss is usually data integrity issues caused by the fraud. Identification of such issues is critical for recovery of revenue from non-fraud subscribers. An example of such case is an internal fraud by illegal configuration in the system such as suppression of records for fraudsters causing revenue leakage for other subscribers.
- Revenue leakages that may be detected by fraud analysis and vice versa.
    - Due to the nature of fraud and revenue assurance issues, it would be possible to find indications on either system. This is important in case

of new frauds and systems. Use of such information is critical in solving the issues within the shortest possible time to reduce the impact. An example that was detected by a revenue assurance system is Interconnect fraud, which is done by modification of some parameters such as source or origin of calls to apply different rates.

- Fraud management system's real-time processing capability for detecting integrity issues will significantly improve the RA team's resolution/correction response time.

5.3.1. Collaboration for multi-dimensional leakage:

As illustrated by the above cases, there is a need to look at each issue identified by fraud management or revenue assurance systems in multiple perspectives.

- It is usually possible to detect the leakage and identify the cause area. However, it is difficult to find out the root cause (such as intent or process error) without taking a holistic view of the issue;
- It is possible that a revenue assurance problem, such as scenario defined in case 4 can easily pave the way for fraud to be committed on the network. The revenue assurance problem, if not corrected with a holistic view, can provide loopholes for fraudsters to attack the network. Identification of the relationship and its effects is critical for choosing the correct resolution and prevention methodology.
- Certain internal frauds are likely to be detected by the revenue assurance system first. Unless the exact cause and intent of the problem is identified, it may not be possible to prevent the issue from reappearing. If treated as a revenue assurance problem alone, it is likely to be used in a different manner by the fraudster to exploit the loopholes. Therefore, the issue requires analysis by both revenue assurance as well as fraud management systems.
- Time for resolution of issues is critical. For faster resolution of certain problems detected by one of the functions, it may be necessary that the information be passed on to the other relevant function at the earliest opportunity. A collaborative approach facilitates transfer and early action on such issues.

5.4. Recommendations for a Collaborative Approach

To analyze and resolve revenue leakage issues at a holistic level and in many cases evolve revenue generation opportunities out of this effort, it is important to adopt a collaborative approach to revenue assurance. We recommend collaboration between Revenue Assurance and Fraud Management at three levels: the team level, the process level, and the tool level. In many cases, such collaboration permits analysis and resolution of revenue leakage at a holistic level that would be missed otherwise.

Nevertheless, our recommendation is for collaboration between RA and Fraud teams, and not necessarily for having common people dealing with both.

Similarly our recommendation is to use tools and processes for RA and Fraud that permit sharing data, KPIs, case management, dashboards and reports. However, we do not necessarily recommend using the same tool or process for revenue assurance and fraud (additionally, we do not necessarily recommend to use of the same tool for all revenue assurance tasks, we recommend rather to use the best of breed). Our recommendations are explained in the following sections.

5.4.1. Collaboration Components

Collaboration of Teams:

Collaboration of fraud management and revenue assurance teams results in more effective dissemination and transfer of information helping in faster resolution of issues. Some of the options for collaboration of teams are:

- Co-location of the teams that allows easier communication;
- Common team members and managers with clear roles and responsibilities who can liaise between the two teams;
- Common team members who analyze both fraud and revenue assurance issues.

Key advantages of collaboration between teams are:

- Cross-fertilization of information;
- Faster communication of issues and detected discrepancies;
- Faster handover of issues between the teams;
- Faster identification of key issues and information

Challenges in collaboration between revenue assurance and fraud management teams are:

- In many CSPs, Fraud and Revenue Assurance teams exist as different departments and may even have different executive sponsors. There may be a need to change existing organizational structures or define structures that allow effective exchange of information.
- Prioritization of issues – Fraud is usually given high importance since it is considered an unwelcome attack from outside. It may be necessary for organizations to define new priorities.
- Political considerations on the role, responsibilities and authority of members of collaborative team.
- Security issues: Access to information from the fraud management team can be restricted in some CSPs due to regulatory issues. Hence it may be necessary to address such restrictions;
- Mission Differences – The Fraud team typically tries to stop the fraud without sharing information with the whole organization (to prevent others from doing a similar fraud). On the other hand the RA mission is to divulge the information found throughout the whole organization, both to help entities prevent similar RA issues in the future, and to gain future collaboration.
- Skill-sets: Collaborative team members may need to acquire additional skill-sets to handle issues related to both domains.

Process

Integration of the fraud management and revenue assurance processes helps streamline information flow and improve issue resolution. Integration of processes encompasses setting common objectives and KPIs, integrated resolution methodology and procedures, transfer of information and cases, inter-department communication and other related areas. Depending on the nature of the business,

scope and ability to affect changes in the existing structure, integration can be adopted in all the processes or specific areas. For example, integration can be adopted only for prevention activities and not for operations.

Advantages of collaboration of process:

- Streamlined activities that facilitate faster resolution of issues, especially for cross-functional issues;
- Reduce redundant processes.

Challenges brought about by process integration are:

- Risk of increasing complexity;
- Most of the service providers have established working processes and procedures to fight fraud and operational inefficiency. There may be resistance to modify these;
- Political considerations in treating processes from both domains.

Tools

Fraud Management and Revenue Assurance tools can be integrated at two levels – Data Management layer and Business layer.

- At the data management layer, the systems use the same data processing and storage for the interfaces that are commonly used by both. Integration of tools can provide in significant operational expenditure and infrastructure savings for the CSP.
- At the business layer, the integration involves common alarms, workflow, reporting and presentation. This allows users to share and collaborate effectively. Automation helps in faster issue communication and resolution, provided appropriate processes are set up and issues are summarized correctly.

Advantages of integration of tools:

- Integrated view of the revenue assurance and fraud management issues;
- Ease in impact analysis of enterprise wide issues at a management level
- Holistic problem resolution and workflow.

Challenges:

- Integrated platform that can address both revenue assurance and fraud management issues;
- Modes of operation of fraud management tool and revenue assurance tools are typically different. Due to the nature of the problem, its perceived impact on the business and economic considerations, fraud management tools are typically real-time systems whereas RA tools generally work in a batch-processing mode.
- Standard interfaces for tools to collaborate.
-

5.4.2. Key Benefits of a collaborative approach

Key benefits of a collaborative approach are:

- Faster issue resolution: A collaborative approach facilitates easy transfer of information from one system and team to another. This enables faster resolution of issues.
- Increased productivity through eliminated repetitive processes: A collaborative approach calls for tighter processes that are common to the different activities. It eliminates processes that are redundant and streamlines the activities.
- Resource optimization through shared infrastructure: Eliminate separate systems to address fraud and revenue assurance results. A collaborative platform can help in reduction of infrastructure.

6. Solution Approaches

The following chapter lays out a number of solution approaches to tackling revenue assurance. These approaches are drawn from a number of different service providers and software and consultancy vendors and intended here to highlight the breadth of approaches that are possible and the common themes underlying them all. There is a more lengthy discussion of the Maturity Model in the GB941b Guidebook.

6.1. Reactive vs. Proactive Revenue Assurance

6.1.1. Reactive, Active and Proactive

To be reactive is to do something as a response. To be active is to do something presently. To be proactive is to act in anticipation. From the perspective of assurance, reactive assurance occurs after something has gone wrong, as a response, whereas proactive assurance seeks to anticipate problems, so that they never materialize. Between the two falls an active response, still strictly speaking a response, but one where the time lag between cause and effect is so short we can disregard it. The definitions lend themselves to a categorization of revenue assurance activities:

- A project to identify and resolve the causes of historic revenue loss is reactive.
- Monitoring of problems in real-time designed to instigate corrective responses before any revenue loss takes place is active.
- The implementation of controls and other measures to prevent problems is proactive.

6.1.2. A Trend between Maturity and Timing of Action

We can observe tendencies for maturing revenue assurance departments to shift from reactivity to proactivity. However, not all the revenue assurance activities will develop at the same rate. The degree of proactivity will relate to both the general maturity of revenue assurance and the maturity at satisfying each specific objective. A mature and proactive function will still tend to start with a reactive approach when increasing its sphere of influence to an unfamiliar subject area.

The trends in timing of actions follow two distinct patterns, often confused because they can occur in tandem.

There is a tendency to reduce the time taken to respond to problems, in order to reduce the loss that occurs before correction takes place – a shift from reactive to active assurance. There a number of ways to do this:

- reduce the intervals between the activities that detect problems to the point where they become continuous (a shift from a project or review approach to a real-time monitoring approach);
- automation of assurance to speed the processing of large amounts of data;
- improvement in times to resolve incidents; and
- through obtaining data on problems extracted from points that are increasingly close to the root cause (e.g. identifying missing records from controls in mediation rather than inspection of bills).

There is a tendency to supplement a responsive approach to assurance with a pre-emptive approach. The goal here is to anticipate what can go wrong and seek to prevent it. Some of the techniques are:

- explicitly including revenue assurance considerations into decision-making for designs, procurement, etc;
- maintaining communication channels to assist co-ordination and ensure goal synergy when changes involve more than one organizational unit;
- risk management;
- avoiding unnecessary complexity and encouraging flexibility and future-proofing.

We can crudely map the response times to maturity as follows:

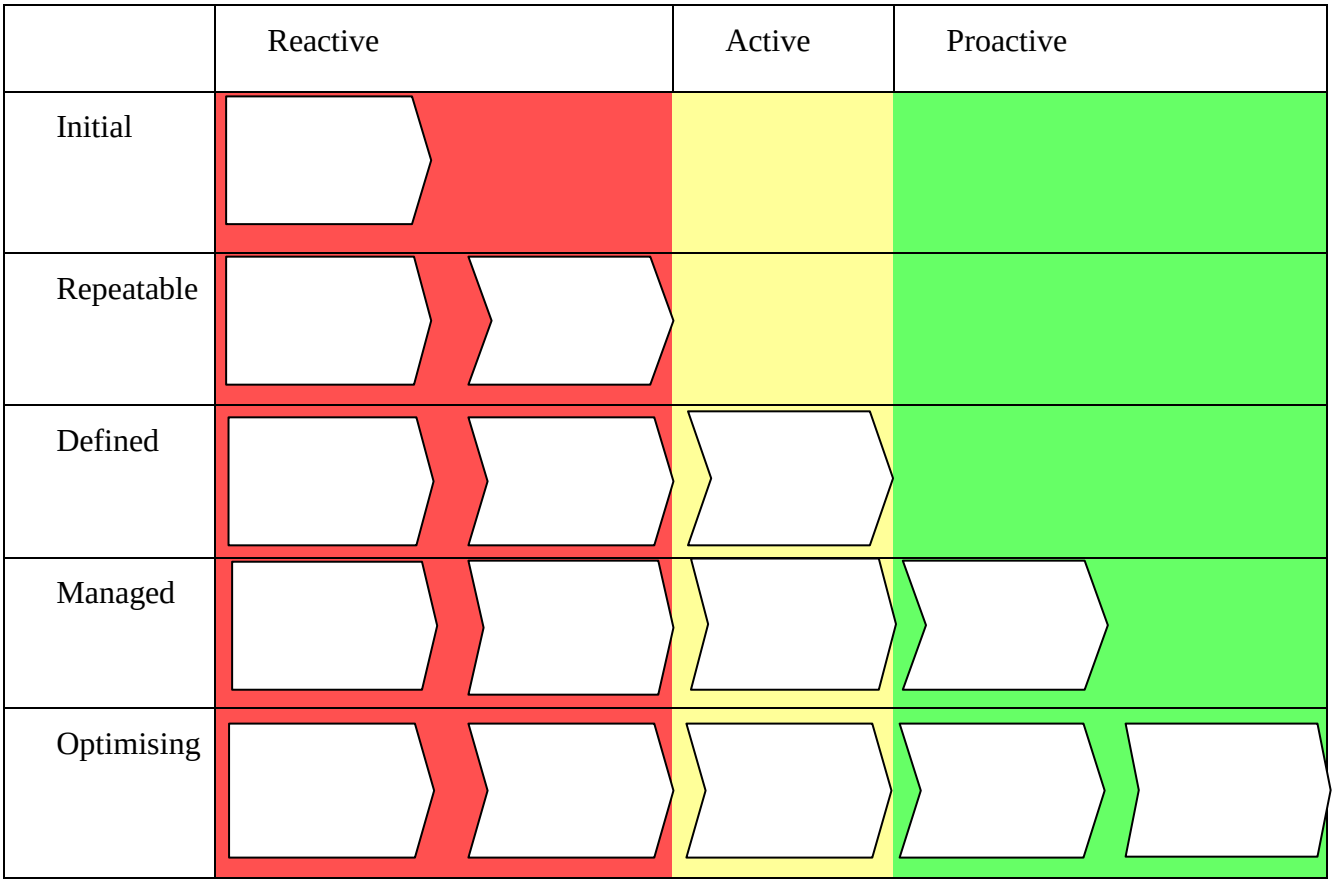


Figure 6-1 Simple Link of Maturity to Proactivity

This chart is over-simple, in that there is no single answer on whether prevention will be more or less cost-effective than detection and correction. Hence, this crude mapping associating preventative controls with increased maturity fail to represent that increasing maturity should also mean constant improvement of all of the reactive and active elements of revenue assurance. Arguably, any business should consider a blend of reactive, active and proactive approaches to all aspects of assurance because it will be difficult to predict which methods will find which particular errors.

Some errors may be easier to prevent than detect, some may be most cost-effective to find and correct using continuous monitoring, and some may only be found after slipping through the net and being caught by a one-off review. So whilst becoming increasingly proactive is generally desirable, this reduces to two distinct approaches to improving efficiency, which can be mapped on a timeline as shown in the diagram below. Increasing proactivity can be taken to mean a shift from

- reacting to errors to preventing errors (reactive to proactive); or
- reacting more quickly to errors (reactive to active)

There is a definitive point in time that distinguishes proactive or preventative assurance; it takes place before an actual error occurs. The difference in time between reactive and active assurance, though, is not so easy to define. This may be best left to each business to define for itself. For example, the difference between active and reactive monitoring may be that active monitoring occurs before the problem is represented on an actual bill, reactive only after, but this distinction may be academic if there is insufficient time to correct the problem before the bill cycle. A distinction based on time of billing is also unhelpful when analyzing errors in updates of prepaid accounts. The concept is useful in that there may be a temptation when discussing the desire to be less reactive to overlook the completely different nature of approaches designed to *anticipate* errors before they occur, and those designed to *improve timeliness* of monitoring and correction of errors after they take place.

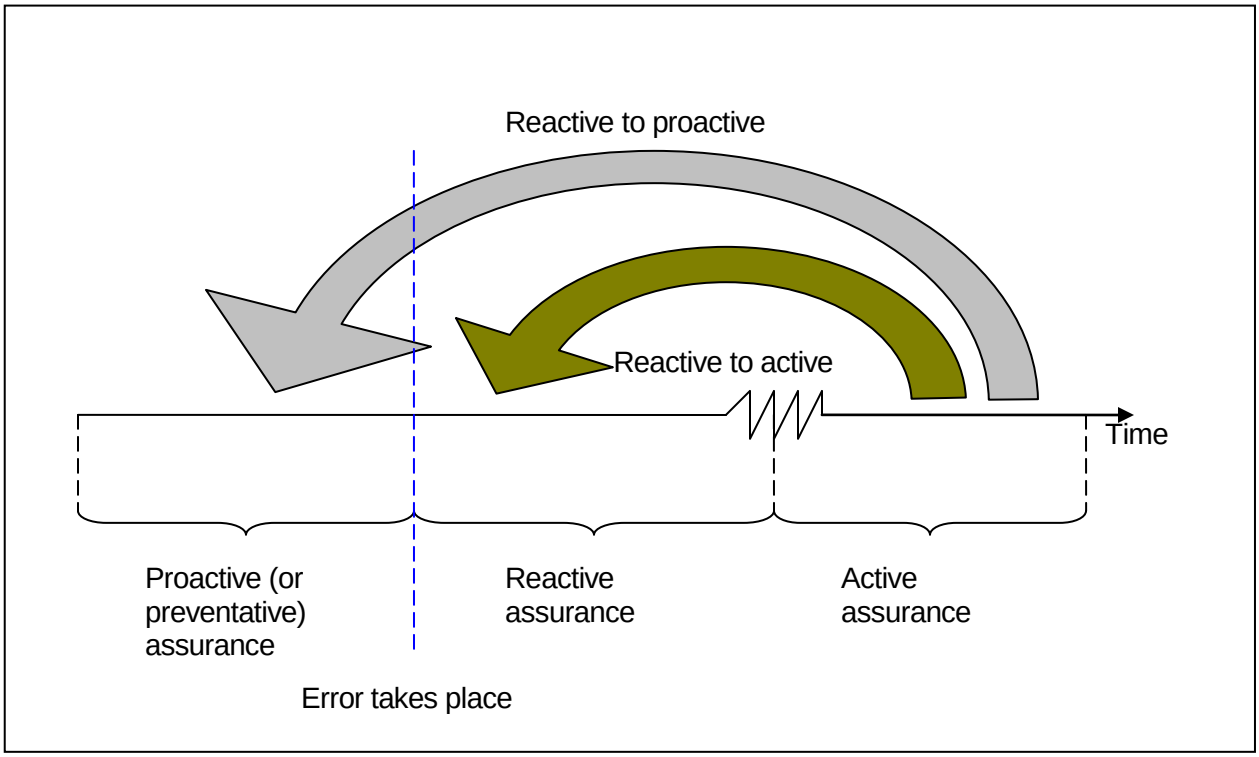


Figure 6-2 Two Kinds of Increasing Proactivity

6.2. Data Quality vs. Process Improvement

Revenue assurance is an important activity for any Service provider that wants to ensure they are billing for all the revenues to which they are entitled. There are fundamentally two different approaches to ensuring capture of all revenues, both of which have advantages when well implemented but also have disadvantages when applied in isolation. This chapter compares and contrasts these two approaches.

6.2.1. Data Quality

The first approach centers on improving the quality of data to ensure accuracy of revenue.

This normally involves the extraction of data, from either one or a number of systems, and validation that there is consistency in the data moving from network to billing and/or that any data added to a record is valid and correct.

The approach taken varies depending on the type of revenue assurance activity that is being undertaken. The following is an example of the steps that would typically be undertaken for providing assurance that CDRs are being are being correctly guided through the mediation process.

- An extract of CDR files is taken prior to processing by the mediation system (extract A)
- An extract of CDR files is taken following processing by the mediation system (extract B)
- An extract is taken of any error or discard files generated by the mediation system (extract C)
- Business rules for determining what the mediation system does with CDR files and how error and discard files are managed are collected

Independently of the mediation system, the business rules are applied to extract A and the output is matched against extract B on fields identified as critical for revenue assurance. This includes matching fields across the two extracts, such as date/time, duration, A number, B number as well as independent re-calculation of any values generated by the mediation process, such as destination name, distance band and product or service used.

Where CDRs in extract A are not identified in extract B, these are further matched against the error and discard files to determine how they were handled by the mediation system or supporting business process.

Revenue leakages can then be identified through the following outputs:

- Inconsistencies in data in fields critical to revenue between extract A and extract B
- CDRs missing between extract A and extract B, not accounted for in error or discard files
- CDRs that have been incorrectly placed in a discard file
- CDRs that are in an error file because there is inadequate data in extract A to allow for the mediation system to process the CDR

Adopting this approach to identify revenue leakage has the following key benefits:

- Knowledge of the processing within the platform is not required. The approach that can be taken compares what there is against what there should be, without the need to understand the detail of how this is accomplished by the core system. This means that revenue leakage could be identified due to reasons not necessarily identified as a potential risk if a process review was undertaken.
- Quantification of the extent of any leakage can be easily quantified assuming the sample size is sufficient. This allows for prioritization of resolution activity against financial returns.

There are also a number of dependencies and potential weaknesses in this approach. These include:

- Desktop software is unlikely to be able to either manage the sample size needed or be able to reflect all the potential complex business rules that apply. The software used needs to be able to cater for different formats and constructs of data, which may not always be ready for extraction from an operational or business support system. Typically a customized or off-the-shelf revenue assurance software product is needed.
- The output of the analysis depends on the business rules that are captured. Failure to capture all business rules can lead to false positive results where leakages are claimed that do not exist. This can undermine the confidence in the business of work being undertaken in revenue assurance. This can be particularly difficult when rules are not easily accessible or held on complex, individually negotiated contracts such as for corporate customers or interconnect and wholesale partners.
- In addition, business rule interpretation can be open and any identified discrepancies may be the example of different views of seemingly simple phrase. As above, this can lead to issues with business acceptance of revenue assurance findings.
- The quality of data presented for analysis needs to accurately reflect the operational or business support system that is being tested if conclusions drawn about leakages are to be complete. Data from data warehouses or data marts is at risk from being changed through an ETL process.
- Interpretation of exceptions can be difficult, especially if significant numbers are identified. Drill down and business intelligence applications are often needed to assist in determining what commonalities exist between exceptions and how these may indicate a possible reason for revenue leakage.
- Identifying the cause of the leakage can be problematic if the processes of the platform are not understood. Even more difficult with this approach is identifying the root cause that caused a problem, as these are very rarely revealed by data analysis alone. This can mean that an issue is fixed but the underlying problem is not and so either the issue can reoccur at a later stage or other issues relating to the failed process can cause revenue leakage.

6.2.2. Process Improvement

The second approach revolves around process improvement.

This is normally done by a review of the business processes that support the generation and management of revenue generating events. Adopting an audit style

approach, the critical path of revenue is mapped to identify where potential areas of exposure could exist. This could be around system functionality, handovers across systems, supporting business processes or interaction between processes and systems.

The approach is more generic in its approach in that business processes mapping is not dependent on any vagrancies associated with file and data manipulation. The following is an example of a process driven approach to the same problem as above, validating that CDRs are being correctly guided through the mediation process.

- The process (system or business) for collection of files into the mediation device are understood including any control processes
- The processes for how the mediation device handles calls is understood, including any business rules
- Finally the process for how the mediation device outputs any calls is understood and mapped

Exact revenue leakages cannot then be identified, as there has been no evidence that a process has failed as expected. Typically recommendations would focus on the controls in place to ensure the process is performing as expected and the following outputs can be expected as part of a process improvement assessment:

- Business knowledge in how a process operates is identified as needing improvement either through dependence on a third party, lack of understanding internally or inadequate documentation of the process
- A lack of control and check mechanisms can be identified whereby if there were a revenue leakage then there would be no method to identify it
- Existing controls in place are inadequate for identifying potential revenue leakage in a way that allows the organization to respond in a timely manner. This though can be more dangerous to an organization that has false confidence that the controls they have in place are adequate when they are not.

Adopting this approach to identify revenue leakage has the following key benefits:

- Skill with data manipulation or IT knowledge is not needed. Skills associated with questioning to understand an approach can be applied across different network or business domains.
- Often an identified weakness in a process, resolves the root cause of a number of problems, without even knowing the extent of the problem.

There are also a number of dependencies and potential weaknesses in this approach. These include:

- There is no data to support recommendations for process improvement. This can make calculations of business case benefits difficult to justify and means revenue assurance needs to adopt a similar “what-if” style approach as usually deployed to sell fraud or security prevention measures.
- Process improvement relies on correct understanding of the entire process, which can be problematic for complex processes with many interactions across the organization.

- Process improvement relies on the revenue assurance area knowing where all potential leakages may exist. This needs a skilled and experienced approach and knowledge of the area to identify where revenue leakages may exist.

6.2.3. Combined Approach

This chapter suggests that a balanced approach between data analysis and process improvement is recommended and that revenue assurance really adds value to an organization when these two powerful disciplines are combined.

This can be performed either with data quality or process improvement approaches leading.

If data quality is first, then the following is a typical approach that is undertaken.

- Data is extracted from various points in the revenue stream or from offline data repositories and reporting systems.
- This data is initially analyzed to determine potential areas of revenue exposure that should be considered so that resource can be directed at the target likely to yield the greatest return. This assumes that resources of finance, time and expertise are limited and some prioritization effort must be undertaken prior to commencing an RA activity. In reality, the scooping effort to determine the best places to search for revenue leakage can take some time depending on the level of confidence that the service provider requires before starting work. However, there are rarely clear indications of where revenue leakage will be found as if these were known and the extent understood, and then there is little value in an RA activity repeating work in the same area.
- Once a target is determined, the next step is the same as the data quality approach whereby business rules are collected, data is extracted, processed and subsequently analyzed and the results are made available for resolution.
- Initial efforts can focus on ensuring that the identification and quantification of leakage and opportunity is correct. This will typically identify the exact cause of a leakage but not the root cause.
- The next step uses the process improvement approach to identify which control failed, or was not in place, that allowed the revenue leakage to occur. Whereas process improvement takes an overview of the revenue stream, the combined approach can be targeted on processes that are known to have caused leakage problems because the quantified analysis is available. Driving process change is usually more easily accepted by the business when there are clear business benefits.
- By fixing the root cause of the problem, the benefits to an organization are likely to even greater than the initial data quantification that triggered the activity. A process with sufficient controls in place to prevent revenue leakage will yield benefit to all revenue activity that flows through the process. For example, a root cause of a tariff inaccuracy was identified as being due to lack of validation testing prior to launch. A validation process was instigated and then all subsequent tariff plan changes will benefit meaning that future leakage is prevented. Quantifying the benefit of this though can be difficult.
- Assuming the root cause and initial leakage are not resolved, the next step is to consider further leakages that may occur because of the process failure. In the

example of tariff plan validation, this would mean that all tariff plans should be considered for review as they have been created out of a leaky process. Depending on the product or service and priorities of the organization, the range of extended data quality testing off weak processes may be significant or minor.

The second approach is to adopt a process improvement strategy first and the following steps could be undertaken:

- A process improvement approach is initially taken as outlined earlier in this chapter where process and systems activities and handoff are documented and potential revenue leakage points identified. This stage allows for the creation of various theories on where an organization may be exposed to revenue leakage.
- These theories are then tested using a data quality approach on a specific portion of a process or system. Whereas data quality may have taken complete revenue stream and followed this end-to-end, this approach lends itself to smaller more strategic initiatives. An example may be where error files are identified as a high revenue leakage risk.
- If the data quality exercise yields a quantified revenue leakage, then resolution of the root cause is more easily undertaken as the processes are already understood.

6.3. Best Practices

Traditionally the revenue assurance function has been carried out by CSPs' finance department, and typically involved some sort of audit function, such as validating that invoice totals closely match previous billing cycles' totals. Today CSPs acknowledge that revenue assurance initiatives must go far beyond this narrow scope. Recognizing that data integrity errors can be introduced anywhere in the revenue chain, and not only lead to revenue leakage but also incur unnecessary costs, CSP are now formulating comprehensive strategies to ensure the accuracy, completeness and timeliness of data across the entire revenue lifecycle. This includes network element configuration data, OSS service activation data, usage data, mediation rules, and customer account data from order entry, billing and CRM.

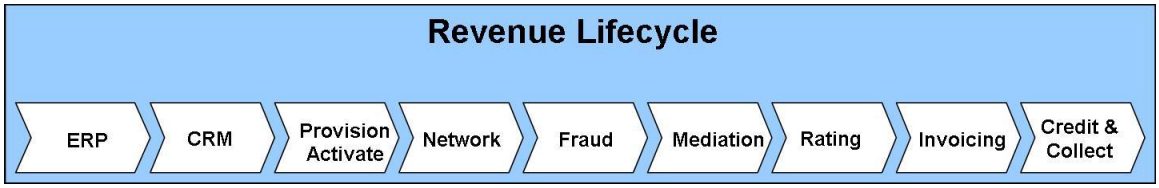


Figure 6-3 Revenue Lifecycle

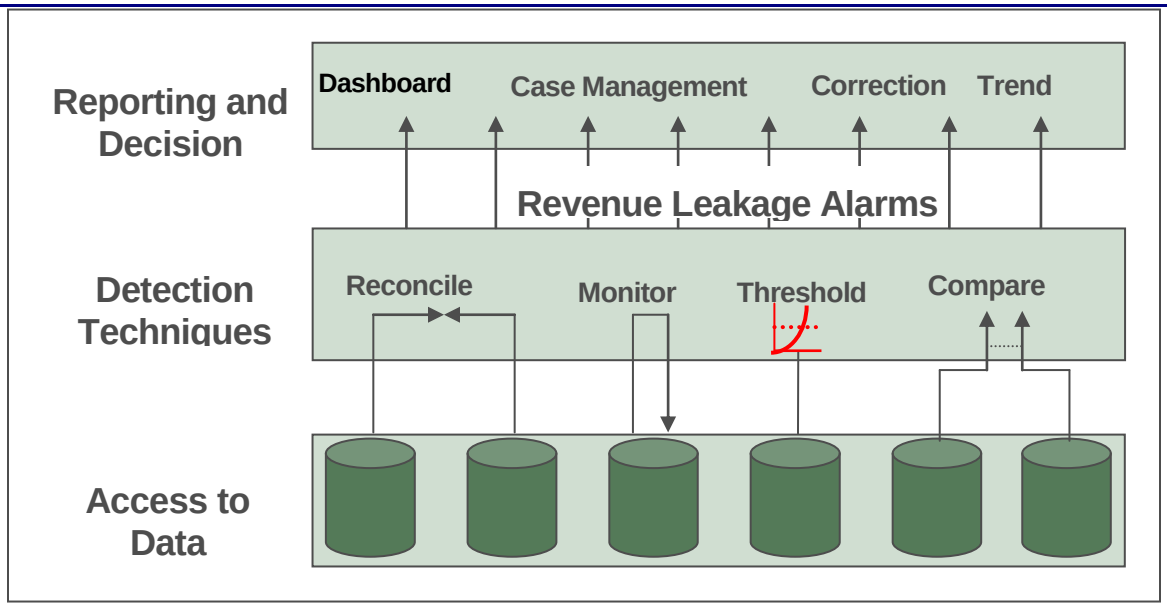
Given the complexity of a CSP's operations, effective RA strategies must rely on three key components - technology, people and processes - to accomplish this goal. Since RA programs spans across complex network technologies, sophisticated IT infrastructures and complicated business processes, a holistic approach is required.

Identifying data discrepancies and prioritizing the correction efforts is a daunting task, and can only be carried out with software support. The challenge of RA is to continually detect integrity problems in a large, complex and constantly changing body of multi-sourced data; prioritize those problems according to their impact on the business; correct the highest priority problems quickly; and prevent the problems from recurring. To overcome this challenge, RA programs must deploy scalable software technologies to monitor and audit data flows at key control points in the revenue chain. When abnormalities occur, RA analysts and subject matter experts need online tools to quickly investigate the suspicious data to determine the validity of threshold violations. A comprehensive resolution management framework is also needed in order to swiftly facilitate the corrective actions, determine root causes and guide overall process improvements to ensure such errors do not recur.

In addition to a robust and scalable technology foundation, successful RA programs must rely on proven methodologies and deep domain expertise. This in-depth knowledge must include a solid understanding of the complex interdependencies among network infrastructure, B/OSS environment and business processes in CSP's operations. Fundamentally, all effective RA programs have three process steps in common:

- Detect - extract and reconcile source data from key control points
- Correct - analyze and validate data discrepancies; classify, prioritize and resolve data integrity errors
- Ensure - provide a continuous feedback loop to report on RA program results, identify root causes, and drive process improvements
-

Based on this notion, RA programs must be designed to support data acquisitions from network elements, provisioning systems, mediation platforms, billing systems, etc. without being obtrusive to CSPs' operations and mission-critical support systems. The following picture depicts Yankee Group's key characteristics of revenue assurance functions and processes.



Source: Yankee Group, July 20, 2004

Figure 6-4 RA Dashboard

Key to an effective RA programs is a thorough understanding of the nature of revenue leakage. Once understood

Key to an effective RA programs is a thorough understanding of the nature of revenue leakage. Once understood, a balanced, holistic approach can be developed to ensure the success of a revenue assurance organization.

6.3.1. Best Practice Conclusion

It can be seen therefore that best practice in revenue assurance represents a dynamic striving for optimization rather than the static delivery of a particular series of methods, controls and tools. It also follows that any assumptions of how to attain best practice are subject to perpetual review and, where suitable, revision. This means that whilst the evolution of best practice requires industry-wide evolution, differences of opinion must be openly recognized. Stating differences of opinion on how to best optimize performance is itself important to the maturation process. Identifying and resolving disagreements on the basics of a discipline enables the discipline to progress and an incremental improvement in the cannon of working knowledge to those working in the discipline. This leads to an organizational approach that can best be described as a Revenue Assurance maturity model.

Appendix A: Terms and Abbreviations Used within this Document

A1. Abbreviations and Acronyms

Abbreviation/ Acronym	Abbreviation/ Acronym Spelled Out
eTOM	Enhanced Telecom Operations Map
SID	Shared Information Data
RA	Revenue Assurance
TMF	Tele Management Forum
CSP	Communications Service Provider
RFI	Request for Information
RFP	Request for Proposal
COTS	Commercial of-the-shelf
CPI	Comparable Performance Indicators
BT	British Telecom
IPR	Intellectual Properties Rights
NGOSS	New Generation Operations System
IP	Internet Protocol
ISP	Internet Service Provider
VoIP	Voice over Internet Protocol
OSS	Operation Support System
BSS	Business Support System
CDR	Call Detailed Record
KPI	Key Performance Indicator
PSTN	Public Switched Telephony Network
ABE	Aggregate Business Entities

ISV	Independent Software Vendors

A.1.a Usage of the Phrase "Revenue Assurance"

An exercise was undertaken to analyze current usage of the phrase "Revenue Assurance" compared to the usage on 2004 when the 1st version of TR131 was written.

The first Internet search was conducted using www.yahoo.com over several days in August 2004, the second search was conducted in December 2007 using www.google.com. Where relevant, repeat searches were conducted using variations on spelling, words with the same root (e.g. "rater" and "rating") and using a variety of synonyms where it was unclear which particular word would be most commonly used (e.g. "cash" and "money", "cost" and "expense"). The number of hits of the most popular variant of a search expression was recorded and other results ignored. The summarized results were as follows.

Search Expression	Number of Hits 2004	Number of Hits 2007	2007 percentage of 2004
"revenue assurance"	168,000	**518,000**	**308%**
"revenue assurance" + communications	139,000	**354,000**	**255%**
"revenue assurance" + provisioning	123,000	**59,500**	**48%**
"revenue assurance" + billing	107,000	**357,000**	**334%**
"revenue assurance" + leading	105,000	**325,000**	**310%**
"revenue assurance" + mediation	98,000	286,000	**292%**
"revenue assurance" + cost	73,800	44,300	**60%**
"revenue assurance" + order	55,000	**106,000**	**193%**
"revenue assurance" + profit	31,000	**55,700**	**180%**
"revenue assurance" + experts	24,900	30,900	**124%**
"revenue assurance" + audit	15,400	**34,100**	**221%**
"revenue assurance" + rating	4,010	**116,000**	**2893%**
"revenue assurance" + cash	3,850	**96,000**	**2494%**
"revenue assurance" + switch	2,740	**276,000**	**10073%**
"revenue assurance" + margin	1,080	**15,300**	**1417%**

"revenue assurance" + governance	786	**12,900**	**1641%**
"revenue assurance" + "Sarbanes-Oxley"	434	**7,430**	**1712%**
"revenue assurance" + "best practice"	418	**3,960**	**947%**
"revenue assurance" + TMF OR tmforum OR TeleManagement	No Data	**11,900**	
"revenue assurance" + eTOM	No Data	**3,410**	
"revenue assurance" + SID	No Data	**4,490**	

Table 1 Internet Search Hits

The following conclusions were reached.

- The total number of links to "revenue assurance" increased from 2004 to 2007 by more than 300%
- In 2007 over 65% of the hits on the phrase "revenue assurance" was in the context of the communications industry. The predominant use of the phrase "revenue assurance" on the internet is in the desired context for this search, making it unnecessary to filter for other contexts where the phrase occurs.
- Similarly to 2004, in 2007 there were a high number of hits linking Revenue Assurance to various stages or platforms involved in processing customer requests or transactions e.g. "order", "provisioning", "mediation", "billing". This suggests that there is a general consensus that Revenue Assurance covers a broad scope of processing and is not specifically focused on any one system or process. In particular, this suggests that the phrase is not considered to represent a subset of "billing". Some of the stages in processing, whose link to "revenue assurance" hits was weak in 2004, were strongly linked in 2007, including the rating of transactions or the collection of cash which each of them increased by approximately 2500%, and each of them is linked to about 20% of linked Revenue Assurance hits. The most dramatic increase was of the "switch" the number of hits increased by 10000% and while in 2004 it was associated with less that 2% of the "revenue Assurance" hits, in 2007 it is associated with more than 50% of them.
- One process whose number of hits decreased significantly is the provisioning process; the percentage of hits was reduced from 73% in 2004, a number that certainly do not represent it relative weight today in RA, to a much more realistic 10% in 2007. The rest of the processes, billing, mediation, ordering, more or less maintained their weight relative to the total number of "Revenue Assurance" Pages.
- The billing, mediation, and switch are on 2007 the process most associated to "revenue assurance", followed by ordering, and rating.
- On 2004 about 50% of all hits link the idea of cost to Revenue Assurance, this number decreased drastically in 2007 to 8%, similarly, in 2004 about a 20% of hits linked Revenue Assurance to profits, in 2007 the linkage was reduced to 10%. There is a significant increase in the linkage between "revenue assurance and margin, from 0.6% in 2004, to 3% in 2007.

- In 2004 about 6% of hits linked Revenue Assurance to audit, this number decreased to 6% in 2007. But at the same time the links linking “revenue assurance” to governance, and “Sarbanes-Oxley” increased respectively from 0.5% and 0.2% in 2004 to 2.5% and 1.4% in 2007
- Uses of words like “leading” and “expert” confirm the expected bias towards marketing sites of suppliers of Revenue Assurance products and services. These terms were linked in total to 77% of the hits in 2004, and this ratio decreased a bit in 2007 to 69%
- Searches involving terms like “data” and “process” scored high numbers of hits but were excluded from the analysis as inconclusive because of the many different senses in how the words had been used in this context.

Appendix B: References

B.1 References

Reference	Description	Brief Use Summary
Project Charter	Revenue Assurance Project Charter	This document is a deliverable as stated in the original Revenue Assurance Project Charter
TMF Glossary	TMF Glossary made available to public and members Version 130	
TMF Project Management, Process and Methodology Documents	TMF Team Leader Handbook, TMF Process Guides, TMF Templates, TMF Template Guides, TMF Modeling Methodology Manual	Referred to during the collation and production of this document
eTOM	eTOM Solution Suite (GB921)	The eTOM provides the map and common language of business processes that are used in Service Providers.
GB922	Information Framework (SID)	The shared information and data model provides a “common language” for software providers and integrators to use in describing management information.
GB941	Revenue Assurance Guidebook, GB941	This guidebook is a practical tool for RA professionals. It offers real life examples of issues.
GB941-a	Revenue Assurance KPI Metrics Workbook	This addendum provides a hierarchy of Revenue Assurance Key Performance Indicators (KPI) at Strategic, Tactical and Operational level in 3 main categories.
GB941-b	Maturity Model	This appendix discusses a way to assess maturity of business activities to deliver revenue assurance objectives.

TAM	GB929 Telecom Applications Map	

B.2 Source or Use

Every reasonable attempt has been made to ensure that all information used in this document is attributed to its owner / author. This is done in line in the document.

B.3 IPR Releases and Patent Disclosures

This document may involve a claim of patent rights by one or more of the contributors to this document, pursuant to the Agreement on Intellectual Rights between the TM Forum and its members. Interested parties should contact the TM Forum office to obtain notice of current patent rights claims subject to this document.

To date, no claims of IPR or Patentable Interest have been identified.

Appendix C: Worked Examples

C.1 Introduction

It is notoriously difficult to explain Revenue Assurance without giving practical examples. On the other hand, examples often cause confusion to many who are new to Revenue Assurance. The biggest mistakes are:

- to assume that any list of examples is comprehensive, and fail to recognize that there are innumerable scenarios where revenue loss may occur and hence where Revenue Assurance can be applied;
- to assume that any one solution to a given problem is definitive, as there may be a variety of solutions to any given problem, and the correct choice will depend on factors such as cost, available resources, and any plans for future system or process change that would eliminate loss as a by-product.

We offer these three RA scenarios and direct the user to further their knowledge, with the exploration of the RA Guidebook, GB941.

The scenarios focus on services with recurrent charges (as opposed to minutes or bandwidth based charged services). The scenarios focus on how a revenue assurance discrepancy case is found and treated; the scenarios do not deal with the causes for the RA discrepancies (human errors, software errors, procedural errors, hardware problems, etc.).

C.2 Scenario 1 – New Service Activated, Billing fails to start

Context

A consumer orders a new service with recurrent charges, the service is activated, but the billing system does not receive the order to start billing

Description

- A revenue assurance system compares the information in the NMS or physical network, Provisioning/Activation system, Network Inventory system, authentication, and billing systems
- The revenue assurance system finds that the service is provisioned and activated at the network level, at the provisioning/activation system, and at the network inventory system, and that the customer is actually using the service, and yet that the user is not being billed.
- A RA discrepancy ticket is opened
- The ticket is passed to the Billing system/staff for generating the invoice; the customer is given the invoice, the RA ticket is marked as fixed
- The RA system checks the situation again, if it finds that the problem is solved then it closes the RA ticket; otherwise the RA ticket is reopened.

C.3 Scenario 2 – Ordering changes not applied during provisioning process

Context

A customer ordered a new service with recurrent charges (e.g., ADSL, Voice Mail), during the provisioning the order is changed, not all the systems are updated, the network is provisioned according to the updated order, yet the customer is billed according to the original ordered, the invoice has not been sent yet.

Description

- A revenue assurance system compares the information in the NMS or physical network, Provisioning/Activation system, Network Inventory system, and billing systems, the discrepancy is found.
- A RA discrepancy ticket is opened
- The ticket is passed to the Billing system/staff for correcting the invoice; the customer is given the corrected invoice, and the RA ticket's status is changed to fix.
- The RA system checks the situation again, if it finds that the problem is solved, it closes the RA ticket; otherwise the RA ticket is reopened.

Appendix D: Draft Vendor Standards

Purpose of setting RA standards

As discussed elsewhere in this document, the remit of Revenue Assurance can be viewed as a broad company wide end to end process initiative that crosses multiple departments, processes and disciplines. As such it can be seen to touch on practically any information system or network element that is deployed by a service provider. Accordingly at the very least it is incumbent upon these systems to record the pertinent operations that aid in the validation aspect of the Revenue Assurance processes or at least it should be. The scope of this discussion is focused solely on why the Revenue Assurance Practitioners might formulate a set of common metrics to enable the base hardware and software providers to better serve them and aid in delivering the key metrics and KPIs desired as a core feature of their products.

In the realm of product development the primary goal is typically to capture and deliver upon a common set of features that are universal to all potential customers and then to enable extensibility of the product to cover known cases that are particular to specific customers. From a software vendor perspective the key issue is one of standards or de facto benchmarks against which to measure capabilities. While every OSS/BSS based RFP contains at least the question 'Does your product provide revenue assurance capabilities?' if not a more complete section there is little in the way of requirements, common or otherwise against which to construct a response and more importantly a software or hardware module, which does, comply. More often than not the answer to the question is yes but only insofar as a generic reporting interface is provided and the capability to define statistical counters within the product to be reported against is available.

Revenue assurance is a hot topic and many of the independent software vendors (ISV) are touting these features as enhanced added value whereas one could argue as stated in "To the Max, Revenue Maximization: Capturing the opportunities within", Browning & Kumar (2003 Pwc) that these are simply functions that should always have been in the product.

If we consider the path to maturity that an service provider typically goes through from manual / ad hoc through to automated we see that there is little in terms of common approaches that can allow an ISV to actually build something in terms of automation that is not bespoke, hence the reluctance on their parts to grasp the nettle in any more than general low level terms such as the ability to define counters and the ability to define custom reports. This invariably leads to extended product rollouts as a lot of work needs to be done to deliver the necessary functionality and more importantly because these capabilities are being tacked on after the fact their cost in performance can be much higher than if they had been engineered into the product from the outset.

In order to justify this expense in terms of architecture and product development however the ISVs need to have some sort of yardstick against which to develop. Any initial reluctance in agreeing such common standards should be ameliorated by considering the value that standard formats and techniques have throughout the rest of the service provider processes say with GTP' or AMA for collection or billing, or TAP and CIBER for interconnect settlements without reducing the differentiation of the players

Benefits to the software vendor and service provider of a standards based approach

The key benefits that shall accrue from such a standards based approach to the requirements for Revenue Assurance are:

- The ISV has a base of common requirements to work from,
- The ISV has a justification for development in core engineering as the requirements are de facto or universal
- The ISV has an opportunity to build features from the outset rather than retro fitting or tacking on to the outside
- As standard evolves so too can the product offering
- The ISV has the possibility of being certified as RA ready by an external body such as the TMF, GBA or other
- The systems integrator or ISV can better estimate project delivery times as certain tasks are fulfilled through configuration rather than development
- The service provider knows that a vendor has a true base capability
- The service provider gets a product with built in features rather than an integration project leads to performance and credibility
- The service provider gets reports on KPIs out of the box
- The service provider can focus effort of RA team elsewhere rather than on the definition and development of base reports.
- The service provider can easily compare ISV offerings

Mediation straw man

The following is written as a straw man for how standardized RA requirements for mediation may be explained and communicated.

Mediation

Mediation consists of the following activities:

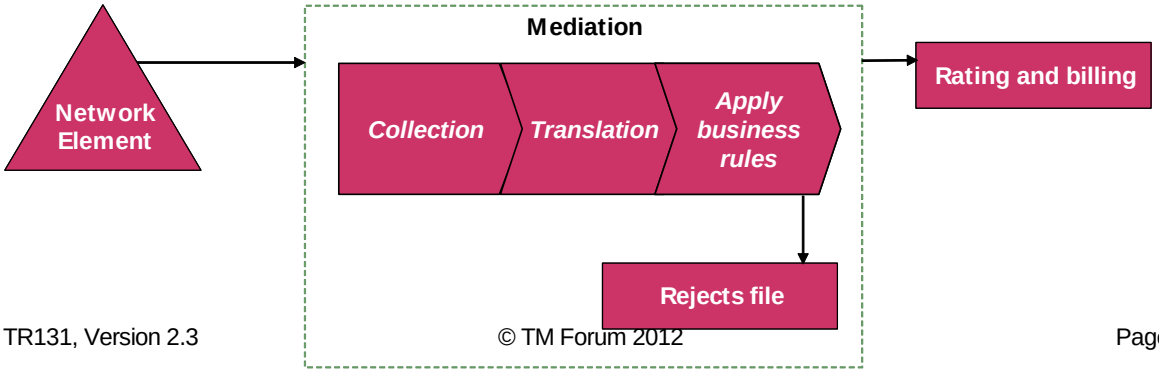


Figure D-5 Mediation Activities

Rejects can occur for a number of reasons including corrupt events, events not required for billing and events deemed to be non-billable due once the business rules have been applied.

Revenue Assurance Techniques for Mediation

The Completeness and Trending techniques are applicable for monitoring the flow of information through mediation.

Completeness Technique - Counts (events, minutes) are taken for inputs and outputs and the totals are reconciled, A=B+C+D+E or where reprocessing takes place A approximates B+C+D+E

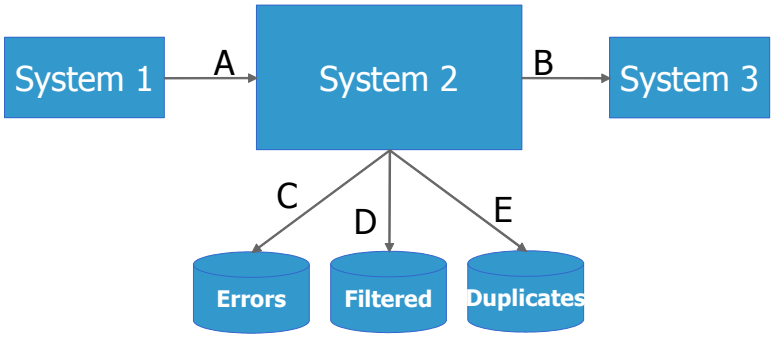
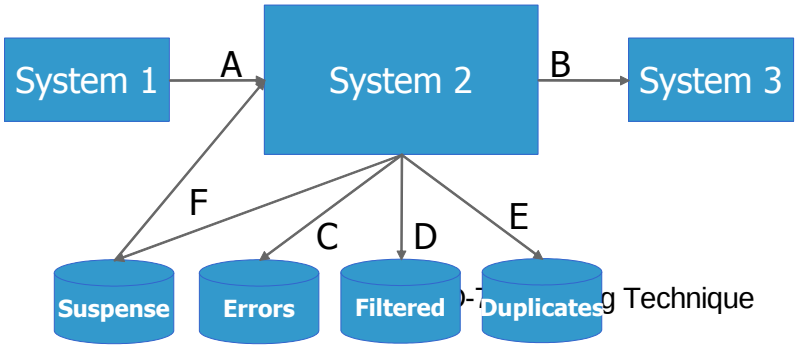


Figure D-6 Completeness Technique

Trending Technique – Counts (events, minutes) are taken for inputs and outputs and compared to historical information. Counts are typically taken at the total and event type level.



g Technique

Business Assurance Techniques that are applicable for mediation are:

- Reviewing the events that fall into the reject buckets
- Auditing the completeness, accuracy, validity and timeliness of the business rule data
- Using call generators to create events that exercise the business rules of mediation

Requirements for Vendors of Mediation Systems

The types of requirement for Mediation Vendors are:

- Provision of functional specifications: to enable the control design review to be undertaken by the service provider. Any gaps will be confirmed with the vendor and appropriate action undertaken.
- Provision of data feeds to the service provider's Revenue Assurance systems so that they can perform the techniques described above.

Typical controls that the service provider would expect to find when reviewing the functional specification would be:

- **Gap analysis:** The Mediation System should analyze the data that it receives from the network elements to determine if data is missing. Examples include:
    - **Time gap analysis:** Mediation should check the time and date stamp of the last file or event that has been received from the switch against the first time and date stamp of the next file or event received from the switch to determine whether data has gone missing. For example if the switch typically sends data every five minutes then this control would detect a ten minute gap between data sent and set off an alarm.
    - **Sequence number analysis:** Mediation should check the sequence number of the last file or event that has been received against the sequence number of the next file or event that has been received to determine if there are any gaps. This check will also for duplicates and allow mediation to filter them out.
    - **Statistical count analysis:** Mediation should count the number of events received and compare this to the statistical feed from the network element. For example the switch may provide a count of the events sent as well as sending the actual events. Mediation can then compare the two and highlight differences.
    - **Network element requirements**: For the gap analysis to take place, the network element will need to provide the following functionality:
        - Time and date stamps
        - Sequence numbering
        - Statistical data feed
- **Audit trail:** The Mediation System should stamp each chargeable event record that it produces with a unique number. This number can then be used for tracking the event from Mediation through Rating and Billing.
- **Reference data changes:** The Mediation System should provide an audit trail of changes to the reference data that it uses, such as the business rule data set.

Administrative Appendix

The Revenue Assurance Overview is being issued as Version 2.1. All documents approved by the TM Forum undergo a formal review and approval process. This document will continue under formal change control. Further work will be reflected in revisions to this document.

Document History

Version History

Version	Date	Purpose/Changes from Previous/Status
0.1	2004.11.01	Initial Draft
0.1.1	2004.11.11	Rework of 2.2.1 into a general plus telephony section, deletion of 2.3.1 title “mobile vs. wireline”, insertion of new section 3, deletion of headings 4.2.1 “CxO ownership” and 4.2.2 “central vs. distributed RA”, miscellaneous reworking of headings.
0.1.2	2004.12.09	Added Sections provided by Mike Willett (Telstra), André Kopostynski (Connexion), John Reilly (Metasolv)
0.1.3	2004.12.13	Completed all cosmetic updates and edits prior to final team review.
0.1.4	2004.12.17	Final edits pre distribution to TMF Membership
0.2	2005.01.21	Final updates prior to web posting for Member Evaluation.
0.3	2005.04.03	Final edits prior publications post TMF members’ evaluation to incorporate relevant suggestions
0.4	2005.04.27	Final edits prior to public offering of Member Evaluated version of TR131
2.0	2007.12.1	Updating document to accommodate the existence of the RA guidebook, GB941 and update relevant content.
2.1	2008.08.01	Addition of an Executive Summary at section 1.1, applied current template and mad other administrative changes.
2.2	2012.04.01	Alignment of terminology and graphics with Frameworx 12.0
2.3	2012.04.13	Notice updated, minor formatting and cosmetic corrections prior to web posting and Member Evaluation

Release History

Release Number	Date Modified	Modified by:	Description of changes
1.0	December 2004	Revenue Assurance Team	First issue of document
2.0	July 2008	Kathryn Dunham	This document is released as a single document in preparation for release 3.0 of the Revenue Assurance artifacts
2.2	April 2012	Steve Cotton	Alignment only.
3.6	April 2012		Alignment of terminology and graphics with Frameworx 12.0

Company Contact Details

	Revenue Assurance Team Leader
	Gadi Solotorevsky, cVidya
	Phone : +972 3 644 1644
	Fax : +972 3 644 1881
	email : gadi@cvidya.com

Use of Fonts

None Applicable

Time Stamp

This version of the Revenue Assurance Overview, TR131 Version 2.1, can be considered valid until further notice. As each version of the TMF131 document is made available, it can be assumed to supersede the previously numbered version.

How to obtain a copy

An electronic copy of this document can be downloaded at the TM Forum Web Site (www.tmforum.org), Publications or through a link to Publications from a specific team's public project area.

If the document version has only been released to members for review and comment, the document can be downloaded from the Members Only area of the TM Forum Web Site.

Paper versions can be made available for a small fee to cover copying, mailing and handling. If you would like a paper version of this document, please order via the TM

Forum Web Site or contact the TM Forum office. If you are not a member, please contact the TM Forum office on +1 973-944-5100

How to comment on the document

Comments must be in written form and addressed to the team editor for review with the project team. Please send your comments to the editor using the editor's e-mail shown in the Contacts Section below.

Individuals or companies who are not members of the TM Forum are encouraged to provide comments on this document. However, in order for their comments to be considered, a signed waiver must be on file with TM Forum pertaining to intellectual property rights. To obtain this form, please contact the TM Forum.

Acknowledgments

The Revenue Assurance Overview, TR131 Version 2.2 is an update from the version 2.1 and is required with the publication of the team's RA Guidebook GB941. The TeleManagement Forum would like to thank the RA technical team for their input into the required changes and the review of the changes made.

Kathryn S. Dunham, the Billing College

Gadi Solotorevsky, cVidya Networks

Eric Priezkalns, Revenue Protect Limited

Agbi Bajrushi, Stevens Institute of Technology

Neekunj Bhanderi, Stevens Institute of Technology

Debbie Burkett, TM Forum

We wish to acknowledge the original Technical Team members who created the first Revenue Assurance technical report, which was a genuinely collaborative effort

Gadi Solotorevsky, cVidya Networks

Eric Priezkalns, Revenue Protect Limited

Shane O'Flynn, Openet Telecom

Mike Willett, Telstra Corporation

John Reilly, Metasolv Software

André Kopostynski, Azure

Additional contributors of the original document include:

Paul Masters, KPMG

Ruth Cox – Azure

Viviane Cohen, Amdocs

Jaime Aronowitz, cVidya Networks

Hugh Roberts, TMF

Debbie Burkett, TMF

Ian Best, TMF

Nitin Patel, Cable & Wireless (UK)

Geoff Ibbett – Azure

Nilesh Karani – Convergys

Sachdeva Deepika - Siemens Information Systems

Vinoo P Jacob – Subex

Greg Fidler - Practical Enterprise Architecture P/L

The technical team would like to acknowledge the work, effort and validation results of the Revenue Assurance Catalysts. From this catalyst, results successfully validate the work of the technical team on the technical report and the guidebook (GB941).

Reactive to Proactive Revenue Assurance – Closing the Loop -- TeleManagement World Nice 2005 – Sponsors: China Unicom, TeliaSonera, Participants: Atos Origin, cVidya Networks Inc, Datamat SpA, Huawei, MetraTech Corp, Subex Systems Limited, WebMethods Inc

Sarbanes Oxley Catalyst - Sponsors: Internap Network Services, Mobile TeleSystems OJSC, TM Forum, Participants: Convergys, Casewise, cVidya, Ernst and Young, Subex Systems

IPTV Impact on FAB - Sponsor: Swisscom AG, Participants: cVidya Networks, Metratech, Microsoft, Nakina Systems, Syndesis, Tata Consultancy Services, The Billing College, Tigerstipe Software, Wipro

Revenue Assurance Catalyst - Sponsor: China Unicom; Participants: ATOS Origin, Convergys, cVidya, Datamat, Sonic Software

Revenue Assurance Standard KPIs (RASK) - Sponsors are China Unicom, Mobile TeleSystems and Swisscom. Participating companies are cVidya, Datamat, Ernst & Young, Microsoft, SubexAzure, and Tata Consultancy Services