Next Generation Revenue Assurance

Sunny Gajbhiye*

**Consultant, Ericsson, India*
Email: sunnygajbhiye@gmail.com

Abstract

In the increasingly competitive and fast-moving telecom environment, Mobile Network Operators are encountering a greater number of challenges to maintain their revenue. With eroding margins and looming cost pressure Telco's are facing great threats of long term sustenance, scalability and vulnerability toward revenue leakages.

The need of hour for Telco's is not only to monitor each and every billable transaction to retain and cover revenue, but also perform root cause analysis and provide strategic solution to the problems. This is where Next Generation Revenue Assurance (NGRA) comes into picture, which gives thorough results after incorporating business analytics and advanced analytics like analytic profiles and neural network models.

NGRA is facing challenges when it comes to the advancements and penetration of smart phones, enhanced internet connectivity, next generation mobile interaction, rising capex/opex and flat lining revenues. Besides these regulatory compliances, skilled manpower, handling high data volume and need of technology agnostic solutions are also the major hurdles in its path.

The next generation technologies have created a market place for NGRA to evolve. Next generation leakages, integration of RA and fraud management systems, advancements in processing and storage, mobile security risk management will drive NGRA. NGRA implementation would require Telco's to optimize their business strategies, processes, administrative structures and infrastructure. A successful implementation would be based on managed services, software as a service (SaaS) and RA consultancy.

NGRA will provide strong support to expose hard to detect leaks, increase productivity and ROI, lower total cost of ownership and will give bird's eye view of entire revenue chain. It will help Telco's in accelerating their decision making process and implementing go to market strategies.

Keywords: Revenue Assurance, Next Generation Revenue Assurance, Fraud Management

1. Revenue Assurance and Fraud Management in a nutshell

RA (Revenue Assurance) as a proactive BSS (Business Support System) practice of accurately reconciling the complete billing lifecycle from switch to bill generation and dispatch, minimizing bad debts and recovering revenue. RA is the process of ensuring all billable transactions are executed, rated, billed and collected correctly in a timely manner. In short, this is the assurance that maximum revenues are realized and that a product, customer, or operation is not losing money.

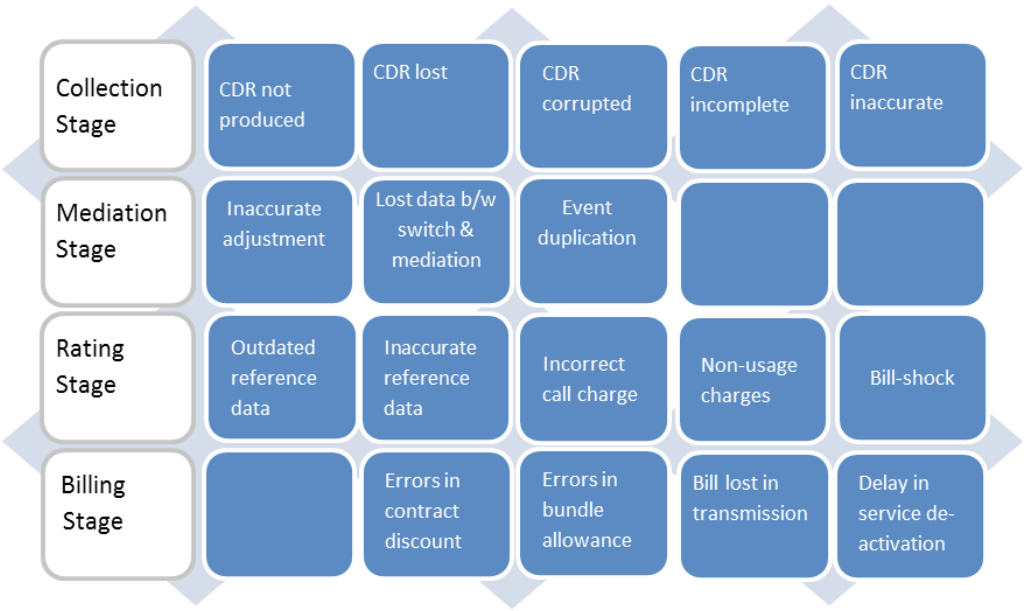
Fraud in an essence is a well-organized business and a criminal activity involving deliberate deception to a service or product illegally for financial or personal gain. Unlike RA, fraud is a non-recoverable loss. Cellular Service Provider limits such risks by installing a system to monitor and react to criminal activity in real-time, continuously feeding-back new rules and thresholds to minimize the threat of the event reoccurring in the future. Fraud management teams are concerned with individual cases and demographic-based data for identifying the location of criminal activity, the perpetrator involved and analysis of behavioral profiles.

2. The Threat of Leakage – A big issue

2.1. Revenue Leakages

At each point of the transaction there is a potential for a revenue leakage in the switch-to-bill process, from network, mediation, to billing, as well as those related to collections and dunning, provisioning and customer-service and product development. There can be a number of reasons that lie behind a leakage; these include poor order accuracy, incorrect client data within the system, incorrect service provisioning or process inefficiency and

Figure 1 Revenue leakages at various stages.



can take many different forms. In terms of mobile content commerce, a revenue leakage may be incurred as a repayment where there has been an incomplete download or non-delivery of purchase. A leakage can occur in equal measures for both pre-paid and post-paid accounts. Another cause of leakages may be the lack of cross-organizational standardization of KPIs, which undermines a broader business objective of cash-flow maximization. Leakages tend to occur predominantly earlier in the sales process whilst only detected downstream later in the customer-to-cash lifecycle.

2.2. Fraud Based Leakages

Unique to each case, it is almost impossible to classify fraud, often resulting in unconstructive over simplification. Instead, classification is based on the types of products and services that are stolen and then sub-classified by access points. Some commonly known frauds are listed below.[1]

- **Subscription Fraud** - Subscription fraud occurs at the activation stage; it is the act of gaining access to a product or service without having the intention to pay.
- **SIM-Cloning** - Hacking the ESN (Electronic serial Number) and making the two phones identical to the operator and resulting in charges made by the fraudster being billed unknowingly to the original, legitimate account.
- **Interconnect Bypass Fraud** - Having acquired a SIM (Subscriber Identification Module), a fraudster may attempt to bypass such interconnections, routing calls onto or away from the MNO's network, rather than generating interconnection terminated calls, by using cheaper, unauthorized routes such as VoIP (Voice over Internet Protocol).
- **International Call Bypass** - This is the act of placing off-net calls onto an operator's network but avoiding international gateway to evade the international inter connect charge.
- **PRS Fraud** - Having acquired network access, the subscriber might procure content or services charged at premium rate, such as chat-lines, television vote-lines, gambling, horoscopes, ringtones and logo downloads, charitable fund-raising lines, sports results and directory enquiry services with the intention of not paying for them.
- **Roaming Fraud** - Roaming fraud is the use of an operator's network outside the user's home country, wherein there is no intention of paying for calls made.
- **PABX (Private Area Branch Exchange) Hacking** – Through intelligent code-breaking ac-

Figure 2 A holistic view of frauds in Telecom Industry

tivity, fraudsters gain access to a company's IP-based switchboards (PABX) to make unpaid calls or other revenue generating frauds such as PRS fraud; illegitimate usage then appears on the company's bill.

- **Internal Fraud** - Due to detailed knowledge of the system and processes, telecom employees are ideally situated to attack the network at any point, abusing their permissions and access levels.
- **Dealer and Supplier Fraud** - Dealer fraud is the any activities performed by the dealer or supplier with the intention of depriving the MNO of revenue whilst increasing their own commission by abusing the terms and conditions of the contract.
- **M2M (Machine to Machine) Fraud** - This involves criminals tampering with SIM embedded devices to illegitimately obtain mobile services.
- **Malware and SIM Hijack** - With the rise of smartphone devices, the use of mobile malware and SIM hijack is undoubtedly on the increase, enabling fraudsters to acquire personal information and network access, running their bills to others' accounts and increasing illegitimate network data volume.

3. Contemporary Mobile Eco-System – The challenges faced:

3.1. Enhanced Internet Connectivity

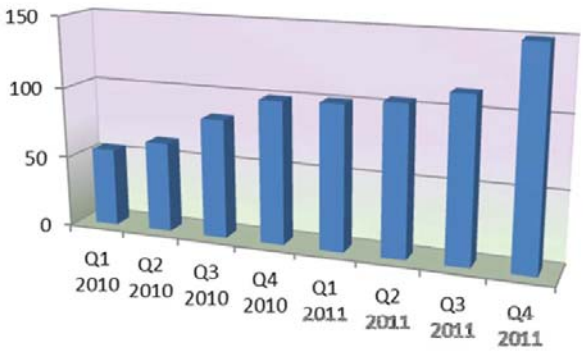
The surge in popularity of mobile transactions has indubitably been driven by the development of national UMTS/HSPA/3/3.5/4G networks in concomitance to the increasing availability of Wi-Fi, stimulating accelerated mobile device adoption and enhanced usage.

Yet whilst improved connectivity is enabling critical revenue channels, the availability of multiple access points presents a number of security risks wherein it is difficult for the operator to ascertain ownership of the network and identify a consumer given that their IP location is constantly changing. The MNO must additionally rely on a number of third-parties to support network operations such as roaming and interconnect partners or other MVNOs (Mobile Virtual Network Operators).

3.2. The Advancement and Domination of Smartphones

The evolution of the smartphone device has revolutionized the mobile technology market, fundamentally transforming consumer behavior. Equipped with MP3 playback, cameras and gameplay also combined with the facility to download apps, consume popular content and share user-generated content, fundamentally differentiates smartphones from non-smartphones. The rise in smartphones reflects a global shift which is increasing the level of data volume encountered by MNOs on their network as they engage with a number of other industries to provide value-added services beyond simply voice and data.

Figure 3 Global Smartphone Shipment Volumes (million) over Q12010 - Q42011 – Source: Juniper Research[2]



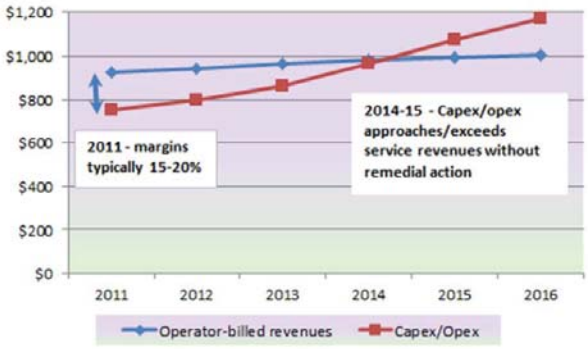
3.3. Next-Generation Mobile Interaction

The subsequent convergence in communications and internet computing has interconnected a broad range of industries positioning MNOs at the intersection for delivering next-generation connectivity and content. Consequently, RA and fraud management systems must further take into account whether offers and incentives are being realized with external parties. This has led to enabling 24/7 connectivity, encouraging new ways of communicating, reading, watching videos, banking, managing health and so forth. This is resulting in an inexorable growth in the wireless data traffic needing to be absorbed and processed by the mobile network.

3.4. Flat lining Revenues, Rising Capex, Rising Opex

MNO subscribers are expected to increase while on the other hand global ARPU is expected to decrease consistently as seen and forecasted based on previous trends. Revenues plateau, costs (both capex and opex) are rising. To meet the demands of consumers, MNOs must upgrade their networks to offer 3.5G and 4G services, thereby paying both for new spectrum and new infrastructure: during this transition (and beyond) they must cope with the surge of traffic endangered by the consumer smartphone boom, which has implications both from a network congestion and cost perspective.

Figure 4 The 'Nightmare' Scenario: Global MNO Service Revenues vs. Capex/Opex ($bn) 2011-2016 – Source Juniper Networks[3]



4. An Evolving Marketplace for Next Generation Revenue Assurance:

4.1. Next-Generation Leakages

Revenue management is becoming increasingly more challenging as MNOs move towards next-generation services and content provision, ineluctability increasing the incidence and nature of business risk. The proliferation of new data services has increased the incidence of billing problems with frequent additions and alterations

in offerings, new and additional billing systems, unfamiliarity with an event and content-based billing and converged billing systems. Operators will need to adopt greater real-time functionality for responding to fraudulent activity by being able to monitor and identify a typical usage behavior from a provisioned SIM card.

4.2. Tiered Data Pricing: a Billing Headache?

In order to better monetize their networks and data services, MNOs are moving away from unlimited data packages for a fixed price; such plans tend to render the network vulnerable to heavy bandwidth consumption, high volumes of data and therefore leakages, with operators gaining no more incremental revenue. Instead, using online charging and policy, operators are now able to offer tiered-service and value-based price plans and personalized packages that better corresponds revenue to consumption, usage patterns and in some cases, quality of service. As a consequence of the smartphone revolution, MNOs have significantly expanded their portfolio of available cell-plan packages resulting in mediation teams struggling to ensure correct billing and rating.

4.3. Integration of Revenue Assurance and Fraud Management Systems

The Telco's are observing a considerable level of integration between RA and FMS functionalities by exploiting technical synergies. Such a development is in recognition that the two areas are partly related and complementary given that both teams require the same billing, customer and usage information. MNOs are seeking greater cross-domain cooperation facilitated by capabilities such as case-management, allowing both teams to work together on cases and share reports to gain a greater cross-organizational review.

4.4. Formalized Business Perspective

Over the past two years, RA has moved significantly towards a 'formal risk management process'18, wherein operators are adopting an objective approach in identifying new revenue streams to be incorporated into the RA reconciliation process and their importance for generating a vast quantity of transactions and cash-flow. This has involved greater leverage of business intelligence capabilities that is allowing operators to integrate dedicated and proactive modules within their BSS to pre-empt network threats.

4.5. Advancements in Processing and Storage

Driven by cross-industry collaboration, the rate of technological innovation in hardware and software has been dramatic. Earlier an installation based on hard-disk technology might process on average 100 million events a day. Today; however, leveraging multi-core processers and SSDs (Solid State Drives), an average CPU is capable of running 600 million events per day. Similarly, there has been an improvement in data storage capacity, speed and costs. Vendors are now also offering cloud-based solutions: large, distant server farms providing virtual, online storage and hosted by a third party, accessible from various geographies which is becoming more attractive.

4.6. Mobile Security: Managing Risk in a 4G/LTE Environment

Moving into a 3.5/4G telecom environment, end-point and network security are becoming increasingly challenging, compounded by the accelerated adoption of smart devices and new technologies that is allowing consumers much greater control over the service than they did in the past. This new complex reality has engendered a level of co-ordination and integration of system security applications within the Revenue Management solution.

4.7. Cross-industry Co-operation and Re-Sale

As MNOs attempt to secure their end-to-end revenue stream more tightly and manage an expanded ecosystem, some vendors are increasingly observing that an MNO will purchase a RA and FM solution and re-sell or promote it to their dealers and content providers. This is part of a collaborative strategy to inhibit system after-shock and prevent leakages from a source point, bearing critical imperatives not only in terms of revenue, but costs, margins and company reputation.

5. Business Strategies for Next Generation Revenue Assurance:

5.1. Ensuring Effective Business Assurance

By exploiting a single repository of data, for optimum business performance, the RA and FM components should be able to easily integrate with and support other

mutually-beneficial BSS components such as margin assurance or customer experience management as well as OSS elements such as network management for complete Business Assurance.

5.2. Ensuring Next Generation Revenue Assurance Automation and Flexibility

Broadly, the automated infrastructure should be scalable enough to process large volumes of data from multiple sources, rapidly and accurately in real-time that can visibly improve time of resolution. Additionally, the solution should be flexible enough to integrate new internal and external data streams easily, ultimately providing complete visibility of the revenue-chain.

5.3. Optimizing the Administrative Structure

Telco's must distribute revenue management responsibilities strategically across the organization, creating a balanced organizational structure. Prioritizing improved inter departmental communication will increase the amount of available intelligence, improve end-to-end visibility and subsequently support the realization of high-level metrics that can facilitate co-ordination. RA and FM teams must be sufficiently educated and keep a-pace with the ever-altering threat environment provisioned with the correct skill-set and relevant experience.

5.4. Optimizing the Business Processes and Leakage prevention

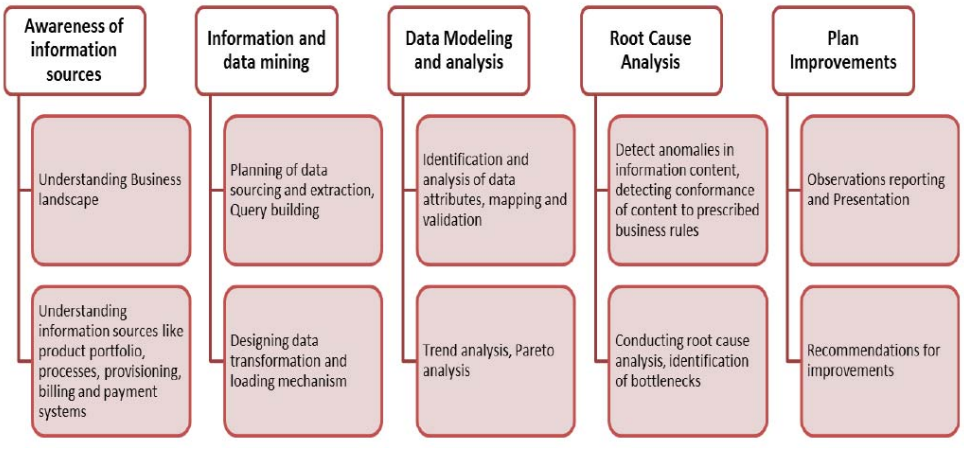
Not all revenue leakages can be predicted meaning it is essential to have a proactive component that can capture a problem by applying rule and profiling logic, combined with subscriber information. Yet if this component fails to identify the threat, the system should transform it into a proactive rule to be fed back in to the system having been captured at the reactive level. Having analyzed the structure of behavior, the system can then stop the problem almost immediately if it should occur again.

Prevention requires systems ascertaining the root-causes of revenue leakages. Adopting a prevention based strategy involves the use of case-modeling: a drill-down analytical process that is refined further to system modeling for investigating the logical system architecture, service design and data object or subject.

5.5. Optimizing Infrastructure for Next Generation Revenue Assurance

The infrastructure should be lightweight and modular-based to allow CSPs to add and detract applications, solving the most critical challenges first and proceeding strategically using a flexible, scalable and cost effective approach. Furthermore, the infrastructure should be self-learning, able to continuously feedback and integrate new rules to proactively secure the system.

Figure 5 Business Analytics Methodology in Telecom Revenue Assurance[4]



6. Next Generation Revenue Assurance - Advanced Methodologies

6.1. Analytic Profiles

Advanced profiling capability enables it to profile the behavior of customers. Unique profiles are automatically learned and maintained for each and every customer, and continually evolve to reflect a customer's normal behavior. In this way any anomalous and unusual activity is flagged up for investigation.

6.2. Business Analytics

Business Analytics approach helps support business with process re-engineering, re-organization initiative and large transformation initiatives by providing predictive analytical metrics and recommendations.

Below diagram illustrates Business Analytics.

6.3. Neural Networks

Neural Networks look at the nonlinear interrelationship between thousands of data points at a time. Powerful pattern recognition capabilities enable to recognize them subtle, hidden and emerging patterns of revenue leakage across the networks. The Neural Network models are trained on actual data to spot these complex data driven variable patterns associated with revenue leakage. As a result Neural Network based systems detect problems that providers don't even know they should be looking for.

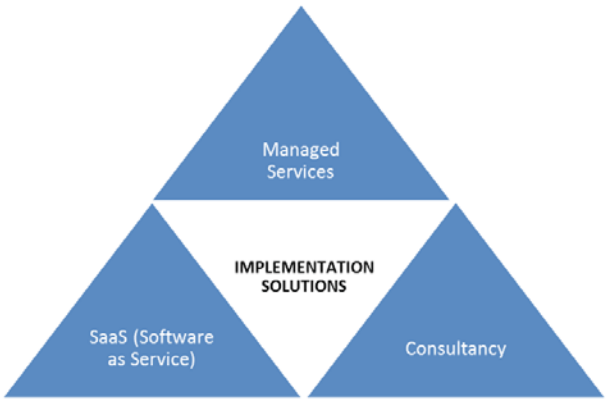
E.g. **Tromboning**: Neural Networks can detect revenue leaks from "Tromboning" by determining when the number of hops with interconnect carrier is unusual and inappropriate given contemporaneous network conditions and events.[5]

7. Implementation Solutions for Next Generation Revenue Assurance

7.1. Managed Services

Managed services involve a third-party ASP (Applications Service Provider) taking complete control of the full RA and FM process tailored to the MNO from implementation to deployment, followed by system maintenance and upgrade. The solution includes IT infrastructure, application management and business operations. Utilizing its own technology platform, the vendor is able to provide industry-level, domain-specific expertise with well-developed product expertise and well established processes. The vendor makes available a ready trained team to be rapidly deployed and rigorously managed, able to exploit the full capabilities of the IT platform. The solution can offer greater accountability by embedding strict, industry standard KPIs and SLAs (Service Level Agreements) reinforced by best practices and processes.

Figure 6 Implementation Solutions



7.2. SaaS (Software as Service)

An on-demand service, this is the renting of technology infrastructure from a third party wherein the Cloud can either be deployed on-site or hosted centrally via the vendor. An on-demand cloud-based solution can provide for the smaller CSP as an easy-to-use, pre-configured, software solution based on their data and fully web enabled and secure. Such a solution requires minimal capital outlay, low subscription feeds, no need for a dedicated infrastructure and no on-going maintenance charges. Instead software upgrades are automatic, integrated into the hosted platform. The offering provides for real-time data processing, intuitive user interface, built-in tutorials, online community support and robust alarm management, workflow and reporting.

7.3. Consultancy

Consultancy services enable customers to be able to focus their efforts in a particular area where is necessary by providing up-to-date, relevant industry expertise. The process of consultancy is to demonstrate value-adding services and to realign the RA and FM teams mind-

set to a formalized risk management perspective rather than a short-term fix. Essentially, the vendor takes a risk assessment of the CSP environment and recommends appropriate solutions. Indeed, consultants are able to assist CSPs to sort through vendors and construct a system with specific functionalities purposeful for their organization aligned to cost structures. This might be a more applicable solution in developing markets where operators cannot afford to put in a fully-fledged RA and FM system.

8. Conclusions and Strategic Recommendations

Clearly, revenue leakages cannot be reduced to zero; this is the hard reality that Telco's must accept while operating in an innately risky environment. As we move rapidly towards 4G/LTE connectivity, the volume of revenue leakages is set to accelerate yet more dramatically with operators having to manage an extended, more complex revenue chain and to incorporate data from multiple internal and external sources.

Some of the remedial measures to establish a 360-degree, customer-centric perspective of the business and e2e visibility of the revenue chain would be acknowledging that loss can occur at any point within the transactional life cycle. Fundamentally, this begins with implementing an automated revenue assurance (RA) and fraud management (FM) system that replaces manual processes no longer able to manage the expanded volume of cellular network traffic, particularly from data services.

Some of the strategic recommendations are listed below:

8.1. Operators Should Deploy a Single Technology Platform

Given that both RA and FM utilize the same data, operators can and should deploy a single technology platform that enables both sets of operations.

8.2. The ETL(Extract Transform and Load) Platform Should Allow Real-Time and Near-Real Time Analytics

The ETL platform should operate in both real-time and near real-time to continuously extract data, transform it for operational requirements and load it into an end-storage to be made readily accessible to analytics. The infrastructure should be self-learning, able to continuously give feedback, to integrate new rules and to proactively tighten the system.

8.3. The System Should be Flexible

The infrastructure should be lightweight and modular-based to allow CSPs to add and detract applications, solving the most critical challenges first and proceeding strategically using a flexible, scalable and cost effective approach.

8.4. The System Should be Self-Learning and Intuitive

Whilst systems must necessarily be reactive, as they mature they will become increasingly preventative by applying rule and profiling logic, combined with subscriber information. E.g. using predictive analytics and neural networks.

8.5. The Business Support System Should Enable 360 Vision of The Business by Integrating Complementary Business Applications

It is insubstantial to simply have standalone RA and FM systems operating in independent silos. Instead, there should be greater cross-departmental communication for realizing broader business objectives that align revenues with costs and margins, enabled by KPIs.

8.6. Operators Should Adopt a Formalized Risk Management Approach

The telecom industry often operates in an ad-hoc fashion, reacting to the 'latest', so-called threat rather than maintaining consistency. Through cross-industry cooperation, operators should assume a more formalized risk management approach.

8.7. RA and FM Teams Should Collaborate with Mobile Security Teams

Handling large volumes of sensitive data, operators should seek greater co-operation with mobile security vendors that can protect the network infrastructure and

the end-device, allowing comprehensive and mutually beneficial risk management.

8.8. Operators Should Enlist Consultancy Services to Select an Optimal Solution

All operators should engage consultancy services as a critical component of the process. Consultants can assist in enabling more focused investment by undertaking a risk assessment to recommend appropriate action and to construct a system with specific functionalities purposeful for their organization and aligned to cost structures.

8.9. A More Customized Solution and Greater Responsibility Over the System will Increase the ROI

The greater the level of customization, the greater the ROI; the most successful implementations tend to be those where the operator takes complete or near-complete responsibility of the implementation and configuration of purchased-system. This enables greater alignment of product with the operator's specific business processes and objectives, giving them greater control and improving productivity.

8.10. Smaller MNOs Can Reduce Costs with Outsourcing Options

Given the initial high costs involved, smaller operators should begin by outsourcing a large proportion of the solution to a third-party vendor with the competencies to implement a system immediately.

9. Glossary

NGRA	Next Generation Revenue Assurance
RA	Revenue Assurance
FMS	Fraud Management System
ETL	Extract Transform and Load
MNO	Mobile Network Operator
ROI	Return on Investment
CSP	Cellular Service Provider
KPI	Key Performance Indicator

References

Retrieved from http://www.juniperresearch.com/shop/products/report/pdf/contents/9009MRA12_TOCs.pdf

Mobile Revenue Assurance & Fraud Management: Business Strategies & Forecasts 2012-2016

Retrieved from http://www.techmahindra.com/Documents/WhitePaper/2012/white_paper_revenue_assurance.pdf

Retrieved from http://www.rhcvisualwriting.com/pdfs/telrevass.pdf

Author's Profile

Mr. Sunny Gajbhiye is a consultant at Ericsson. He is an MBA from Symbiosis Institute of Telecom Management and an Engineer in Electronics & Telecommunication from Mumbai University. Sunny has over 4 years of Telecom Industry experience. He has worked with Tech Mahindra prior to his MBA and has gained rich experience in end to end Telecom Billing. Currently in Ericsson, he is engaged in consulting projects of Business Intelligence, Revenue Assurance and Next Generation Networks.