Importance of Migration Assurance for Telecom Operators

A telecom operator’s goals from transformation projects may be multiple, like reduced cost of operations, increased functionality, gaining competitive advantage etc., but it is necessary to understand that many of these goals/objectives may eventually be defeated without the overlay of an effective Revenue Assurance and Fraud Management system during the transformation phase.
Introduction
Increase in revenues is largely driven by consistent service innovation and effective management of subscriber growth in saturated and emerging markets respectively. In most cases, competition is often intense and telecom operators inevitably need to concurrently manage fast paced growth as well as innovation.

Operators’ ARPU is no longer solely dependent on traditional circuit switched voice and data. A considerable percentage of ARPU gets derived from a diverse set of packet data services. Pressurized by severe competition, increasing hardware capabilities of devices and greater demands by consumers, operators have to keep innovating to offer newer services in order to stay atop competition. With such augmentation in the services offered, migrating to next-generation operations and billing systems is inevitable.

Another major driver for operators to switch from legacy systems is to enable evolution towards a Lean IT paradigm. The undisputable mantra to succeed in today’s market conditions is to enhance efficiency which in turn will boost the organizational agility. This enables operators to rapidly respond to changes and helps bring products/services faster and more competitive to the market.

While the above mentioned factors are keeping telecom operators in the positive quadrant, they should be prepared for the challenges inherent to the transition phase itself and its impact on their revenue chain.

Impact of Transformation Projects – A Business Optimisation Perspective
Lot has been discussed in the telecommunications industry about the need and advantages of migrating to newer OSS/BSS since more and more operators are switching from legacy systems. However, it is essential to understand the impacts of such a transformation to ensure proper controls are deployed to tackle these challenges effectively.

One of the areas of prime concern is the integration of various systems involved. Operators deploy a number of systems in their OSS/BSS environment which do not necessarily communicate to each other. This leads to fragmentation of processes/data across multiple systems, which in turn breeds inefficiencies. Adding to this are the problems of multiple data formats and constant updates to vendors’ systems which together cause considerable inconsistencies in data and hence induce scope for revenue leakages.

The functionality and data being migrated from legacy systems is dynamic (Tariffs are revised; new tariffs are still being launched, new customers, churn, etc.). Therefore it needs continuous monitoring. Additionally, the target solution needs to know about any new capability to be supported.

It is a known fact that transformation projects are not simple and easy to perform. Independent ‘end to end’ verification of data collection, processing and migration can identify problems that may have been missed by the migration team and end up in the new production system leading to outages, a poor experience for customers and expensive fixes.
A recent survey by KPMG indicates that 49% of the telecom operators undergoing transformation projects saw a significant increase in revenue leakage and threat of fraud while another 45% indicated a partial increase in revenue leakage and threat of fraud. Put together, 94% of operators have encountered some kind of increase in revenue leakages during the transformation phase from legacy to next generation OSS/BSS. The same survey also indicates that new transformational projects had the highest impact on making the business vulnerable to leakages and frauds.

### Aspects of the business most vulnerable to revenue leakage/fraud

Respondents were asked to rank the vulnerability of each business aspect, on a scale of 1–10, with 10 being the highest.

- **New transformational projects**: 6.5
- **Poor system integration from MSC-IN-Mediation-Billing systems**: 6.4
- **Frauds (internal or external)**: 6.3
- **Interconnect and roaming billing**: 6.2
- **New product development and tariff configuration**: 6.0
- **CDR generation issues at MSCs/incorrect usage data**: 5.6
- **Intelligent network charging failures**: 5.6
- **VAS partner payments**: 5.3
- **Retail billing systems errors**: 5.3
- **Complex tier-based pricing**: 5.2
- **Sales commissions**: 5.1

The major impacts of transformation projects are seen through data inconsistencies and operational inefficiencies, both leading to secondary issues which in turn increase the potential for leakage.
Importance of Migration Assurance for Telecom Operators

Causes of Vulnerability during Transformation Projects

Data inconsistency across different systems
Migration of data from legacy systems to next generation systems without ensuring integrity, accuracy and completeness leads to data inconsistency. One of the main reasons for this inconsistency is the intrinsic difference in reference, meta-data and configuration data storage in the legacy system viz. a viz. the next generation platform. What makes this more complicated is the use of multiple data formats in different systems. Unless measures are taken to consolidate all their IT into one fully-integrated platform, operators always run huge risk of leakages.

Lack of rigid policies and procedures in the organization
Implementation of next generation systems requires revamped security mechanisms and policies to operate in a secure manner. An existing set of such policies and guidelines would have many shortcomings due to the fact that they were built considering the older systems that were in place. What this indicates is the possibility of vulnerabilities in the system until a time when the policies and guidelines are thoroughly updated. Telecom operators that engage in establishment of enterprise-wide Revenue Assurance policy framework and building an associated operational capability are often shielded from such vulnerabilities in the migration phase.

Reduced focus on detecting and plugging leakages
Transformation projects require substantial CAPEX and a considerable investment of time, effort and energy from senior management to be successful. Often, this implies that there is intense focus and attention on such project pushing other activities to the backseat. Subsequently, Revenue Assurance activities are neglected, and are not given the attention required. In the absence of a proactive and effective Revenue Assurance system, operators are prone to leakages during transformation projects.

From a fraudster’s perspective, barriers in an operator’s environment are lowered during migration and offer them a favorable test-bed to carry out fraudulent activities.

Lack of controls
In case of migration scenarios, it is common to see a system UAT which doesn’t take into consideration scenarios which might be better diagnosed and analyzed over a longer period of time. While there are parallel runs which are considered for certain critical systems (e.g. Retail Billing), we can find that such considerations would take a back-seat for less critical systems given the key drivers of rapid transformation and time to market for new solutions. It would be beneficial for the operator to implement a comprehensive continuous monitoring paradigm which takes into consideration alignment of existing controls to the new platform; while also simultaneously redefining the control framework to cater to the technical evolution of the next generation platform (e.g. an active mediation device as opposed to the legacy mediation system). This will enable a seamless cut-over of existing risk metrics which also incorporates new controls on an on-going basis in a manner which can be thought of as “virtual parallel runs”.

Internal Frauds
Apart from the leakages prevalent in the transition phase, operators are also subjected to exploitation of temporary glitches in the monitoring quality. For example, a retail advisor becomes aware that a limited product range has had its pre-pay flags removed as a result of a faulty migration. The advisor also knows there is a small amount of time required to fix the issue. This exposes a window of opportunity for free calls on prepaid mobiles for a defined period of time, without need for recharge. This in turn gives the advisor an opportunity to exploit this glitch in the system for personal gain.
Importance of Migration Assurance for Telecom Operators

Further, with the introduction of new services and their relatively under-matured operations, operators are often caught off guard by the fraudsters within. Configuration errors, process gaps and system integration issues are some of the factors that give rise to such fraudsters.

Ensuring a Safe Migration

When new OSS/BSS systems are being replaced and data & functionality is being migrated to new systems it is essential that regular automated repeatable comparisons between the old and new systems can be made to ensure the roadmap to the new system does not get out of step. A telecom operator’s goals from transformation projects may be multiple, like reduced cost of operations, increased functionality, gaining competitive advantage etc. but it is necessary to understand that many of these goals/objectives may eventually be defeated without the overlay of an effective Revenue Assurance system during the transformation phase.

The need of the hour is a system for Revenue Assurance and Fraud Management that is proactive in nature and requires minimal focus which facilitates senior management with the luxury of channelizing their attention to other strategic aspects in the organization.

In general, a system that is functionally proficient in the following aspects is the doctor’s prescription to secure revenues and prevent frauds through and after an OSS/BSS transformation:

- Flexible and Agile ETL Capability
- Comprehensive Record Integrity
- Comprehensive File Integrity
- Service Usage Check
- Re-rating capability (specifically relevant during billing transformation projects)
- Quantification of leakages
- Data cross-referencing
- Business Rule Validation
- Systemic Flexibility

Visit www.subex.com or email us at info@subex.com to understand more about ROC® Revenue Assurance and ROC Fraud Management and how it can help you in maximizing the benefits out of your transformation projects.
About Subex

Subex Limited is a leading global provider of Business Support Systems (BSS) that empowers communications service providers (CSPs) to achieve competitive advantage through Business Optimisation - thereby enabling them to improve their operational efficiency to deliver enhanced service experiences to subscribers.

The company pioneered the concept of a Revenue Operations Centre (ROC®) – a centralized approach that sustains profitable growth and financial health through coordinated operational control. Subex’s product portfolio powers the ROC and its best-in-class solutions such as revenue assurance, fraud management, asset assurance, capacity management, data integrity management, credit risk management, cost management, route optimization and partner settlement.

Subex also offers a scalable Managed Services program and has been the market leader in Revenue Assurance and Fraud Management for 2 years in a row according to Gartner (2010 & 2011). Subex has also been enjoying market leadership in Business Optimisation for five consecutive years according to Analysys Mason (2007, 2008, 2009, 2010 & 2011). Business Optimisation includes fraud, revenue assurance, analytics, cost management and credit risk management. Subex has been awarded the Global Telecoms Business Innovation Award for 2012 along with Idea Cellular and 2011 along with Swisscom for fraud management. Subex has also been awarded the Global Market Share Leader in Financial Assurance 2012 by Frost & Sullivan.

Subex’s customers include 29 of top 50 operators* and 33 of the world’s 50 biggest† telecommunications service providers worldwide. The company has more than 300 installations across 70 countries.

*Total Telecom Top 500 Telecom Brands, 2013
†Forbes’ Global 2000 list, 2013