REVENUE ASSURANCE:

What's the big deal!?

Isheanesu Sithole

CISA, CISSP, CISM, CRISC, BSc

SBS Consultants

Harare, Zimbabwe

www.sbsconsultants.co.zw

sbs consultants
simplifying business

YOUNG CEOs

INTRODUCTION

Grandma: "I was waiting for your call all day!!"
Grandson: "Ah, but I sent you a whatsapp in the morning!!!"

Profitability is under immense pressure, for telecommunications companies (telecoms) as legacy revenue streams from voice and SMS are stagnating. The demand for data services is continuously growing. However, these have much lower profit margins. Furthermore, in recent years, there has been increased competition from non-telecoms industry participants and Over the Top (OTT) service providers, for example, Whatsapp, Viber, Skype and many others, thus, pushing revenues even further down.

Globally, telecoms lose billions of dollars annually through revenue leakage caused by inadequate internal control processes, systems and fraud. As if that's not bad enough, recently there has been increasing competition in the telecoms industry in both growing and mature markets. This has led to falling (if not plummeting) profit margins on both voice and data services.

One of the greatest challenges many telecoms grapple with is ensuring they are billing for and collecting all the revenue due to them. In light of all this, any slight endeavour to help increase revenue or avoid revenue leakage and enable more efficient delivery of service is more welcome today than ever before.

REVENUE LEAKAGES

"Where's all that water coming from?"

Most scholars equate revenue leakages to leaking water from a pipe, where water stands in place of revenues or cash flows, and the leaks represent waste. The success of revenue assurance is measured by the size of the leaks "plugged", i.e. the amount of losses reduced. Another way to measure the value of revenue assurance is determined by the value of revenue losses prevented, before they occur. Telecom operators continue to lose billions of dollars every year due to revenue leakage and fraud.

Fraud

Fraud is one of the most prevalent causes of revenue loss for telecoms. Due to the growing problem of fraud in telecoms, globally, companies need to be particularly vigilant since these are present in all network types. In most cases, the driving force is to gain access to services without paying the relevant cost or to obtain money from offering the company's services by staff and third parties (e.g. call selling /subscription fraud) or by providing services to other people using infrastructures with fake identification (identity theft).

Other scams may involve cloned mobile SIM cards where an existing customer's hardware is replicated and used to make calls on their account without them knowing until they get their monthly bill.

Tracking fraud is vital for the survival of telecoms companies as various vulnerabilities exist in their value chain, both internally and externally. Usually these fraudulent activities center on individuals or organisations seeking to dodge payment in one way or the other. Internally, fraud results from employees manipulating system flaws and loopholes in their organisations' processes and procedures. Externally, fraud may result from third parties and dealers manipulating the network elements and operator processes to obtain higher commissions.

Leakage Areas

"Hey, Jack!! I've spotted where the water is leaking from

Telecoms in emerging markets, such as Africa and South America, where new products and services are being introduced rapidly, are more vulnerable to higher leakages. They tend to be more tolerant to higher leakages, with assurance processes being sacrificed for time to market, as more and more value-added services are introduced to the market. However, in developed markets, more attention is put on revenue augmentation as there is slow growth due to market saturation.

Revenue leakages emanate, mainly from configuration changes in any of the network elements, new product development, configuration of tariffs, and improper system integration on the Call Data Records (CDRs) processing cycle (*MSC-IN-mediation-billing Systems*). Losses usually result from unbilled customers (which usually occurs when subscribers are not recognised by the system), incorrectly billed customer (customers charged the wrong amounts), and stranded network elements (where equipment is misconstrued as unavailable or not operational, resulting in CDRs being lost/ corrupted. Described below are the typical sources of revenue leakage for telecoms companies.

Inadequate Operational Processes and Procedures

Poor operational processes and procedures are the major sources of revenue leakages. The absence of monitoring of processes and tasks by employees may lead to errors or deliberate actions that result in revenue loss. Human errors in the service activation process where the order details are first entered into the billings system may cause a leakage before a single call is made by the customer. Human errors can also impact the invoicing system when wrong data is entered into the rating engine, for instance, a charge of 18 cents per minute is entered as 8 cents per minute or a promotion of 10cents discount per minute, that is supposed to end on the 5th of July is entered with the wrong termination date of 25 July. Such errors would affect many subscribers and result in the telecoms company losing large amounts of unbilled revenue.

Network Elements

Problems in network elements are another key cause of revenue leakages. Signal challenges during a call, may lead to customers being under-billed as a result of genuine traffic not reaching the relevant mediation, rating and/ or billing systems. There are instances where CDRs do not reach the appropriate destination due to mal-functioning of network equipment and network elements. Leakages will also result when CDRs in Switch are not sent to Mediation system, or CDRs in Mediation are not sent downstream; as well as, when authentic CDRs are rejected by the rating or billing system. Considering that a typical telecoms company handles millions of CDRs a day, leakage can occur anywhere along the network as the CDR is transported from the switch to the mediation system, to the billing system, whereby the CDR is misrouted, corrupted or misidentified.

Network configuration issues can produce incomplete usage information or cause unexpected call routing, resulting in higher costs or lower quality. Other aspects of the network that telecoms grapple with, regarding revenue losses include; wrong duration on the CDRs, incorrect business rules being applied on services, errors in service provisioning to subscribers, as well as incorrect routing of traffic.

Rating & Billing Complexities

Not only must a telecoms company be able to track usage, but they must also juggle complex billing rules around individual prices. The speed at which new technology is being introduced, as well as, the haste of marketing efforts in churning out new products and services, does not afford time for process improvement and keeping up with promotions and changing prices. Historically, telecoms would offer one or two new services per year; but these days, various promotions and services are launched each month. These dynamic efforts introduce numerous vulnerabilities and complexities which result in revenue leakages. For instance, when a company bundles different services together, there is a sophisticated pricing schemes such as a discounts sliding scale based on how many services are subscribed to. Bundling is complicated by the multiple billing systems and provides more opportunities for losses if the company's systems cannot properly bill for services rendered.

Revenue leakages may also result from the use of incorrect rejection logic in the rating/ billing systems. The level of rating/ billing accuracy, or the lack thereof, determines the level of revenue losses.

Other issues, under rating and billing complexities include; incorrect tariff plans being applied on services, late rating / billing of service; incorrect configurations (for example, rating minutes instead of seconds); as well as incorrect disconnection of service, where a service is disconnected when billing had already stopped.

Partner Management

Telecoms companies work with numerous partners and third parties, which include, other telecoms, recharge card vendors, content providers, etc. Interconnection arrangements are the most dominant partner challenges. This includes roaming agreements and third party content provider contracts.

Telecoms users cannot communicate with each other or connect with services they demand unless necessary interconnection arrangements are in place. Interconnection of a multitude of different types of networks has brought tremendous benefits to consumers and businesses around the world in the last decade. Without efficient interconnection arrangements, services such as direct international dialling, all Internet-delivered services, ATMs and e-commerce would not be possible. However, it has also brought some challenges with it.

There is no standardised level and structure of interconnection charges and hence no basis for calculation. As a result, smaller telecoms are prejudiced by larger ones. For example, they may charge excessive rates for interconnection, refuse to build or make available adequate interconnection capacity, and refuse to unbundle network elements or services necessary for efficient interconnection.

Roaming charges and 'value added services' are also vulnerable to leakage as they require records to be exchanged with different providers - be they international operators or content owners - and require more complex technical and business processes. Tests, incongruence, inefficient processes, settlement inconsistencies, late payments, incorrect invoices and customer complaints also account for revenue lost in roaming services. Roaming revenue is very difficult to manage due to constant changes of contracts between countries, the high volume of data traffic and the complexity of information transfer. However, the roaming business processes must be accurate and up-to-date in order to protect roaming margins, which are already lowered by intense competition.

With regards to third party content providers, who provide services such as ringtones and music downloads, telecoms can lose revenues when they cannot collect revenue from the customer but still have to pay content providers for their services. The risk of leakage is increased exponentially with proliferation of content offerings, the number of suppliers and rapidly changing products. Reconciliation of data is important because as data volumes increase, the risk of inaccuracy increases as well

Systems Integration Challenges

Flexibility is a key requirement in telecoms systems and equipment to accommodate the fast-paced changes occurring with technology and in the industry. Many different types of equipment, systems and technologies from different vendors are used by telecoms and these have to be seamlessly integrated to ensure optimum performance. However, integration of the different back office systems is often done poorly because management do not have the resources to undertake such a project and also because these technologies were not made to work with each other in the first place. The gaps between the systems are usually handled manually and as a result, the risk of inconsistencies, errors and leakage is particularly high.

More often than not, different systems have different data structures, and hence, extra effort and investment has to be made to ensure a seamless integration of these. System upgrades and also changes to the existing network systems may also contribute to integration challenges and consequently, risk of leakage. Many errors also occur at the point of interconnection between two operators, since the interfacing systems are originally not meant to exchange data and services. This can also cause the problem of phantom traffic whereby revenue can be lost due to the inability to identify the originating carrier and therefore interconnection fees cannot be billed.

...And Many More

Other areas of revenue losses and/ or leakages are:

- **Finance and Accounting** – Revenue reported in the financial statements may not accurately reflect usage, or billed amounts. Excessive outstanding debt and disputes with customers, vendors, partners or distributors may also contribute to leakages.
- **Customer Management -** Unauthorized special customer billing and/or inaccurate rating and discounting, as well as unauthorised or unverified customer credits may result in leakages.
- **Order Entry and Provisioning –** Inaccurate order entry and provisioning may result in leakages, where a client is provisioned with a more expensive product than the one they are actually being billed for.
- **Network and Usage Management** – If capacity is not properly managed, leakage may occur as a result of investment in redundant network equipment.
- **Product and Offer Management** – Investing in unprofitable products and sale of incorrect plans and/or promotions could also lead to leakages.

REVENUE ASSURANCE

"I assure you sir; we have received all our dues."

Revenue assurance can be defined as; a means to identify and remedy, and perhaps also to prevent, problems that result in financial underperformance without seeking to generate additional sales. The value added also includes the recovery of "lost" revenues or costs (through issuing additional bills, chasing uncollected payments, renegotiating with suppliers a refund of costs etc.) after the fact. The most debated part of revenue assurance is where to start checking, i.e. at the network side, the rating side, the billing side, the interconnect side, the CRM side, etc. However, most surveys and reports state that the maximum leakage happens during the flow of Call Detail Records (CDRs) or Event Detail Records (EDRs) from the Switch to the respective rating / billing engines.

Research shows that, globally, more than 50% of identified leakages are not recovered. It is important to have a cross-function mandate to recover revenue wherever possible. These require strong executive sponsorship. Telecoms companies need to strike a balance between control execution and new opportunities identification.

As new services develop, identifying new areas of opportunity will be increasingly important to overall profitability. New service assurance is less dependent on traditional switch-to-bill activities. Revenue Assurance needs to expand its scope up and down the revenue cycle to ensure that it can meet the challenge of assuring these services.

Revenue Assurance Process Categories

The Revenue Assurance processes in many ways can be regarded as an auditing process. The objective is to ensure that policies of the organization are well implemented and that no or minimal revenue leakage is occurring. These can be categorized into Detective, Corrective and Preventive controls or processes.

Detective Processes

Revenue Assurance Detection is the process of spotting a change in value of a dimension relative to its movement from System A to System B or within a given system itself. Detection in RA can be achieved by both manual and automated means and the typical activities include monitoring, summarization, investigation and auditing.

Monitoring:- Typically, monitoring activities in Revenue Assurance refer to observing data, system or a process for any changes which may occur over a period of time. With the use of automated tools one can typically achieve constant monitoring which can notify the user or administrator (via email, SMS or other alarms) in case of any changes. The various processes which typically are monitored by a Revenue Assurance department include daily network usage, profile and configuration changes, mediation, rating, billing, settlement, roaming, collections and related processes.

Summarising:- When dealing with large volumes of information like network usage, it may not be practical to go through CDR by CDR and compare the same between 2 systems. In such cases summarisation will help in quickly examining and finding out the preliminary problem areas. Such rapid assessments help in identifying the problem areas or dimensions quickly and a further detailed investigation can be carried out for those dimensions identified. Summarization greatly reduces the manual effort in identifying problem areas within a large data stream.

Auditing:- A revenue assurance audit is a set of activities carried out to ensure that the organization is taking necessary steps to remain compliant to the evolving changes of organizational policies, regulations and market conditions. Every Revenue Assurance audit has a list of specific objectives which may come from management, regulations or industry standards. The actual tasks of the audit can differ based on the information, system or departmental processes being audited.

Investigation:- Investigation is the act of detecting something new, or something "old" that had been unknown. Investigation leads to discovery which is the observation of new actions, or new events and providing new reasoning to explain the knowledge gathered. A Revenue Assurance investigation is a series of processes or procedures carried out to identify the Root Cause of an anomaly. This is also known as Root Causes Analysis (RCA) procedures or activities. RCA is a method of problem solving that tries to identify the root causes of faults or problems that cause operating events. An investigation would try to identify and correct the root causes of events, as opposed to simply addressing their symptoms. By focusing on correction of root causes, revenue assurance problem recurrence can be prevented.

Corrective Processes

Correction is the set of activities and processes related around getting the process structures correct in order to minimize the changes identified as per the detection techniques. Correction itself is the act or method of correcting a discrepancy. Typically some information, configuration, amount or quantity needs to be added, edited or removed from a system, process or procedure in order to correct the anomaly.

In Revenue Assurance activities, the process of correction of a root cause could involve correction of information, processes, technology or people.

Information Correction:- This refers to the process of correcting or updating a value for a configuration element or a reference table. This is typically the result of a missing data set in a particular given table or system file.

Process Correction:- Process correction refers to the modification of an activity by adding, modifying or removing an activity step which will prevent a miss-configuration or revenue leakage in the process. Typically process correction is required to have a pro-active revenue assurance step to provide better governance across the operations.

People Correction:- People correction is required when skills of the resources are in question. Revenue Assurance is a niche business process with limited people present with the right amount of Telecom, Network, Mediation, Billing, IT and Business related experience. This leads to many Revenue Assurance teams with inexperienced people on operational departments. Owing to this, most Revenue Assurance operations end up being only re-active rather than moving into a proactive foundation.

Technology Correction: - The very nature of the telecom business changes frequently. There are 2 aspects to Technology correction:
i) The technology on the Network side, and
ii) Technologies in use by the Revenue Assurance department themselves.

Preventive Processes

Prevention is the process of performing an activity in order to avoid a high risk situation. For example if there is risk that a tariff plan is not correctly implemented, then the preventive action could be to simulate calls on test SIMs on the new tariff plans prior to launch and confirm the tariffs coming in the test CDRs against the marketing or advertising department rates. Preventive activities lead to effective risk management around Revenue Assurance.

Synchronization:- A set of activities which ensure that 2 data sets are synchronized over a period of time. For example a set of Revenue Assurance activities would ensure that all prepaid customers on the CRM systems are represented in the IN - SDP (Intelligent Network) and vice versa.

Integrity Checks:- These are individual activities carried out to ensure the integrity of the system or process. This is an effective check in gaining insight into an individual process and to assess whether it has anything in their immediate background that may be a cause for concern.

Pre Process Checks:- Any checks performed on the input parameters of a process to ensure that the right data is fed into the process. Pre Process checks are necessary for complex processes like rating and billing which involve multiple sub processes and consume a lot of time for each run.

WAY FOWARD

"Now I see the light"

The first step to address all the identified issues and applying the above recommendations, is performing a detailed process assessment of areas of the company in which revenue leakage can occur from customer registration, through service provisioning and billing, as well as their revenue assurance function and capabilities. Management should benchmark the company's existing revenue assurance maturity level against leading industry practices, as well as identify and prioritize the main sources of revenue leakage. At this stage, the business should design the revenue assurance through development and definition of new business processes, roles and responsibilities. A revenue assurance function strategy that promotes the function throughout the whole enterprise should be created to help facilitate the function's integration with other key areas of the company, such as fraud and credit management.

The second stage is the development of targets by the business, that is, in what areas it wants to improve revenue assurance and by what degree—and subsequently define new key performance indicators (KPIs) that will help the company to measure its progress toward reaching those targets.

Development of new revenue assurance business processes or improvement of existing ones should be carried out to enable the organisation to more effectively identify and address sources of revenue leakage. At this stage, the company may take short-term initiatives to resolve the high-priority issues rapidly and begin generating cost savings immediately and gain management commitment to further revenue assurance improvement.

The final stage would be the full implementation of the developed and/ or improved processes. Technology solutions are rolled-out to augment the processes. The company should continuously fine-tune, and refine the solution to enhance the revenue assurance business processes and solutions for optimal performance, and also to enable the support of ongoing review, detection and repair of future issues that could lead to revenue leakage and bottom-line degradation.

CONCLUSION

The core elements of a good revenue assurance strategy include performing a risk assessment in order to prioritize high risk areas, integrating revenue maximization techniques and implementing key automated tools, creating a revenue responsible organization, embedding quantifiable monitoring mechanisms and having committed champions. The strategy should emphasize having a holistic, end-to-end approach, meaning that a review of the full revenue cycle is done to capture more leakage events than when doing separate and disjointed assessments. An organization-wide charter for revenue management is required rather than treating it as the sole responsibility of that single group. The long term effectiveness of revenue assurance strategies will depend on the enterprise's mindset as cultivated by the champions.

About the author

Isheanesu Sithole is a Technology Risk & Information security professional with over 4 years' experience in providing Technology Risk Management, External & Internal Audit, Information Security and Revenue Assurance services to organisations. He has performed risk based audits and third party reporting in compliance to international regulations and standards (e.g. SAS 70, SOX 404, SOC, Basel II, Solvency II, ITAF). Isheanesu has worked with organisations from Zimbabwe, Ghana, South Africa and Zambia and assisted large organisations such as, Econet, Telecel, Airtel (Zambia), Tel-One, FBC, Old Mutual (SA), Mimosa, Zimplats, TRB Bank (Ghana), GCNet (Ghana) and the Government of Ghana, among others. He holds the; Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC) certifications; as well as a BSc Honours Degree in Information Systems.

About SBS Consultants

SBS Consultants is a professional services firm specialising in IT Audit & Risk, Information & Cyber Security and IT Advisory services. It was founded by a group of IS Audit & Information Security professionals with a proven track record of working in the big four professional services. They provide independent and impartial advice to clients. SBS provides Revenue Assurance services (among others) to a number of telecommunications, utilities and financial companies in Zimbabwe and Southern Africa.

About Young CEOs

The Young CEOs is a youth driven non-profit organisation founded in 2009. Its main thrust is to equip young people with skills necessary for entrepreneurship, sustainable development, wealth creation, business leadership and responsible living. Young CEOs offers an opportunity for young people to discover and explore the vast business avenues as well as creating a platform for them to network, mingle, and be inspired and mentored by local business people, corporate executives, industry experts and specialists in Zimbabwe.

Disclaimer

This research paper is published by SBS Consultants in collaboration with Young CEOs international. All content is for guidance purposes only and is not to be construed as a guaranteed outcome. It is not intended to be a substitute for detailed research or the exercise of professional judgment. SBS Consultants and Young CEOs international will not accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor. The views of the author and third parties set out in this publication are not necessarily the views of SBS Consultants.

SBS – 15R86-07-01

sbs consultants

simplifying business

IT AUDIT & RISK | INFORMATION SECURITY | CONSULTING | TRAINING

www.sbsconsultants.co.zw

business@sbsconsultants.co.zw.

+2634 882 364 / +263 735 688 209