Data accuracy and integrity are the tenets of operational excellence for telecommunications and network service providers. The quality, accuracy, consistency and relevancy of data about the actual “as is” state of the network and services is essential for operations processes such as error-free provisioning, service design and activation, customer care, and capacity and network planning.
Introduction

Data accuracy and integrity are the tenets of operational excellence for telecommunications and network service providers. The quality, accuracy, consistency and relevancy of data about the actual “as is” state of the network and services is essential for operations processes such as error-free provisioning, service design and activation, customer care, and capacity and network planning.

Poor data integrity has an increasing negative impact in today’s telecommunications environment. As companies either move toward real-time (or near real-time) provisioning of services, data integrity problems in the inventory are huge roadblocks for effective service delivery. At the same time, as companies focus on cost containment and belt tightening, improving data integrity between inventory systems and the network presents a gold mine to those wanting to identify stranded assets in the network. This problem is related to the prolific amount of and variety of complex, legacy and often “siloeed” systems that support network-facing and customer-facing operations.

These data problems are due to system integration and process problems. Methods and procedures (M&Ps) in place at many carriers exacerbate data integrity problems. Compounding this problem is the fact that these processes can’t change overnight and often rely on human interaction. Therefore, the various business processes of Operations Support Systems (OSS) and Business Support Systems (BSS) increasingly create data integrity problems where inventory systems fall out of synch with the actual network and services. This leads to inefficient operations, increased costs and revenue loss. Just as important is the need for a system to continually monitor the data integrity and make corrections.

In today’s demanding environment, with complex next-generation networks, value-conscious customers and the need to do “more with less” faster and better than the competition, a comprehensive data integrity management solution is a business imperative for all carriers – large and small. This white paper highlights the impact of poor network and service data integrity on operations and describes how current processes and systems are insufficient to address the problem. The paper also outlines best practices for data integrity management including the concept of a data stewardship team and describes how a comprehensive data integrity management system, such as ROC® Data Integrity Management from Subex, enables and supports these processes to achieve superior operational results.

OSS Data Integrity Problem

The OSS data integrity problem is a longstanding, chronic issue in tele-communications operations environments. The inventory system or database of record (DBoR) at a typical service provider is often 40% out of synch with the actual physical and logical state of the network. Furthermore, in a typical service provider environment, data integrity only becomes worse over time because of the limitations of manual, time-consuming steps for updating and maintaining OSS data. For example:

- Field staffers responding to an outage fail to update the OSS with changes
- Provisioners trying to get customers up quickly grab the first free ports they can find
- Service delivery teams, under pressure to shorten cycle times, take shortcuts and develops workarounds which never get reconciled back into provisioning systems
- Network planners take a best guess as to what is actually in the network
Poor data integrity impacts critical service fulfillment, assurance and billing processes, driving up operational expenditures, increasing revenue leakage and leading to unnecessary capital expenditures. This impact on operations is significant and across the board. For example:

**Provisioning Delays and Fall-out**
Inaccurate and incomplete data about the state of the network requires the provisioning staff to conduct time consuming resource verification and reconciliation with the DBoR before services can be designed, provisioned and activated. Telecom analysts estimate that automated provisioning can result in a 15-30 day reduction in typical service provisioning time. However, these efficiency gains and operational improvements cannot be realized without a reliable source of high quality, accurate data, a representation of the “as is” network.

**Network and Capacity Planning and Design**
Capacity planning, network design and service design are dependent on accurate knowledge of the network and service riding on that network. Planners need to understand the utilization of the network at any given moment. Effective network design and capacity planning requires one know where overutilization threatens quality of service. With changes to today’s complex networks occurring frequently and provisioning problems leading to stranded network resources, capacity planners and network designers are often flying blind. Analysts estimate that the typical service provider has 20-30% stranded assets that are not visible to the planners and other operations personnel. Typically, this leads to untimely and unnecessary deployment of additional capital and equipment.

**Revenue Assurance**
Identifying under-billed or unbilled services is a key to preventing revenue leakage. This activity is difficult and time-consuming without having a real-time source of the actual logical service connections in the network and maintaining the integrity of that data across the enterprise. Analysts estimate that more than 15% of broadband services are not properly accounted for at any given time.

**Trouble Resolution and Service Assurance**
Customer care operations and trouble management tasks are hindered by not having visibility into how the network status directly relates to an individual customer’s services. Superior customer service — a key competitive differentiator for carriers — is impeded by not knowing which specific circuits and service paths are affected by the fault status of given network elements. This makes it more difficult to determine how service restoration should be prioritized to meet service level agreement commitments. When faced with service-affecting outage situations, NOC personnel often expend valuable time validating outage information directly with the network element and inventory systems. This results in reduced productivity and long mean-time-to-repair (MTTR).

The systems and processes used in the typical carrier environment today to address data integrity issues are actually contributing to the data integrity problems. Given that these systems and processes are slow to change, this is an insufficient vehicle to address the scope of the problem. The various OSS/BSS systems and processes that support the carrier operations are sub-optimal due to an inconsistent knowledge of the state of the network. Typically, this knowledge is also incomplete since these systems are designed to access only the specific network/service data required for their
functions. Consequently, the various systems “mistrust” each other’s data and are run as “siloed” systems. Often, functional/operational groups set up their own workflow and processes that are typically paper-based and involve manual hand-offs. These processes are not only error-prone but they also introduce information latency and reduce overall visibility across functions. In addition, they consume expensive, well-trained personnel and become a drag on overall productivity.

Service providers may also undertake manual network data reconciliation projects in an effort to improve data integrity across their systems. These projects aim to determine the “as is” network through manual means and match it up with “as intended” network represented in the inventory system or DBoR. These projects are usually in reactive mode and rely on time-consuming, manual processes to synchronize the data. They are expensive, often infrequent or ad-hoc, and provide a snapshot that is obsolete before the completion of the project.

Manual efforts and one-off discovery scripts do not provide the breadth and depth of network and service element coverage necessary for effective data integrity management because of the expense of a labor-intensive effort. In addition, the same processes and systems that created the data integrity problems in the first place whittle away at the one-time investment. This results in expensive, manually intensive followup efforts a short time later to perform the same task.

Continually upgrading network systems to respond to device firmware version changes and extending these systems to support new gear and device types becomes exponentially complex as the network environment changes ever more rapidly. Even in a small network such manual reconciliation efforts easily become overwhelmed by the sheer volume of discrepancies between the network “as is” and the network “as intended.” Networks also change. Tomorrow’s “as-is” network is today’s “to-be” network. This is because these approaches do not offer automated ways to identify, prioritize and resolve discrepancies. Furthermore, building and maintaining script-based systems requires investment of expensive, hard-to-find personnel with development and network vendor expertise.

Compounding the data integrity problem is the fact no individual or group has ownership of networkbased data quality at a typical carrier. Data reconciliation projects are often run with project teams comprising borrowed resources from groups such as IT, Operations, Network Engineering and others. However, these individuals’ core functions remain in the original groups and the creation and application of standards and processes for data integrity is a part-time commitment, at best. Consequently, maintenance and enhancement of network-based data quality is a losing battle in most carrier environments. In fact, some service providers know of the network and OSS data discrepancies but cannot allocate the staff time to resolve them – personnel do not have data quality in their performance objectives as an incentive.
Figure 1. OSS/BSS operate without a live, continuous feedback loop from the network to keep the “as is” and “as intended” networks in sync.

The data integrity problem in carrier environments today is the result of the de-facto open loop that exists between the network and the OSS/BSS as shown in Figure 1. This feedback loop is essentially open due to the time-consuming, human-based, and therefore expensive, methods and procedures that are implemented for synchronizing the “as is” and “as intended” networks. For effective data integrity management and the consequent operational efficiencies, this loop needs to be closed through a management system capable of providing “as is” data on the network and automating the necessary workflow for discrepancy management and reconciliation. ROC Data Integrity Management, the industry’s first network-driven data integrity system, focuses on addressing this problem and supporting the breadth of critical operations at today’s service providers.

Best Practices for Data Integrity Management

Success in today’s economic environment demands the ability to optimize the use of the network and the productivity of personnel through effective network resource management and business process management. Doing so calls for OSS and BSS that can accurately and precisely track and monitor network resources – all layers and all types. Additionally, it calls for processes to be put in place that can proactively and automatically maintain the integrity of data and enable enterprise-wide visibility into it.
At a high level, the data integrity management system must form an “as is” picture of the network and services and then synchronize the representations in the OSS/BSS with this live picture. Best practices for effective data integrity management through a “closing of the loop” between the network and the OSS/BSS, as illustrated in Figure 2, impose requirements for automated, intelligent discovery of the network, configurable rules-based discrepancy management and customizable workflow-based reconciliation. In addition, data integrity management needs to be an on-going operational function, just as network fault management is today, with a Data Quality team having stewardship of the standards and procedures. Several carriers have adopted this organizational strategy today and are finding distinct competitive advantages can be gained by leveraging improvements in network utilization, lowered operations costs and increased productivity.

**Network Discovery**

A data integrity management system must support the complete OSS/BSS that service providers have in place and therefore needs to build a comprehensive picture of the network. The system must be capable of discovering and assimilating a breadth of data about the devices, topology and service structure of the network that is needed to improve key service fulfillment and assurance functions. For example, the discovery source should provide sufficient data to support processes such as provisioning and activation, fault and performance monitoring, customer trouble management and others. Many different systems offer rudimentary discovery capabilities today, but these systems in general do not offer a sufficiently comprehensive scope of data needed for OSS reconciliation.

The data integrity management system must discover critical details from the network on a wide variety of device types, service configurations and supporting technologies. For effectively enabling network-driven data integrity, the system must provide the following capabilities for discovery:

**Figure 2.** Closing the loop between the network and OSS/BSS with a Data Integrity Management System and a team tasked to support data quality improvements.
**Broad and Deep Functional and Core-to-edge Discovery**

Core-to-edge discovery is the ability to pull comprehensive data from devices from the core to the edge of the network, at the multiple network layers of the OSI stack, and maintain the complex hierarchical relationships between these technologies. Discovery should cover Layers 1, 2 and 3 of the OSI stack, focusing on the transport layer, switching layer and routing layer. The system must be able to model the hierarchical dependencies of the layers because the higher layer services, such as VPNs, TLAN, ATM service and others, depend on the lower layers of the network such as SONET/SDH for service delivery.

Network discovery must also be broad and deep functionally to support the detail needed to drive all OSS functions. From a traditional inventory perspective, this means discovering each network system's shelves, cards, ports and detailed attributes of each physical component such as software version, card and port types, port configurations and others. In addition to physical components, network discovery must include logical configuration details, often called "service elements," from each device. This discovery identifies the internal software connections such as TDM cross-connects or ATM PVCs that are provisioned from port-to-port to enable an end-to-end service for a particular customer. Deep discovery also captures attributes for logical connections, the parent-child relationships between service elements and the service element – physical element dependencies.

The combined details of multi-layer physical components, logical connections and their attributes, and interdependencies provide the required information in managing the data integrity of service records for critical OSS/BSS functions.

**Configurability**

Configuration of the discovery capabilities is a critical component of the system and must be flexible to meet the needs of rapidly changing service provider environments. Separately configurable areas must be available to manage network sweeps, device accessibility and scheduling, bandwidth and CPU throttling, and simultaneous device discovery. These highly granular configuration parameters are required for administrators to dynamically optimize the discovery performance of the system and non-intrusively capture the “as is” network in real time.

**Support for Multiple Mediation Interfaces**

A core requirement for network discovery is a mechanism to remotely communicate (mediate) with devices using any network protocol over any management network. Furthermore, it is critical for the discovery system to support these protocols and methods simultaneously and in combination to capture the comprehensive, multi-layer information needed for effective data integrity management.

**Extensibility and Scalability**

With today’s complex, fast-changing networks, the system must provide capabilities to extend comprehensive discovery to new network element types seamlessly and at low cost and effort. An easy-to-use development environment for these extensions must be provided. This enables rapid implementation and deployment by carrier IT personnel or third-party integrators which in turn lowers the cost of ownership. The system must be built on a modular architecture so that such extensions can be “plugged in” without requiring upgrades to the system framework from the vendor. In addition, as the
networks change and grow, the system must have the capability to scale-up and scale-out as needed to maintain reliability and performance.

Discrepancy Management
The data integrity management system must be capable of using the discovered network data and service definitions to construct end-to-end service views and identify discrepancies with the “as intended” representation in the various OSS and BSS. These service definition rules need to be highly configurable permitting rapid customization and enabling service definitions to be easily updated to fit evolving service models. The discrepancy management process should include the following:

Data Import and Normalization
Discrepancy management requires that the “as intended” network from the inventory system or other OSS be imported and normalized for comparison with the discovered and assembled “as is” network. The system must also allow the administrator to configure and control the scope and schedule of data import as optimal for the carrier’s operations policies.

Granular Matching
The system must support configurable rules to establish whether network and service elements in the “as is” and “as intended” network are equivalent. In addition, the system should attach a level of confidence to this determination to help with prioritization and reconciliation, if needed. Definable rules should be supported to establish consistency of secondary attributes also and enable the staff to build a complete picture of the object as it actually exists in the network.

Prioritization
If the OSS is significantly out of synch with the “as is” network, the identified discrepancies could number in thousands, if not millions, and would overwhelm any manual data integrity management process. Therefore, the system must provide capabilities to expedite discrepancy resolution by classifying and prioritizing discrepancies based on rules and enabling drill-down investigation. These rules to determine the severity and priority of discrepancies must be configurable to conform to the carrier’s data integrity policies and the processes of assigned users.

Discrepancy Analysis
Even without the issue of sheer volume, analyzing the prioritized set of discrepancies and aggregating them, recognizing dependencies and identifying resolutions is an extremely time-consuming and challenging task for the operations staff. When this happens, discrepancies pile up and the job becomes virtually insurmountable. Without the benefit of sophisticated pattern-recognition algorithms and computer-based intelligence, discrepancy management can quickly become unmanageable and consume enormous amounts of expensive staff time and drag down productivity. Therefore, discrepancy management must include intelligent analytics and decision support that enables operators to quickly “see the forest from the trees” and take appropriate action. The system must provide capabilities to identify complex chains of cascading and inter-related discrepancies, pinpoint the most probable root cause and recommend resolution plans based on configurable rules. These automated functions help the data integrity staff be much more productive in managing, investigating and resolving discrepancies. The savings in work and time can improve efficiency by as much as 95% over manual processes.
**Workflow-Based Reconciliation**

The data integrity management system must provide capabilities for customizable workflow to take action on and reconcile the identified discrepancies. Based on the carrier’s methods and procedures for resource and asset management, the actions, approvals, access, etc. to reconcile a discrepancy must be supported in the data integrity management system. This would typically include workflow-based routing, say for approval, combined with manual actions, such as updating an inventory record. Data integrity systems must also support automated reconciliation actions without manual intervention for commonly encountered discrepancies, as determined by the service provider. As service providers become increasingly comfortable with data integrity management, systems should support “flow-through” reconciliation with provisions for exception handling so that operator efficiency can be maximized. The system must also provide open interfaces for integration to support the carrier’s data integrity workflow that may require communication with other systems such as a work order system to initiate a work order for investigating a missing device in the field or an email system to notify appropriate staff of high priority discrepancies. Figure 3 below shows the interactions between these various best practice capabilities in a data integrity management system.

![Diagram](image-url)

**Figure 3.** Automated network discovery, rules-based discrepancy management and workflow-based reconciliation aspects of a data integrity management system.
Data Stewardship

In a carrier environment, data integrity management cannot be a one-time or project-based event but rather should be an on-going operational function. Thankfully, because of the automated tools available today, this can be accomplished by a small, focused team tasked with having ownership of data quality and the processes that enable and support it. Some carriers have incorporated the data integrity function into the IT group that is responsible for implementing and administering the various OSS/BSS databases and is well-versed in the concepts and process of data synchronization. For some network service providers, the operations group has taken on the responsibility for data integrity and, as the consumer of the data, sets the standards for data quality and the processes to support it. Given its criticality for operational excellence, a recommended best practice is to form a cross-functional Data Quality Team that has the focus of maintaining and enhancing carrier-wide data integrity.

The cross-functional Data Quality Team comprising representatives from IT, operations, network engineering, billing, etc. should have a charter similar to the department and enterprise-wide Six Sigma and Quality teams common in manufacturing concerns. The staff on this team would have data integrity management as their core function and would be given data quality objectives and measured against results in accomplishing those objectives. The team would be responsible for evaluating and setting up the tools/systems and processes, establishing quality standards and measuring against them, enforcing the methods and procedures for effective data integrity management, and identifying “process holes” that lead to data integrity issues.

As with any quality initiative, measurement is critical and must be made an integral part of the data stewardship charter. The success of data integrity initiatives require that data quality be measured through high-granularity reports that monitor and track over time measures such as:

- Discrepancy growth – the number and rate at which discrepancies are occurring between the data sources being compared. The team also should track the types of discrepancies and locations of discrepancies being uncovered, which can give insight into the process problems that are the source of data inaccuracies.
- Discrepancy resolution – the number and rate at which discrepancies are being resolved, resolution cycle times and costs. This metric is essential for measuring the effect of the data integrity improvement processes themselves.

The measurements should be classified based on geographic, functional, network and other parameters so that process and organizational changes necessary for improved data integrity can be easily identified. In addition, improvements in data integrity should be measured through the value realized in the various operations by correlating specific discrepancy resolutions to the derived benefits in shorter cycle time, reduced costs, etc. For example, a measurement program might consider the additional revenue being generated by discovering a stranded network element and placing it in service. It also might document the value of the recovered asset, which can have important implications for tax purposes, depreciation and regulatory compliance. A roll-up of these reports gives the aggregated impact of data integrity on operational results and provides the ROI justification for the data integrity effort.

Benefits

The impacts on cost reduction and revenue generation from the application of these best practices for data integrity management cut across all critical operations in a carrier environment. ROC Data Integrity Management supports these best practices.
for data integrity management and has been deployed successfully at Tier 1 service providers to support their full breadth of critical operations. Some examples of the benefits in operational effectiveness and productivity gains that these customers have seen are described below:

**Greater Provisioning Efficiency**

The breadth and depth of ROC Data Integrity Management discovery permits service design to be based on the actual state of the network and services at multiple layers and results in shorter provisioning cycle times and “first-timeright” provisioning. This also forms the foundation for flow-through provisioning and further operational efficiencies associated with it. Additionally, operations staff can immediately verify the successful activation of a new service and understand its impact on the network. Customers using ROC Data Integrity Management have reported a 30% increase in provisioning success.

**Stranded Asset Recovery**

ROC Data Integrity Management locates and identifies undocumented network elements and helps identify unrecorded changes to devices or services. ROC Data Integrity Management also ascertains the availability of cards, ports and service capacity to aid asset management tasks. ROC Data Integrity Management’s ability to discover and assimilate logical service connections helps identify service fragments that are utilizing resources but not generating revenue. The system also helps uncover unbilled or under-billed services reducing revenue leakage. Customers using ROC Data Integrity Management have reported a 25% improvement in network utilization.

**Faster Fault Resolution and Improved Assurance**

Service assurance tasks such as fault and performance management are aided by ROC Data Integrity Management’s ability to associate network resources, services and customers. Operations staff reduces troubleshooting time by pinpointing which services and customers are affected by network outages, aiding service restoration and SLA compliance. In addition, this also enables the carrier to support and charge for differentiated service levels, thereby increasing revenue.

**Rapid Return on Investment (ROI)**

Many customers have found that ROC Data Integrity Management pays for itself in less than six months by recovering stranded network assets and by quickly improving the accuracy of data available for processes such as provisioning. For example, one major North-American carrier recovered more than $1.5 million worth of stranded assets during their initial data cleanse, paying for their ROC Data Integrity Management investment within 6 months. Within 18 months, they had realized more than 200% return on investment from asset recovery alone.

**Summary**

Maximizing the value and usage of network and service resources and the productivity of personnel is essential for network service providers to succeed in the current highly competitive and cost-conscious environment. Data integrity management is an absolute imperative in this environment since it drives operational efficiency and, thereby, financial health. Poor data integrity has been a longstanding problem in carrier environments that leads to inefficiencies and expensive manual re-work across the full range of operations such as provisioning and activation, service assurance, billing and capacity planning. A comprehensive data integrity management system, such as ROC Data Integrity Management, that supports the best practices of automated non-intrusive discovery, rules-based discrepancy management and workflow-based reconciliation, enables the concept of an ‘active’ inventory. In addition, a Data Stewardship team should own data quality as a core function and make proactive data integrity management a part of the standard operating procedure for carriers. The results are asset recovery leading to lower capital expenditures, greater efficiency and success in service provisioning and activation, and faster fault resolution for improved SLA compliance.
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 Optimization - thereby enabling them to improve their operational efficiency to deliver enhanced service experiences to subscribers.

The company pioneered the concept of a Revenue Operations Center (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, credit risk management, cost management, route optimization, data integrity management and interconnect / inter-party settlement.

Subex also offers a scalable Managed Services program and has been the market leader in Business optimization for four consecutive years according to Analysys Mason (2007, 2008, 2009 & 2010). Business optimisation includes fraud, revenue assurance, analytics, cost management and credit risk management. Subex has been awarded the Global Telecoms Business Innovation Award 2011 along with Swisscom for the industry's first successful Risk Reward Sharing model for Fraud Management.

Subex’s customers include 16 of top 20 wireless operators worldwide* and 26 of the world’s 50 biggest* telecommunications service providers. The company has more than 300 installations across 70 countries.

*RCR Wireless list, 2010
#Forbes’ Global 2000 list, 2010