IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Brought to You by Amdocs, Powered by IDC

While risk management and revenue assurance are not new disciplines, formerly rules-based fraud management solutions or exception-based manual revenue assurance processes are no longer fit for service in a business environment where dynamic usage conditions apply. A new breed of business assurance is essential for long-term success.

Business Assurance with Automation and AI Provides Digital Services Sustainability

August 2020

Written by: Karl Whitelock, Research Vice President, Communications Service Provider Operations and Monetization

Introduction

In the age of digital services, network technology evolution, and changing business priorities, assurance comes in many forms. Network assurance is essential for effective network operations. Service assurance is important for managing a positive customer experience. Revenue assurance is critical to financial accountability. Business assurance — the convergence of revenue assurance and risk management — is strategic for managing the impact of traditional services and new digital solutions on top-line revenue and bottom-line profitability.

Managing and maintaining business assurance processes in today's complex services environment require new methods, analytical insight, and enhanced business practices to meet customer needs and to deliver positive business results. The role of business assurance has grown well beyond its founding roots, which were tied to making sure earned revenue would continuously flow without problem from the network source to the communications service provider (SP) balance sheet.

AT A GLANCE

- Understanding risk and mitigating the impacts risk can have on a business when threats strike mean risk mitigation is just as important as technology advances and business model evolution.
- The challenges associated with revenue assurance and fraud management exponentially increase as devices — those providing a digital interface for humans and those delivering a connectivity portal for machines — using a network propagate. When private network interconnection is added to the mix, artificial intelligence/ machine learning (AI/ML)–driven business assurance becomes a mandatory means of business survival.

Why Business Assurance Is So Important

Today, there is much talk about network flexibility and operations agility. However, these are not the only challenges today's business environment faces in meeting customer needs and addressing business and technological changes. Hybrid networks composed of fixed broadband along with 3G/4G and now 5G mobile, customer services involving ubiquitous indoor/outdoor coverage through cellular and Wi-Fi interaction, multiple telco cloud and edge endpoints, and new business models composed of partner ecosystems complicate what was the traditional flow of call detail records (CDRs) from the network to the monetization and data management functions.

As network complexity grows, so do the elements of risk. The challenges associated with identifying risk and mitigating its impacts have traditionally included:

- Identifying the likelihood of customers to become fraudsters or to be bad debtors who systematically request refunds and compensations
- Recognizing anomalies and unknown fraudulent patterns involving postpaid customers, finding the perpetrators of bypass traffic fraud, and identifying anomalous usage/top-up patterns among prepaid customers
- Understanding the extent and number of risky business transactions that may be carried out by external and internal sales channels
- Spotting fraudulent mobile money activities engaged in by customers, dealers, or merchants
- Pinpointing suspicious patterns within loyalty points programs or noting when internal procedures are not followed in granting goodwill credits or in making payment adjustments
- Documenting anomalies in content provider invoice processing or in suspicious billing procedure patterns

As network complexity expands and new operations functions are introduced and then evolve, manual processes and rules-based anomaly detection methods move closer to obsolescence while the need for automated risk resolution expands on multiple fronts.

It is easy to assume that the previously mentioned business assurance challenges stem from day-to-day operations pertaining to customer engagements, partner relationships, and internal process change. But such an assumption falls short of realizing how other factors, especially those of a dynamic nature or that involve new ways of doing business, contribute to the increased need for advanced business assurance practices. As network complexity expands and new operations functions are introduced and then evolve, manual processes and rules-based anomaly detection methods move closer to obsolescence while the need for automated risk resolution expands on multiple fronts.

Automation and Data Analytics Are Essential to an Effective Assurance Strategy

In the ever-changing digital services world, many new risk types are forming in new ways. As with traditional connectivity services, each risk needs to be monitored and managed. Examples include:

- **Systems evolution to the cloud.** The "cloudification" and redefinition of business management and network operations systems introduce a new type of business risk not previously monitored, especially when transitioning workflows from older systems to new cloud-based functions. How will new workflows be tracked and checked for accuracy? Will workflow data be allowed to mingle with other data, and if so, under what conditions? If conditional, how will policy be applied to data access and storage? How will these practices be enforced?

- **Dynamic network configuration.** Even after previously defined business assurance workflows are transitioned, the dynamic nature of new network technology and the personalization options contained within a growing number of services escalate the opportunity for misaligning revenue flows or establishing new types of fraud based on rapidly changing network configurations. How will personalized network performance be tracked against service-level agreement (SLA) guarantees? If dynamically adjusted network parameters are measured and then compared with SLA definitions, how will out-of-compliance measures be addressed (calculated refund) versus in-compliance measures (billable events)? Could in-compliance and out-of-compliance measures be compiled into a less dynamic key performance indicator (KPI) for settlement purposes? Will these measures need to be protected via a distributed ledger for proof of premium-differentiated service delivery?

Rules-based fraud management or exception-based manual revenue assurance are no longer fit for service in a business environment where dynamic usage conditions apply.

- **eSIM management.** In the case of Internet of Things (IoT) solutions, if monitoring service delivery and then finding machine data irregularities with SIM or eSIM provisioning, activation, and data results, how will these violations be reported? How will subscriber usage that is legitimately changed be recognized and regularly monitored for fraudulent usage? How will unauthorized changes be detected, noted, and reported?

- **Partner ecosystems.** Onboarding and then enabling partners to bring digital services or physical goods together to provide enhanced customer value is a higher risk that didn't exist previously. Identifying problems and noting concerns are especially important as partner ecosystems form around select B2C service offerings and B2B2X business solutions. How will services be monitored so that the right types of partner resources are delivered at the right time? How will resource usage be noted against contract commitment, and how can partner settlement streams be tracked against customer usage for accuracy?

- **Network virtualization.** Virtualized network functions (VNFs) and cloud-native containerized network functions (CNFs) are likely the most unknown risks to a communications SP's business today due to limited deployment, technical complexity, and relatively unknown best practices for procuring VNF/CNF licenses from software owners. The creators of VNFs/CNFs are not always the typical network equipment suppliers; this pool of developers will include traditional network equipment suppliers, IT software suppliers, systems integrators, and even a communications SP's internal development teams as the virtualization concept evolves. Because these parties are cloud hosted, the ultimate seller of a VNF/CNF may be acting as an agent for the original software developer.

  In all cases, how will VNF and CNF assignments be noted against contract commitments or usage definitions? When a VNF or CNF license cache nears exhaustion, what process will automatically trigger the purchase of more licenses from VNF/CNF owners on an on-demand basis? What must be monitored to manage awareness of software license validation against possible contracted license expirations? What types of permissions are granted with each license agreement? Are multiple agreements available for the sale of a VNF/CNF? To understand service usage profitability, how will VNF/CNF deployment and revenue settlement be compared, especially when IoT solutions can theoretically consume large quantities of VNF and CNF licenses?

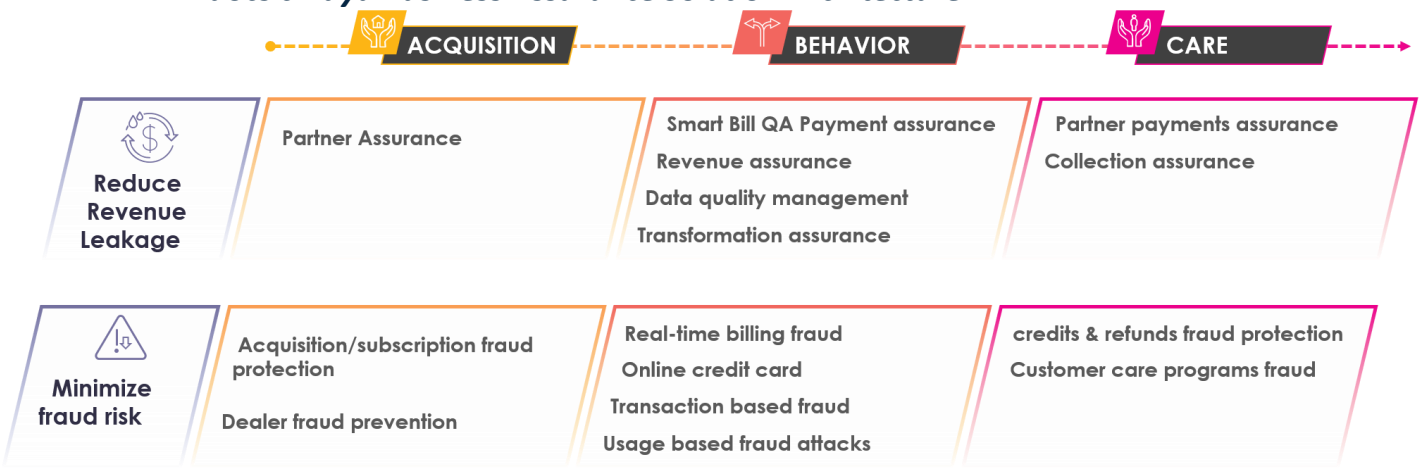
Considering Amdocs cVidya Business Assurance

Amdocs cVidya enables communications SPs to have an AI-powered suite of solutions that are intended to reduce revenue leakage and to minimize the risk of fraud. The Amdocs cVidya business assurance solution, shown in Figure 1, is designed to meet business and operational needs during the acquisition, behavior, and care phases of the business assurance life cycle. More specifically:

- **Acquisition.** Amdocs cVidya is built to reduce revenue leakage during partner acquisition and minimize the risk of acquisition-, subscription-, and dealer-related fraud.
- **Behavior.** Amdocs cVidya is constructed with the goal of reducing revenue leakage through payment, revenue, and transformation assurance. It is also designed to provide data quality management and to minimize the risk of fraud associated with real-time billing, usage, online credit card, and related monetization transactions.
- **Care.** Amdocs cVidya can address revenue assurance needs relating to partner payments and collections and minimize the risk of fraud related to credits or refunds in addition to supporting care programs.

Amdocs cVidya services are designed to ensure proactive, fast, and accurate prediction, prevention, detection, and resolution of revenue leakage, fraud, and cyberfraud. They are also designed to improve operational inefficiencies.

FIGURE 1: *Amdocs cVidya Business Assurance Solution Architecture*



Source: Amdocs, 2020

Industry Challenges

In today's evolving technical and business environments, automated processes and machine learning algorithms will soon be the only means of detecting anomalies and minimizing potential losses to the business from the effects of any known or unknown risk. Business complexity has grown beyond what is manually possible to address. Automated processes become the means of protecting suppliers from the misuse of resources. However, some challenges remain.

Risk Mitigation

In the past, revenue assurance could be managed through a rules-based approach designed to recognize where mostly internal data streams flowed from the network to the account reconciliation functions. Business process and technology evolution have made these risk mitigation processes obsolete. In today's environment where partner-enabled business solutions and edge devices are fast becoming a business reality, new machine-driven approaches to risk mitigation are essential for thwarting unintended consequences from fraud activities or revenue diversion schemes. Active testing of risk mediation strategies is now as important as SLA-based service monitoring.

Systems and Process Transformation

Current market conditions have radically changed from a few months ago due to circumstances beyond anyone's control. Yet, businesses that have already adopted a digital services focus continue to prosper because they previously transformed established systems and processes to meet the dynamic needs of today's business environment. Other organizations are still in a state of transition. Implementing new network technology along with needed changes in existing business processes introduces the potential for revenue disruption and even an inadvertent lack of revenue accountability. Worse still is the potential for fraud in any of its forms from within and outside a communications SP's business environment. Digital operations and monetization solutions capable of responding to market changes when they occur will continue to be a top priority for several months and even years to come.

Organizational Business Focus

Business assurance may sound new, but its functional components — revenue assurance and fraud management — are not. What is new is the combined focus of both disciplines to identify risk and to implement the best ways to mitigate the negative impacts caused by unknowns that may have an adverse impact on an organization's top-line revenue and bottom line profitability. These processes require software tools and services to work together. Existing business processes also must be updated to reflect the current level of thinking and new business model adoption. It will take time to move manually managed services to effective automated functions.

Conclusion

With dynamic conditions as part of the customer experience and now inside the network, the "new normal" becomes an environment where many moving parts, from virtualized network functions to partner ecosystem components, need to come together at the right time and in the right order. This merging will give customers what they want while still enabling the business to make the revenue it needs. When deliberate acts or unintentional actions cause disruption to the various processes delivering value or in creating business outcomes, these situations must be recognized quickly and alleviated. Solutions such as Amdocs cVidya are essential for aligning technology evolution objectives with market needs and end-to-end new business focus.

About the Analyst

Karl Whitelock, *Research Vice President, Communications Service Provider Operations and Monetization*

Karl Whitelock leads IDC's Communications Service Provider Operations and Monetization global practice. He offers strategic insight and global perspectives concerning several operations and monetization functions, formerly known as OSS/BSS, including rating and charging, policy management, partner management, customer experience, revenue assurance and fraud management, service assurance, network data analytics, service orchestration, and network operations.

MESSAGE FROM THE SPONSOR

About Amdocs cVidya

Amdocs' purpose is to enrich lives and progress society, using creativity and technology to build a better connected world. Amdocs and its 25,000 employees partner with the leading players in the communications and media industry, enabling next-generation experiences in 85 countries. Our cloud-native, open and dynamic portfolio of digital solutions, platforms and services brings greater choice, faster time to market and flexibility, to better meet the evolving needs of our customers as they drive growth, transform and take their business to the cloud. Listed on the NASDAQ Global Select Market, Amdocs had revenue of $4.1 billion in fiscal 2019.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com