

---

## Next Generation Revenue Assurance Environment

Next Generation (NG) networks and services will create a challenging environment for Revenue Assurance (RA), as numerous fundamental issues will arise in view of the radical changes that will occur in the network architecture. These major technical changes will dramatically alter the RA evolution process that will need to be applied. This paper discusses some of the envisaged issues and provides an insight into the technical changes, including:

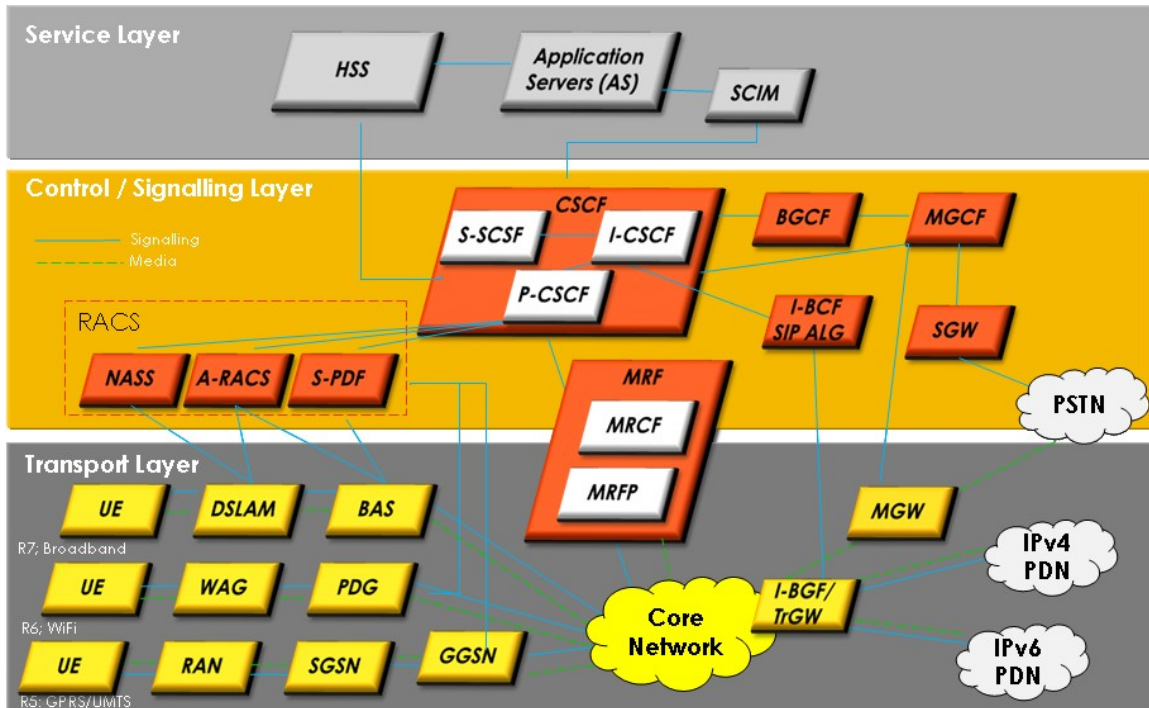
- The telecoms network will become fully IP, which will result in a completely new architecture of networks, with traditional switches being replaced by a number of new network nodes. This fundamental change will alter the way the technology of a network operates and will result in all of the key items managed today being changed.
- The principal RA concepts for items such as “switch-to-bill” will no longer be applicable as events will be made up of non-correlated items. Switches will be replaced with items such as: SBC, SRD, MGW, MGC, HSS, CSCF, ENUM and a range of application servers providing services like VoIP, IPTV, PTT, IM and Presence (*a glossary of abbreviations is given at the end of this article*).
- The bearers and services offered to customers will need to be separately managed with new RA techniques defined.
- There will be new identities to be used and managed - the more traditional concept of ‘A number’, ‘B number’ and duration etc. will be replaced with origination and termination SIPs or Tel URIs, and SIP events for set up connections and termination.
- There will be seamless movement of a customer’s service across a number of bearers, e.g. GSM, Fixed, WiMax, Cable etc.
- There will be a requirement for far greater convergence of RA with other risk management aspects, which will require completely new RA KPIs to be introduced.

### Next Generation Network Technology

NGN (next generation networks) make full use of IP and the type and level of transition from legacy systems to fully IP will dictate the level of new nodes. One major distinction is that the bearers which carry the services offered, such as GSM (3G), Data, WiMAX, Cable or Fixed will be carrying data from an application at the terminal device to an application in the network. This technique has the effect of separating the bearer from the services offered. One of the common forms of NGN is to use IP Multimedia Subsystem (IMS) as an architectural framework. This was originally designed by the wireless standards body 3GPP and is being used for delivering IP multimedia services to end users from a wide variety of bearers. It is part of the vision for evolving mobile networks beyond GSM, but has been updated to include the migration and convergence of the other access bearers – mobile, fixed and NGN platforms. The premise is that where possible, it will use Internet standards and protocols such as SIP. The intention of IMS is not to standardise applications, but to aid access of multimedia and voice applications across wireless and fixed terminals.

A major element of NGN/IMS design is that it provides horizontal control layers that isolate the access network from the service layer as depicted in the diagram below. Each service is not required to have its own control function as it has a common horizontal layer. Because it is an enabling technology, it is difficult on its own to justify and, in particular, to specify the RA and security controls, as they are related to the access provided and to the services carried.

IMS provides the ability to have ‘integrated services’ that are used to deliver specific services, which are independent of the access method and potentially also independent of the network operator. This integrated services approach will provide benefits in the collection of information for the purposes of RA and risk control, which will be dependant on the type and points of collection.



## New Next Generation Identities

NGN enabled terminals, fixed or mobile, need to be able to manage the IP and IMS connections and to handle the associated protocols and new identities used. In existing networks, the identities used are relatively simple and, in principle, are fixed for the customer (eg. a fixed directory number, MSISDN & IMSI).

With NGN there are several new identities, for example, IMPI & IMPU. Both of these are not phone numbers or another series of digits; they are URIs. Numbering can also be different, which is performed using ENUM (DNS), which is set up to allow movement of numbering between the IP and PSTN (legacy) worlds and to enable security or routing changes (call forward, call transfer etc.). Billing events from different information sources occur and control gateways such as an SBC are used instead of interconnect gateways for IP operators.

The identities and numbering used can be dynamic and therefore harder to understand for a RA analyst. The risk management systems will need to manage multiple identities in a logical way, more so than is currently required. In addition, nowadays there is generally one account for the customer who owns and uses the service, but this will not necessarily be the case in an NG environment, as different accounts for different services could be utilised and operated.

## Service Provisioning

The fact that many services will be based on a monthly flat fee (for items such as broadband access, VoIP and IPTV) will focus the RA process more on the provisioning controls in preference to items equivalent to 'switch-to-bill'. RA practices to establish the correct provisioning of the network will need to involve far more points in the network, as provisioned information will reside not only in one or two places (such as the switch or HLR), but also in platforms like HSS, SRD, SBC, application servers (such as a VoIP application) and even in the server controlling access to the bearers such as BRAS. All of these points will need to be compared and validated to establish correct provisioning with the initial provisioning platform.

Therefore, the RA focus will need to change fundamentally to meet these technical changes. Whereas today, where all information is either in the Billing and Customer Care Systems (BCCS) or in the IN platforms for prepaid, in NG converged networks there will need to be a common service profile for the subscribers. This will include the service and bearer component from the fixed and mobile environments. In a full NGN/IMS environment, the HSS user specific details (such as identities) would not be held for the services used. This profile would be in the SRD/application server (unlike in GSM where all information is held in the HLR) and it would only cover the service layer. The bearer layers would have their own controls and access systems, such as BRAS.

For many years there will be a mix of infrastructure with different identities and service profiles defined in several locations, which will add complexity for RA controls. This approach will require additional tools to manage the identities and services actually being used. It is therefore extremely important that the RA function is involved as much as possible to understand exactly how the layout of the network will look – not on a technical level, but from a practical perspective. Even with legacy networks which are much simpler, there are still significant issues providing the data required for reconciliations, monitoring and controlling from an RA and fraud management perspective. If the NGN is designed without any consideration of the future RA requirements, significant additional costs could be incurred by operators, who might have to invest later in workarounds in order to provide the required data.

## **RA Monitoring & Control Points**

The classic approach of determining and setting up monitoring points for data comparison for RA purposes will still exist to some extent, however the network and mediation points are likely to change. Information is more likely to be collected from IP and NGN application servers via special dedicated mediation systems, which will build records based on events in the service set up and use. Events can be collected from either signalling or mediation systems; however, the type and volume of information collected is far more complex than for existing RA purposes. Many existing systems will not be able to cope with the changes required to handle the variety of data. For example, in the IP and NGN environments, the signalling used is SIP and DIAMETER, which is not the same as the SS7 message format or classic billing formats like ASN1. Therefore, the points of collection selected for comparison for IP and IMS RA control will depend on the configuration of the network and the billing/charging model used. It is envisaged there will be many more free services, such as SIP-to-SIP calls. All these changes will necessitate new requirements for RA activities for the control and monitoring of the NGN/IP infrastructure.

## **Identity Mapping**

The integration of the new IP and IMS identities will be a key part of linking the services and transport layers in these networks where these two are separated. The information can be fixed or dynamic; therefore mapping the identities together will be of paramount importance. Operators will need to map these identities to provide one common resource that automatically links information from the different service layers to the respective bearer layers and the relevant account level.

Items to be mapped between systems can be stored either in a separate database of the RA management systems or in the feeder system, such as in the dedicated NGN mediation platform. This would be similar to today, where an enquiry of the billing system and HLR/AuC could be made to view customer details in the network and also the customer name, address information and payment data.

## **Node Log Information**

Due to both the integration and risks associated with IT networks and also the services and bearer layers in the telecoms part being IP based, the control over access will reside with the various network nodes and will not directly be related to one access control device, such as a switch or a mobile network's authentication system. This implies that, to review who accessed the network and to determine which services they used, there will be a requirement to review 'log information' from the nodes. This approach is unlike today, where connections are made for periods of time where there is a billing record, or by directly monitoring all the signalling messages.

Application servers, for example, retain details for a limited period of time of all the SIP messages used in the session set-up. These can be used for RA purposes to ensure that the client has used the correct services, by building up profiles of usage based on the messages. Other network devices can also be used to assist in performing RA analysis of the bearer and service usage by reviewing the activity logs for firewalls, log servers, syslog servers, SBC etc., which can control and log activity. However, the collection devices are generally configured to have limited event logging, due to the loads on the devices themselves and the services passing through them. There is, however, the potential to obtain significantly useful data from these devices, mostly related to events, which would be a valuable source for RA intelligence.

## **Revenue Assurance Measurement**

Similar approaches will be required for measurement in the NG telecoms networks, but the information sources and how this information is interrelated will be different. The convergence of services causes the convergence of risks and revenue loss detection, with services moving between different network bearers. The required tools and changes in perfecting new RA techniques will need to evolve in line with the technology advancements in order to combat these risks.

The level, type and extent of RA losses that will be experienced will be based on the charging method applied by the operators for the bearer and services offered, which will be dictated by the commercial charging methods of the specific operator. There will be a general tendency to migrate away from payment for the level of services used, particularly for voice calls and data consumption, to a scheme of flat fees for use up to certain defined limits. This will necessitate a greater focus on provisioning assurance of both the bearers and services offered, as this is how additional services such as IM/Presence and Call Mobility will be charged for.

The RA control and measurement points for items such as; platform integrity to ensure consistency of CRM systems, real time billing used for prepaid, HSS, SRD, SBC and application servers, and the events processed by nodes such as CSCF, will all need to be defined and tested to provide comparison capabilities for RA. Revenue control will be required for the billing events logged in the nodes versus those generated in the billing events from the application servers and compared against those placed in the final bill or in the on-line billing accounts, in order to ensure revenue integrity and accountability for RA purposes.

## **Next Generation RA KPIs**

KPIs are the critical summary statistics used in RA to measure the changes in the performance of the network on a regular basis. In NGN there will be changes in the points of measurement, which will result in changes being required to the traditional and most commonly accepted KPIs. Some examples of the new KPI requirements will include:

- Provisioning checks and reconciliation between each of the following: HSS, SRD, application servers and other access bearer authentication servers
- IP interconnection accounting and RA using counts of SIP session states - between the interconnect party and the operator, both for SIP and DIAMETER messaging
- Summary of the SIP messages by type to ensure that there is a match between the start and completed messages and also the billed events
- Validation of rates and times based on the event message headers versus the billing system
- Errors generated by the NGN mediation correlate function versus the event messages created
- Continuous streamed events being correctly terminated versus those which are billed, including errors notified by incorrect cause code or customer complaint
- Service headers in SIP messages being correct for the services billed to ensure that no services are carried and incorrectly treated when compared to the billed activity
- Real time event triggered decrementation versus event billing record errors
- Level of SIP-to-SIP based free calls with no external usage compared to billing
- Level of unallocated IP records
- Unknown URIs in the Billing System

## **Next Generation RA System Requirements**

In the NG environment, additional controls will need to be defined and implemented for RA management, and in particular, from a provisioning and non-correlated event perspective, which will necessitate the use of log based information in addition to the existing RA practices currently being conducted. The key areas envisaged for such systems will include:

- Collecting new information for RA monitoring points from signalling systems, the mediation server for building event records and also log information from network nodes
- Flexible aggregation method of IP records and the possibility to allow for additional platforms
- Defining the required KPIs for linking of services and bearer layer identities and identity management
- Profiling the use of services for each individual subscriber and developing service profiles; this is unlike today where it is assumed that people have the right to use the services and where the extent of use is reviewed for fraud
- Profiling the use of service for different network elements to highlight unusual trends
- Monitoring different origination and termination identity types; currently these are generally linked to one account identifier, but in the IP/NG world, the display and management will need to show other identities
- IP and other identity tracking is needed to support the RA analyst to understand customer activity and billing, by mapping the bearer and service routes, and by monitoring and analysing the activity

In the future, profiling which bearers and services the customer uses will need to be performed in order to detect RA risks and to also manage accuracy, completeness, timeliness and validity across both domains. This will be achieved with new forms of provisioning assurance, financial based settlement processes and data assurance, by using the new and existing data sources. Most significantly, there will need to be a greater focus on the RA provisioning activities. There will, however, be new activities to be conducted and new KPIs to be developed, which will impose changes to the Revenue Assurance Systems (RAS), as they will need to be able to deal with new bearer and services types with numerous generic types of NG services that will require monitoring, such as:

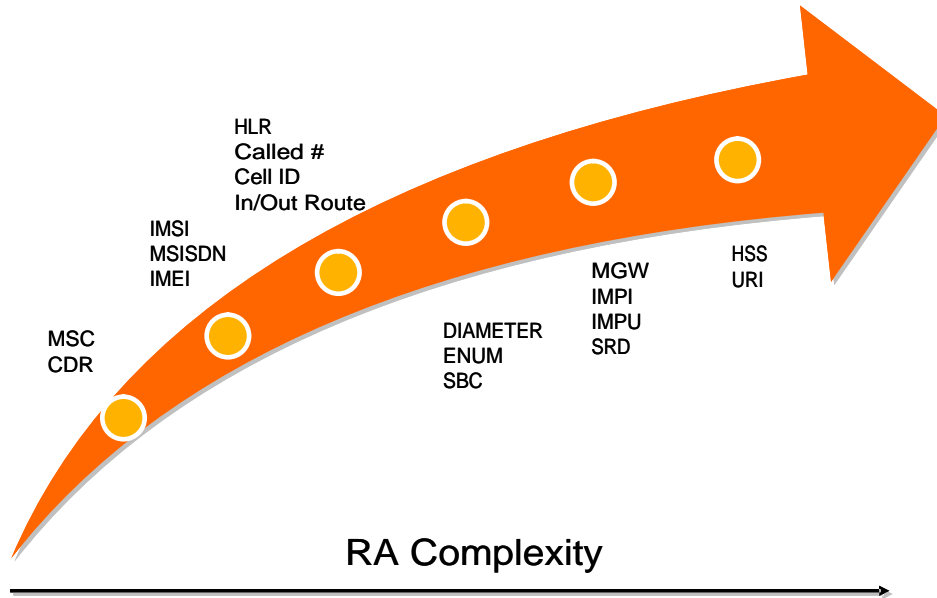
- Voice-based (VoIP, IP Centrex, IMT)
- Message-based (SMS, MMS)
- Streaming-based (IPTV, VoD)
- Interactive (e.g. Second Life gaming)
- Content-based (e.g. games, downloads)
- Subscription-based (e.g. location services, IM, presence indication)
- Pay-per-Push

## **Next Generation RA Strategy**

RA functions will need to comprehend and understand the direction their company is taking as most operators will have deployed NGN within the next few years. The RA strategy will need to be re-evaluated to take into consideration these advancements and the changes in the fundamental technology that will be used. An evaluation of the RA organisation's skills and knowledge will need to be conducted. Consideration will need to be given to the necessary training requirements required on IP and NG networks and systems. The RA capabilities already in place will need to be assessed to determine the effect of all these envisaged changes and to evaluate how RA will be managed in the future.

Existing RA tools and techniques will require evaluation to determine whether they will be able to cope and to assess whether there will be a requirement to look at alternative risk management products and solutions. The overall emphasis and shift in RA activities for data integrity, profiling of services, usage and customer spend will all need to be determined, tested and evaluated. There will be a fundamental requirement to conduct NG risk assessments for all new IP services to establish the RA monitoring and controls required using the new data sources and monitoring points.

These are major changes and challenges not previously faced and most operators do not yet have the required skill sets within their risk management teams. The actual risk assessments will require multi-disciplined approaches, including specialist technical knowledge with an appreciation of the NG networks and systems being deployed, as it is significantly more complex than the previous scenario of simply tracking a call record from the switch to a finance record.



The output from these risk assessments will be required to specify the 'NG-RAS' requirements and the data processing needs and activities required for effective RA in the future. The RA evolution line is changing and operators need to plan accordingly to meet the demands that NG will bring from a revenue protection perspective.

## Glossary

The following glossary is provided as a reference for some of the key NG industry terms:

AS	Application Server	IMS	IP Multimedia Subsystem
BRAS	Broadband Remote Access Server	MGC	Media Gateway Controller
CSCF	Call Service Control Function	MGW	Media Gateway
DNS	Domain Name Server	NGN	Next Generation Networks
ENUM	Electronic NUMbers	PTT	Push To Talk
HSS	Home Subscriber Server	SBC	Session Border Gateway
IM	Instant Messaging	SIP	Session Initiation Protocol
IP	Internet Protocol	SRD	Service Resources Database
IPTV	IP Television	URI	Uniform Resources Identifier
IMPI	IP Multimedia Private Identity	VoD	Video On Demand
IMPU	IP Multimedia Public Identity	VoIP	Voice over IP

## Next Generation RA Consultancy

Præsidium has already developed extensive experience in the provision of NG RA consultancy and offers a range of dedicated NG RA services, including product/service reviews, organisational assessments, RAS requirements definition and employee training. For further information on NG RA, please contact Præsidium:

**Tel: +44 118 922 4444**

**Email: [info@praesidium.com](mailto:info@praesidium.com)**