Anti-Fraud & Revenue Assurance

Who Should Attend?

This training is intended for employees of mobile operators involved in fraud detection/prevention and revenue assurance, including the customer service, finance, and IT departments.

Course Content

Part I: Introduction to Revenue Assurance (1.5 day).

This section covers how to protect revenue (revenue assurance) within the revenue chain. We will discuss threats against main revenue which orginate within the Telco industry itself. Selected processes will be presented:

1. Retail sales / prepaid / postpaid.
2. Wholesale market (interconnect, international roaming, national roaming) – revenue cost assurance.
3. Handset sales / distribution
4. Other (by request)
5. Based on the above processes, the operational controls are presented with the necessary details and examples. In addition, we will discuss a successful RA strategy building process.

Building automated tools for supporting more complex operational controls – embedding automated controls as a target for effective organisation – explaining simple tools for faster loss recovery. What kinds of tools are useful? Self-made or store-bought – which ones are better (pros/cons) and recommended. IT tool preparation – tool configuration, building, and special requirements.

Organisational issues play an important role in building a successful process (SWOT) – selected models:

1. Distributed vs. centralised organisation.
2. Building an organisation from scratch.
3. Reporting level issues.
4. The importance of financial accountability.
5. Key targets for RA organisation distributed over the organisation (management by objectives).
6. Risk Management – potential owners of the risk management process.
7. Benchmarks for an effective organisation, RA KPI.

Business models for outsourcing / consulting for revenue loss recovery – benefit share or fixed price (time and material) – maturity level dependence.

1. How to recognise the possible risks of new products and offers..
2. How to implement operational controls for a new product without killing your business.

Possible synergies, awareness, reporting, an opportunities for extra revenue.

Part II: Technical Fraud, including 3G/4G network fraud (0.5 day).

1. This section explains key procedures for detecting technical fraud (internal/external), and covers how to manage external technical fraud.
2. Technical vulnerabilities in new product development – how to prevent technical fraud. Offer / tariff plan construction (do's/don'ts).
3. Implications of GSM/3G/4G: basic security issues, authentication, SIM cards, 3G services (data transmission, video transmission); 3G/4G implementation risks.
   - SIM Boxes / FCT – examples of bad product marketing in terms of technical fraud; case study.
   - The results of FCT/ negative impact on revenue, customer quality perceptions – key indicators of FCT usage. Revenue impact calculation – high impact on bad debt – case study. FCT types (sim card server, distributed radio, directional antennas) – examples from the market.
   - SIM cards and scratch cards – an important issue for technical fraud prevention. How to deal with the loyalty points exchange (i.e. CRM system) – case study of possible fraud.
   - Prepaid platform charging/billing – key issues impacting revenue loss due to fraud (tariffs, tree of billed data, typical financial reports for detecting technical fraud within prepaid platforms).
   - Premium Rates – drop-box tariff phenomena, how to construct the terms and conditions for the revenue share partners to avoid bad debt/losses.

Part III: Fraud Aspects (2 days).

1. Fraud types in GSM networks.
   - Three major types of fraud:
     - Customer fraud.
     - Dealer fraud.
     - Technical fraud.
   - Fraud vs. collection.
   - Fraud vs. revenue assurance.
   - The definition of fraud.
   - How to calculate fraud.
2. Fraud prevention.
   - Law and regulatory environment.
   - Activation process.
   - Document requirements.
   - External databases - stolen documents, fault documents, etc.
   - Dealer’s obligations.
3. Statistical fraud detection.
   - Customer’s profile identification.
   - Dealer’s network weaknesses detection.
   - Business case for fraud “business”.
   - Fraud generating offers.

- Fraud generating services.
- Recognition of common fraud patterns.

4. Online fraud detection.
   - Fraud segmentation.
   - Rules and threshold settings - case study.
   - Types of alarms, alarm strategy.
   - Alarm setting tuning.
   - Alarm management.
   - Data availability + rating vs. pseudo-rating.
5. Fraud in 3G/4G.
   - 3G/4G specification from the customer’s perspective.
   - New types of Fraud / Revenue Assurance actions.
   - Data transfer vs. roaming.
   - 3G/4G based services => fraud analysis.
6. Fraud vs Mobile Number Portability (MNP).
   - Overviev of mobile number portability process.
   - Main fraud threats.
   - Technical and business aspects of fraud detection for ported customers.

Course Objectives

Various aspects of fraud are studied from an operational and technical perspective. Fraud classification and prevention methods are described. The technical side of fraud is revealed, and various detection methods are explained. Aspects of 3G/4G fraud are mentioned, and the main aspects of the Revenue Assurance process and tools supporting it are described.

Prerequisites

General knowledge of the mobile operator business.

Training structure

Four-day training divided into logical sessions.

Methodology

Instructor-led training, using presentation slides and examples from real networks.