2024 Program

GRAPA

Fraud & Cyber Fraud Management for Telecoms

Telecoms Fraud & Cyber Security: MasterClass

Telecoms Fraud & Cyber

MasterClass

Certification

Certified Analyst — Fraud & Cyber Security Management (CTFA)

This professional level certification focuses on a practical, hands-on, standards-based approach to traditional fraud management along with the inclusion of the critical cyber security dimensions important for modern telecoms fraud management . For practitioners performing the function on a day to day basis, this is an essential program of training and credentialization. It provides team members with the framework and techniques, as well as the professional stature required for analysts to be successful in their organizations – enabling and motivating them to effectively pursue risk wherever it can be found.

Requirements for CTFA Certification

Prerequisites: Attendence and certification in GRAPA Apprentice Certification

- **GRAPA - Free Apprentice Certification Programs are available online live or On-Demand regularly throughout the year. See your membership manager or consult the webiste for details.**
- **Experience and/or participation as a practicing member of a telecoms fraud management, cyber security or risk management team**

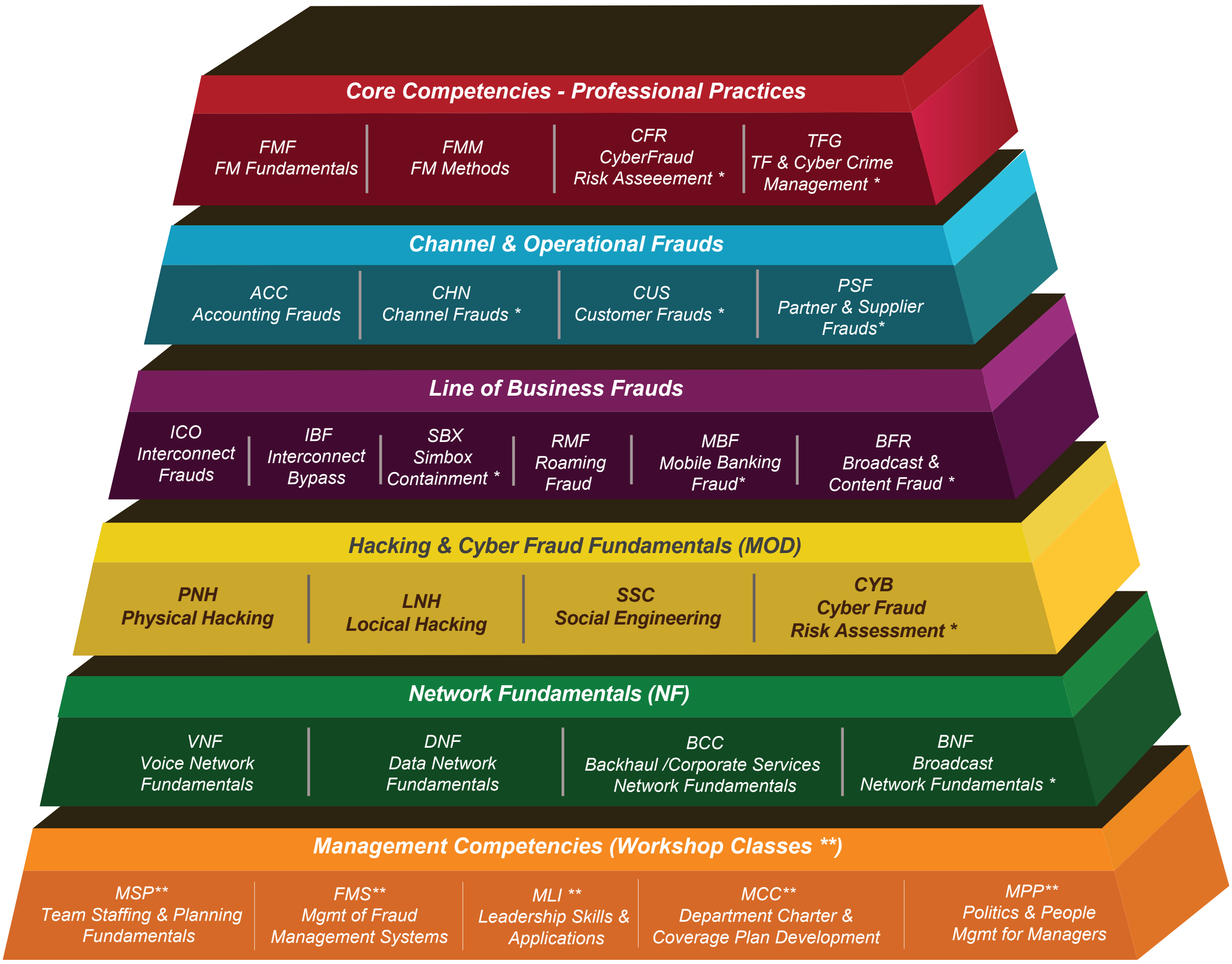
Fraud Management Competency Based Programs

Telecoms Fraud & Cyber Crime Competency “Units”

GRAPA’s training and certification programs are based on the delivery of classes, organized into two four-hour units, where each unit focuses on one of the core competency or applied competency domains critical to the professional and competent practice of Telecoms Fraud & Cyber Crime Deterrence.

This competency pyramid has been organized according to the U.S. Department of Labor guidelines, and summarizes the body of knowledge and competency domains, as defined by GRAPA members and managers from around the world.

Students and managers can build “custom” programs by assembling different units to meet the requirements for a specific certification. Units are available live online, in recorded on-demand sessions, or delivered live onsite at the company’s location.



Core Competencies - Professional Practices

FMF FM Fundamentals | FMM FM Methods | CFR CyberFraud Risk Asseeement * | TFG TF & Cyber Crime Management *

Channel & Operational Frauds

ACC Accounting Frauds | CHN Channel Frauds * | CUS Customer Frauds * | PSF Partner & Supplier Frauds*

Line of Business Frauds

ICO Interconnect Frauds | IBF Interconnect Bypass | SBX Simbox Containment * | RMF Roaming Fraud | MBF Mobile Banking Fraud* | BFR Broadcast & Content Fraud *

Hacking & Cyber Fraud Fundamentals (MOD)

PNH Physical Hacking | LNH Locical Hacking | SSC Social Engineering | CYB Cyber Fraud Risk Assessment *

Network Fundamentals (NF)

VNF Voice Network Fundamentals | DNF Data Network Fundamentals | BCC Backhaul /Corporate Services Network Fundamentals | BNF Broadcast Network Fundamentals *

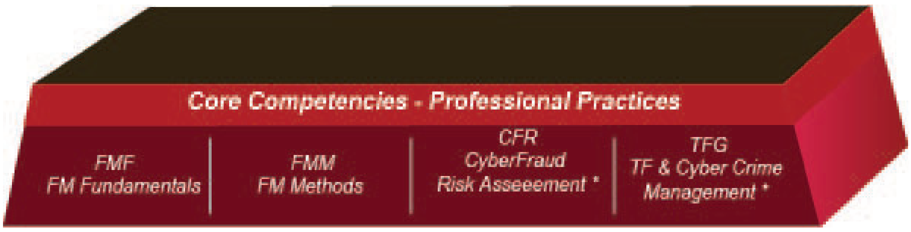
Management Competencies (Workshop Classes **)

MSP** Team Staffing & Planning Fundamentals | FMS** Mgmt of Fraud Management Systems | MLI ** Leadership Skills & Applications | MCC** Department Charter & Coverage Plan Development | MPP** Politics & People Mgmt for Managers

Fraud Management Competency

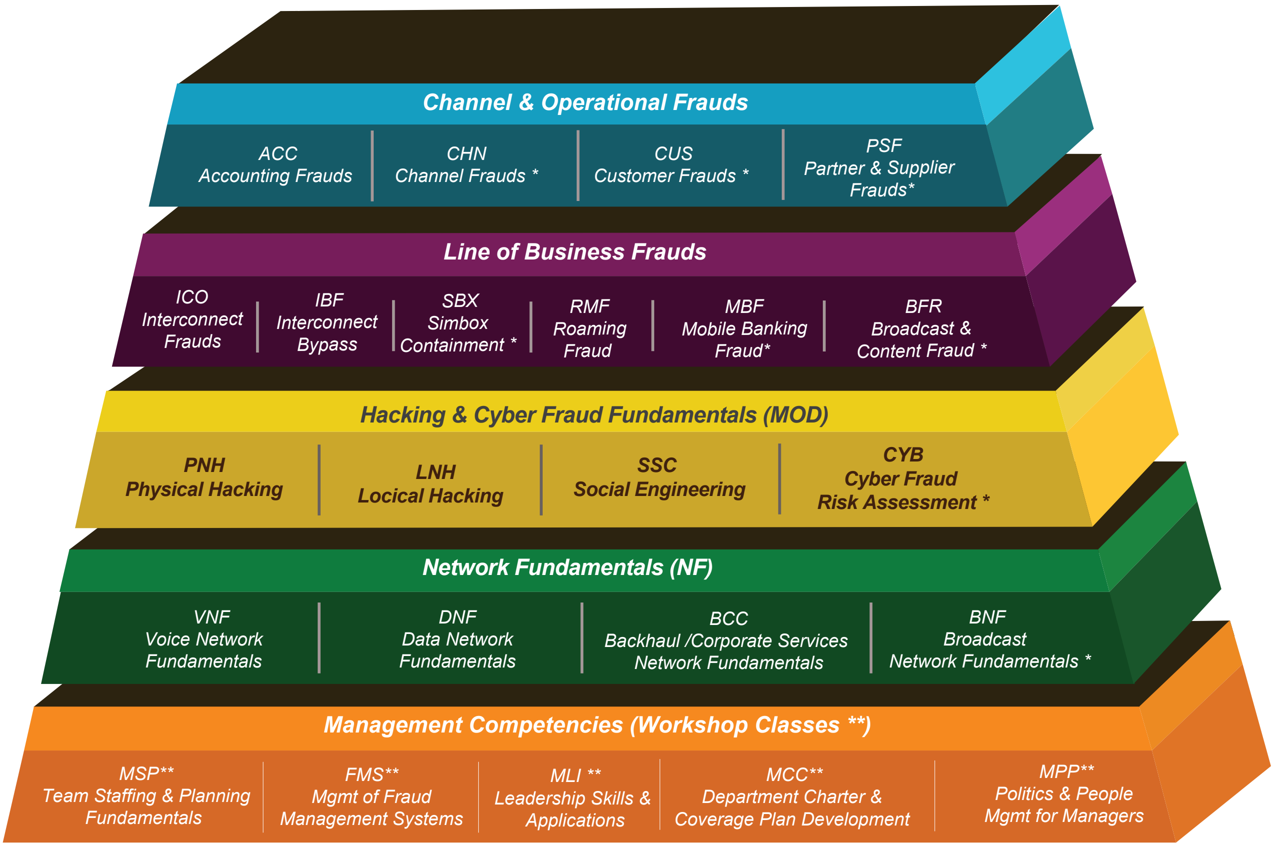
Core Professional Competencies

Core competencies describe the basic methods, best practices, and organizational guidelines that the fraud and cyber-crime analysts apply to any of the situations they face. Core competencies describe how to do the job and how to assess how well the job is being done. These are the fundamental tools that the professional uses in the day to day activities. Students are required to complete the requirements for at least two of the core competency areas in order to certify as a CTFA professional. Specialist certifications will usually require at least one core competency unit as prerequisite to certification. (A student who has qualified once does *not* need to retake any unit.



Applied Competency Areas

The real test of the effectiveness of the professionals is in how well they apply their best practices skills to a diverse assortment of different technologies, business models, and situations. The applied compentency model sections recognize several different areas where the fraud & cybercrime analysts will apply their skills. To qualify for CTFA certification, the student is required to select and complete at least 8 of these applied competency areas. Specialist certifications specify different combinations and prerequisites.



Core Competency Units

FMF - Telecoms Fraud Management Fundamentals

In this fundamental course, students uncover the history, the standard approaches, best practices and key methodologies that help the professional develop an effective, efficient and scientific approach to fraud management.

FMM - Fraud Domains, Tools, and Methods

This unit provides students with the context and case studies of the most commonly addressed telecoms fraud management scenarios, the use of FMS and other approaches.

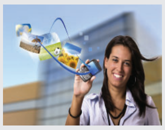
ACC - Accounting & Financial Systems Frauds

This course is designed to provide billing and assurance professionals with a comprehensive guide to the design, assurance, and audit of data roaming environments. Key controls and the roles of DCH, GRX and other roaming exchange models are considered. Standard controls for the environment are highlighted.

Network Fundamentals - Applied Competency

VNF - Voice Network Fundamentals

Understanding voice networks and how AAA (Authentication, Authorization and Accounting) is maintained is one of the most critical and often ignored of the applied competencies. This unit covers the basics of circuit networks, switching, CDR management, and the many fraud exposures inherent in the makeup of voice networks.



DNF - Data Network Fundamentals

Protection of data networks and services associated with public (Internet IP) and private (IPX) data services is the backbone of most modern ICT service offerings. Students are introduced to the terminology, business protocols, and key controls associated with understanding and protecting consumer data networks of all types.

BCC- Backhaul / Corporate Services Fundamentals

This course is designed to provide fraud & cyber crime professionals with a comprehensive guide to the understanding of and fraud protections for broadband and corporate data services. Included is coverage of DCH, GRX, IPX, Tier 1, and other broadband service areas. Also included is an overview of the many fraud/cyber risks inherent in corporate services management.

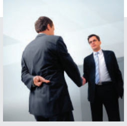
Hacking & Cyber Fraud Protection

PNH - Physical Hacking - Radio & Cable Hacks

This unit provides students with a comprehensive review of the many different ways that fraudsters and hackers can violate the physical network via splices, T-In, Man-in-the-Middle attacks and others. Understanding how fraudsters get in, and how they use physical incursion as their first step to performing fraud, is tantamount in preventing it.

LNH - Logical Network Hacking

After gaining access to the physical networks, the fraudster must figure out how to bypass your logical security mechanisms. The term “hacking” most often refers to the ways that fraudsters bypass logical AAA controls in voice and data networks, and this unit provides a comprehensive review of the different methods, and techniques for containment.



SSC - Social Engineering, Collusion & Customer Frauds

The third leg of any good fraudster’s attack vector is the “social engineering” angle. Good frauds take advantage of people’s weaknesses and distractions to help maximize the money they can make using these time tested and highly effective social engineering techniques. This unit reviews theses methods and sees how they are applied to real world fraud scenarios.

Line of Business Fraud - Applied Competencies

ICF - Interconnect Frauds

In this unit, we provide fixed and mobile professionals with an understanding and a roadmap that shows how their networks are getting from where they were (2G – POTS- ADSL) to where they are going – IMS, MPLS, HETNETs and beyond.

IBF - Interconnect Bypass Frauds

The bypass of earned revenues by fraudsters is one of the major sources of revenue loss for the operator. SIMBOX, refiling and other techniques make it easy for fraudsters to make money at your expense. This unit builds on the foundational information covered in the ICO interconnect fraud class and drills down on the issues of bypass frauds.

RMF - Roaming Fraud Management

This unit presents an overview of assuring financial systems and controls related directly to revenue management, including revenue recognition, revenue accounting, audit of revenue management switches and systems, and the overall *Controls Inventory* and discipline developed and advocated by GRAPA members.

Specialty Units (by special arrangement)

ASC - Channel and Sales Frauds

In this fundamental course, students uncover the history, the standard approaches, best practices and key methodologies that help the professional develop an effective, efficient and scientific approach to fraud management.

CEF - Cyber Enabled Frauds

This unit provides students with the context and case studies of the most commonly addressed telecoms fraud management scenarios, the use of FMS and other approaches.

MBF- mBanking Frauds

This course is designed to provide billing and assurance professionals with a comprehensive guide to the design, assurance, and audit of data roaming environments. Key controls and the roles of DCH, GRX and other roaming exchange models are considered. Standard controls for the environment are highlighted.

MVO -MVNO Frauds

Understanding voice networks and how AAA (Authentication, Authorization and Accounting) is maintained is one of the most critical and often ignored of the applied competencies. This unit covers the basics of circuit networks, switching, CDR management, and the many fraud exposures inherent in the makeup of voice networks.

Specialty Units

Speciality units, like all other GRAPA curriculla, are 4 hour summaries of the latest best practices, methods and competencies associated with the subject. Each unit is prepared based upon: Assumption of prerequisite units from the Core Curricullum, and a specific need and focus as directed by the manager(sponsor) for the certification event.

There are dozens of available specialty units that have been prepared for manager/ sponsors over the years. Information about specific units can be discussed with

Unit 0: TFI - Introduction to Fraud Mgmt

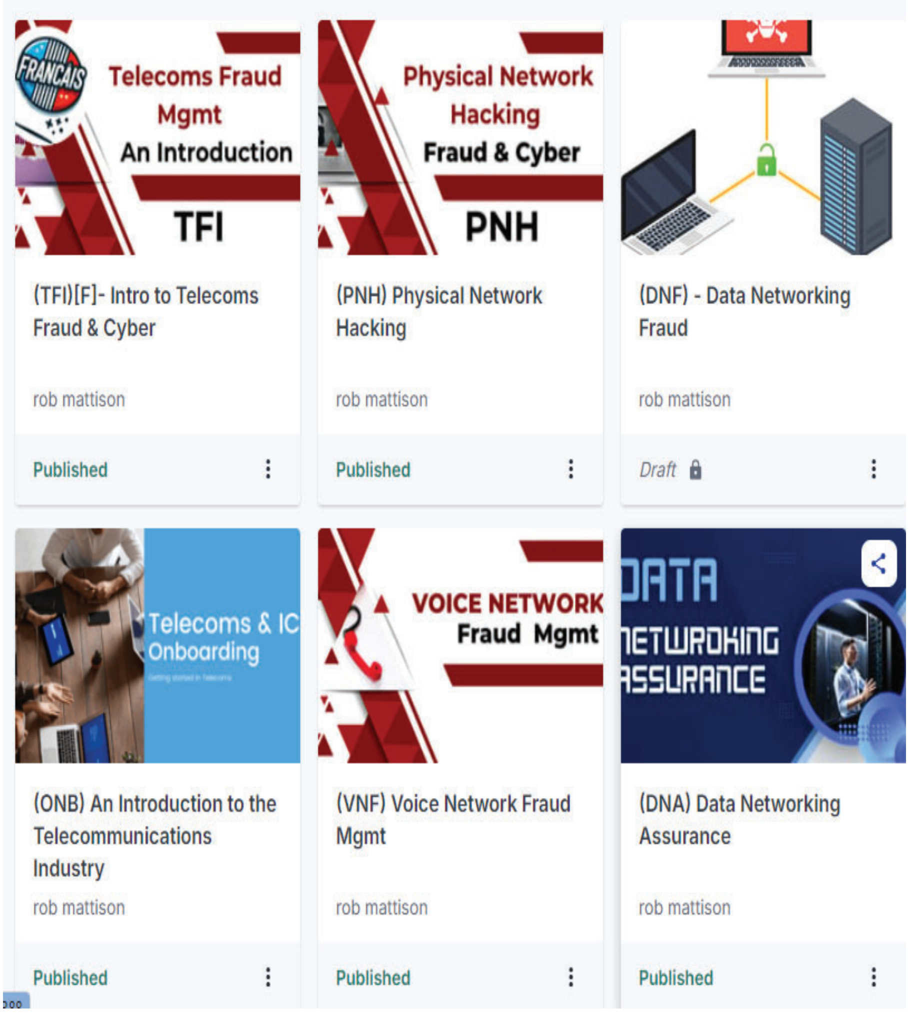
An introduction to the world of Telecoms/ICT and Fraud

Unit Overview:

The telecoms industry is undergoing a significant transition, with the role of Telecoms Fraud professionals becoming increasingly important and complex. As cyber attacks evolve, the expertise of these professionals is more crucial than ever, requiring adaptation to new threats. Students will learn the basic terminology, concepts, and unique approaches that network engineers and telecom professionals use to manage the complex and diverse products and services offered by telecom companies. The course will cover the core competencies of Telecoms Fraud Management, exploring its past, present, and the emerging synergy with Cyber Security that will shape the future of the profession

Key Objectives

- How roles are organized in the telecom
- Roles of Engineers, Sales, Marketing, Finance and Governance
- Role and definition of the Fraud Management function
- How telecoms manage risk in a unique way
- How Telecoms Fraud Managers works to mitigate risk
- The fluid and dynamic nature of the telecoms environment



(TFI)[F]- Intro to Telecoms Fraud & Cyber

rob mattison

Published

(PNH) Physical Network Hacking

rob mattison

Published

(DNF) - Data Networking Fraud

rob mattison

Draft 🔒

(ONB) An Introduction to the Telecommunications Industry

rob mattison

Published

(VNF) Voice Network Fraud Mgmt

rob mattison

Published

(DNA) Data Networking Assurance

rob mattison

Published

Unit 1: FMF - Telecoms Fraud Management Fundamentals

Industry Standard Approach & Methodologies

Unit Overview:

This unit provides the student with a comprehensive overview of Telecommunications Fraud Management and Cyber Crime Prevention as unique disciplines. While most industries have a fraud management function and are vulnerable to cyber crime, the complex telecoms technologies, business models and operational environments require specialized Fraud Management and Cyber Crime professionals with unique skills and knowledge requirements. Discussion of GRAPA's standards-based framework and approaches to telecoms fraud management and cyber crime: the FISHbone methodology, Incident Management Lifecycle, Situational Profiling, Fraudster Profiling, Behavior Profiling, Jurisdictionally analysis and others.

Key Objectives

- An introduction to the different management postures assumed by the telco regarding different types of fraud issues
- Explanation of FMS, how it works and its role as part of the Fraud team
- The principle KPIs for FMS, how to optimize FMS performance
- Understanding of incident management and case management. The incident management method and issues

Unit 2: FMM - Fraud Management Domains, Tools & Methods

Maximizing Fraud Management System Value and Efficiency

Unit Overview:

Learn the key functions and uses of fraud management and criminal forensic systems, what they are, how they are used, functionality, differences and comparisons between key vendors/software, how to buy a system, what to look for, how to benchmark different software/hardware configurations to fit your environment. Some topics included are application of advanced methods to the running of a fraud management system, including the use of advanced statistical analysis, neural networks, regression analysis, as well as key considerations in calibrating alarms, balancing false positives with detection objectives, demarcating responsibilities and KPIs for fraud analysts.

Billing for NextGen Services
Mastering the Telco Business Model
Roaming
Controls Mapping Workshop
RA Managers Toolkit
30 SEP
Corporate Sales Help Desk
Inter-connect
Fraud Protection Certification
Beginners Guide to Telecoms

Key Objectives

- Interconnect Fraud Overview
- Interconnect Controls
- Roaming Overview
- Roaming Frauds
- Accounting Overview
- Accounting Frauds

Unit 3: VNF   Voice Network Fundamentals

(Pssst....You Cannot Secure Your Telco Without This Information)

Unit Overview:

The telecoms fraud management discipline is often applied in an eclectic and often confusing way. Different organizations can have very different ideas about how best to fit the fraud management team into the overall governance framework. For this reason it is critical that the fraud professional understand and have access to the operational templates and best practices for fraud containment on an industry wide basis in order to better equip them to provide management with the guidance required when fraud events occur.

Key Objectives

- AAA (Authentication, Authorization and Accounting) for voice Networks
- Key commercial controls issues for voice network environments
- Fundamentals of Topology, Network Element integrity, and Referential Integrity controls for voice networks
- The role of the RA professional in the assurance of voice network environments

Unit 4: DNF - Data Network Fundamentals

IP Fundamentals for the Fraud Analyst

Unit Overview:

The Data Networks Body of Knowledge for fraud management covers all of those issues associated with the establishment of the security and integrity of 2nd generation and the NextGen – "3rd Generation" networks as well as fixed line networks. In the past, data network security was a relatively simple and straightforward process. But the modern world of Internet/IP based trafficking opens incredibly broad avenues that fraudsters can attack and that can make leakage a foregone conclusion. Included in this section are materials related to the history, principles of operation, operational vulnerabilities and key control areas for data networks. The information covered here has been identified as that matter that is critical foundational material and concepts required to truly understand and protect against nextGen / data / 4G / LTE / IMS/ Fiber and Het Net fraud vulnerabilities.

Key Objectives

- How do commercial internet data networks work from a fraud protection, security, accounting, billing and operational stand points
- Emerging standards in commercial and fraud controls for data networks
- Best practices in network assurance for fixed, wifi and mobile data networks

Unit 5: PNH - Physical Hacking - Radio & Cable Hacks

Traditional Telecoms Hacks & Modern Wireless Fraud Protection

Unit Overview:

Physical hacking is one of the oldest and most well understood exploit in the fraudster's toolkit. The exploding size and reach of today's networks only create more and more opportunities for the fraudster to gain illegal entry through a large number of different mechanisms.

The unit starts with a "hackers conversion guide" , which shows the different ways that physical hacks, logical hacks, social engineering and commercial positioning are combined to create hundreds of possibilities for unique fraud exploit chains.

Key Objectives

- Core networks (Switches, Router and Network element intrusion)
- Transit networks (backhaul intrusion)
- Radio network vulnerabilities and attack methods
- BSS-Billing-Accounting and I/T Systems attack profiles and protections

Unit 6: LNH - Logical Network Hacking

Protecting Customers, Society and The Telco

Unit Overview:

Computer hacking is broadly defined as intentionally accessing a computer without authorization or exceeding authorized access. Various state and federal laws govern computer hacking as a criminal activity, but the telecoms fraudster takes hacking to a whole new level, hacking not only computers but switches, routers and control mechanisms, all to make their fraud possible.

Key Objectives

- Internet IP Hacking – how it is done and used to enable telecoms frauds
- Top 10 IP Hacking techniques – including SQL Injection , PHP Include, Zero Day, Brute Force, et al.
- SS7 Hacking and Spoofing – how fraudster fake SS7 Traffic to enable interconnect, roaming, IRSF and SMS frauds
- Top wireless hacking domains including hacking of WIFI hotspots
- Top targets of fraudster hack including HLR, HSS, IN, Routing Tables, and Registries etc.
- Major types of hack attacks including Distributed Denial of Services (DDOS) as applied to IP and SS7 networks

Unit 7: SSC - Social Engineering, Collusion & Customer Frauds

This Represents 80% of Most Fraud Analysts' Time and Attention!

Unit Overview:

The three biggest enemies of the fraud fighter are social engineering, collusion and customer frauds. In each of these cases the fraudster takes advantage of the companies desire to TRUST EMPLOYEES, TRUST CUSTOMERS when putting together their procedures and systems.

This units provides the fraud analyst with an in-depth investigation of the last and most powerful of the Methods of Deception/Intrusion - the Social Engineering exploits. Social engineering allows the fraudster to gain intelligence about how things are done inside your operation, is tricks or pays employees to assist them in the conducting of their frauds and it allows fraudsters to pose as customers.

Key Objectives

- Social Engineering - An Introduction
- Collusion Roadmap - how to spot and prevent it
- Social Engineering - Old school cons and spoofs- how they do it without a computer
- Cyber Social Engineering - Email and Website Social Engineering techniques
- Customer Frauds - The Challenges of Know Your Customer(KYC)

Unit 8: ICF - Interconnect Bypass Frauds

Fight Traffic Piracy

Unit Overview:

In this unit, students will gain an understanding of the history, principles of operation, and key controls that are required if an adequate job is to be made of mapping and establishing proper fraud and security controls over the many different forms of the interconnect voice business.

Key Objectives

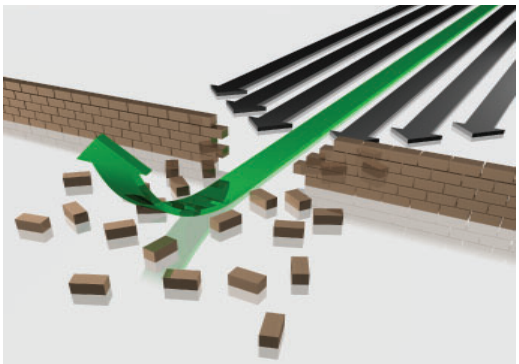
- An overview of the primary domains of interest for the Fraud analyst in the area of wholesale voice (interconnect).
- The traditional voice interconnect architecture, business model and control domains are reviewed.
- A description of the exploit chain, preventive measures and methods of control to prevent and monitor settlement fraud risk
- Review of the major forms of non-network based injection frauds including Call Sell, Premium Rate and Wangiri Frauds

Unit 9: ICB - Interconnect Injection Frauds

Securing the Interconnect Environment

Unit Overview:

Interconnect traffic frauds represent the biggest category of fraud losses to the typical telecom, and are the most difficult to assess and manage. In this unit students will be introduced to the major categories of traffic fraud (Network Injection, Bypass (Simbox), Bypass (Refiling), IP-PBX Hacking, and Tee-In Frauds). Students will understand the architectural and procedural weaknesses that fraudsters exploit in order to make these fraud happen, and will be provided with insight into the many methods of exploit chain mutation that creates the dizzying assortment of variations on the fundamental themes.



Key Objectives

- Overview of the nature and method of execution of bypass frauds. Included are SIMBOX, Tromboning and refiling frauds and how they work
- Study of the working of SIMBOXes as network elements, their legal and illegal application. Definition of the different parties that participate in SIMBOX frauds and the way that they accomplish their conversion
- A review of the 3 primary methods utilized to detect SIMBOXes, the FMS, TestCall and BI based approaches, and their strengths and weaknesses.
- A review of the 5 primary means of attacking simbox revenue loss via : SIM Cut off, SIM Supply Cut off, Prosecution, Arbitrage adjustment & traffic reversal

Unit 10: RMF - Roaming Fraud Management

Securing the Roaming Environment

Unit Overview:

GSM voice roaming represents one of the most profitable of the voice consumer areas for many carriers, but the ease of entry into the roaming ecosystem includes the implementation of dozens of additional fraud risks and the desperate need for additional controls. This unit provides the student with an overview and exploration of the roaming network, partnership and fraudster protection disciplines and the proven standard methods for the detection and deterrence of roaming frauds..

Key Objectives

- Partner selection, agreement management and price controls for roaming
- The settlement process, partner fraud risks and standard controls postures
- Key network provisioning and change management controls (signaling tests - the IREG, TADIG, Signaling partner role, and management)
- Symptoms of key roaming frauds (IRSF, CAP) and their remedies

School of Fraud Management

GRAPA Certification Offers Worldwide Recognition

The GRAPA School of Fraud Management provides the fraud management and cyber professional with an extensive catalog of Fraud Management and Cyber Security best practices, latest methodologies, and standards based approaches to the ever expanding, and ever more complicated world of the fraud and cybercrime in the emerging Information, Communications, and Technology Industry

This School allows professionals to gain access to the latest best practices methods training and certification in a way that is efficient, flexible and economical. Curriculla are organized into a customized selection of short (2 hour) online training sessions, each focusing on different key areas of competency development in the rapidly changing world of telecoms fraud and cyber crime prevention and containment.

GRAPA has offered certification for telecommunications professionals since the beginning of 2009 and in that time, hundreds of Telecoms Fraud and CyberCrime professionals have participated in dozens of different programs.

Our standards and best practices based approach to the develpoment of training programs assures that students are getting the latest in effective practices currently implemented by telcos of all types and sizes around the world. Because GRAPA's certification is based on professional principles and an in-depth standards-driven methodology, GRAPA's certified professionals are able to apply their skills not just to environments where they have personal experience, but across a variety of situations to address whatever new and unique problems they encounter. This is an absolute necessity in an industry where new business models and technologies are producing continuous upheaval and disruptive change.

GRAPA's certifications require intense and exhaustive continuous education and a stringent set of examinations and verification of relevant work experience, so they can provide management with a credible assurance of skills and ability. Management knows that, by utilizing certified professionals, their team members are trained and tested according to a uniform understanding of their profession and that they can apply those skills in real-world situations.

In the breadth and segmentation of GRAPA's certifications, professionals and organizations can be assured that, not only does GRAPA offer a 360º view of telecoms operations and revenues to those it certifies, but it is also able to offer that perspective at levels appropriate to the aptitude, ability and experience of those who seek certification – whether they are National Regulators, CFOs, Internal Auditors, Revenue Assurance and Fraud Managers, those with intermediate experience in telecoms, as well as those who are new or just starting out in Revenue Assurance or Telecoms Fraud.

Why We Are Leaders in Training Telco Professionals Around the Globe

Join the leading provider of fraud-cyber focused certification training events. Featuring exclusive presentations, real-world examples of procedures, solutions, and strategies that have effectively reduced fraud issues for telcos around the world.

After a number of years of providing best-in-class certification and training workshops to hundreds of telecoms risk professionals around the globe, we are pleased to announce our improved course offering.

Depth of knowledge

The topics and examples are "narrow and deep" rather than broad and vague, presenting you with focused, highly targeted information that adds real value.

Tailored content

Training is adjusted to align the needs of the students to the available material. Students are asked to fill out "GRAPA Benchmark Surveys" to determine the level and nature of the training required. The survey results help us determine how well you know your own systems, and provide clues about what you need help with. The principles and practices taught are also applied to cable, satellite, wireless voice, SMS, MMS, IPTV, and MMDS with equal conviction, detail, and effectiveness.

Relevancy

Class material is based on the foundations of GRAPA. GRAPA members from every geography, type of carrier, major type of technology, and carriers of all sizes review and approve these standard approaches. The material serves as the foundation for an industry standard approach that is applicable to everyone, and yet easily focused to the needs of specific sub audiences.

Based on Real-World Situations

The majority of the training is experience based "standard practices" in revenue assurance, harvested from the many revenue assurance, fraud management and cyber professionals who participate in "practices surveys," "strategy sessions," and other information-sharing events. Clear, specific deliverable are provided that apply to real-world situations. The material is never based on speculation, guesses, or invalidated information.

Interactive

The workshops are more than lecture sessions. classes are participative and interactive and students are expected to pro actively join in discussions, problem solve, and fill out benchmarks. Attendees have opportunity for much interaction with the instructor and other students. Lunch and breaks are devised to facilitate more intimate conversation.

Rob Mattison is a world-renowned expert in telecommunications and the revenue assurance , fraud management and cyber-security industry. He has 25+ years of hands-on industry experience. Rob is President of GRAPA and has authored dozens of books, papers and presentations on telecoms security, fraud protection and cyber risk.

Professional development

Students master vocabulary needed for creating a sense of professional identity and opportunities with other like minded people in the industry that share common goals and issues.