# Data, Voice & Cyber Fraud Management

## *Internet and Telecoms Certification Event*

**Communications Industry Fraud Academy**

### Fraud & Cyber Crime Certification Program

**Day 1: CyberCrime: the New Fraud Imperative**
**Creating an integrated cyber-fraud defense strategy** – *Learn the principles required to develop a truly integrated and comprehensive fraud and security protection strategy that protects your own assets, your delivery infrastrucre, and your customers.*

**Day 2: Voice Network: Protection & Vulnerabilities**
**The Phreak's Handbook - and how to beat it** – *Learn about the different and easy ways that phreaks (voice hackers) are able to penetrate your networks and hack into your systems. Learn the best controls and approaches to protecting your voice network services.*

**Day 3: Cyber Tech Foundations for Internet Security**
**Understanding the Internet Ecosystem - and how to protect it** – *Cyber Fraud is a lot more than just hacking a computer. Modern frauds are sophisticated exploits that involve the coordination of the efforts of dozens of parties. Learn about each of the layers and roles of fraudsters in the world, how they get in, and how they get away with it.*

**Day 4: Partner Frauds - The worst of the worst**
**Interconnect, Roaming, Content, SIMbox/Bypass, CAMEL** – *We will focus on the protection of partner-based business models (interconnect/CABs, roaming, content), and the key fraud exposures they bring. Detection and deterrence of SIMbox and roaming frauds are also discussed.*

**Day 5: CyberFraud Defense Strategies**
**Converged Security Approaches - Creating a team that can handle it all** – *The future of Information, Communication, and Technology carriers is bright, but the opportunities for cyber fraudsters is even brighter. Learn how to build a comprehensive CyberFraud Defense plan that leverages the best and brightest from your I/T, Audit, Network, and Fraud teams. Make your team CYBER-SENSITIVE and aware.*

**FRAUD**

**Hackers**

**computer viruses**

**Identity Fraud**

## Get Certified This Week!
### Join 1000 other professionals!

*Learn how to create an integrated and aware CYBER-PROTECTION TEAM.*

*Combine the best of Telecoms Fraud, IT, Security, and Cyber-Crime expertise*

- *Reprioritize your efforts*
- *Reduce costs and increase impact*
- *Make Cyber Fraud detection and PREVENTION a more mission-critical function*

**GRAPA**

# TABLE OF CONTENTS

# Certification and Customization
## Choose the Topics you Want Most at this 5-Day Certification Event

**The Unit-Based Curriculum Approach:**

Based on student feedback, GRAPA has updated the Telecoms Fraud and CyberCrime training to meet a wider variety of student objectives. While the majority of our attendees look to GRAPA training to help them earn the industry-recognized Telecom Fraud Analyst certification, more and more are now requesting a greater amount of flexibility and customization to their training experience.

To meet this need, we have re-structured our programs to leave more room for you to let us know exactly what you need to learn in your situation. This *unit-based approach* combines the pre-requisite training in fundamentals you need to understand advanced topic, and then allows the student to specify which advanced topics you want to pursue in greater detail.

Each day of this event is focused on core topics, and then allows for focused "on demand" drill down on the most critical areas.

**Results-Driven Training Approach**

GRAPA programs are grounded in the day-to-day, real world activities of Fraud, Security and CyberCrime professionals. Those who attend our events return to work with measurably greater understanding, tools, and skills to face the challenges of their environment. In fact, we define the success of our training by the increased value our alumni bring to their teams and organizations.

For this reason, as we communicate with prospective students, we will provide you with a "Customization Guide" and we request that you review this guide on your own and with your manager, and get agreement that the most critical learning objectives are being met. By incorporating a manager's perspective, potential students will have the opportunity to confirm that the topics covered in the training will make them immediately more valuable to their team and organization. Furthermore, it enables us to ensure that those issues most critical to our students' professional success are incorporated into the event.

**I Want Certification:**

Do you want to join the ranks of the 500+ GRAPA Certified Fraud Professionals? You can earn this honor at this event by successfully completing all 40 hours listed below. Taken as a whole, this certification program will provide you with some of the most tested, practical, and logical ways to prevent fraud and deliver real value to your organizations.

*Next Steps:*

➤ Express interest in certifying at this event
➤ Complete the pre-training course objectives survey to clarify training needs
➤ Based on survey results, we will provide you with a comprehensive lesson plan for the event
➤ Verify your lesson plan with your manager to ensure that training objectives will be met
➤ Work with your faculty advisor and membership manager to complete your registration for this event

## Fraud & CyberCrime Certification At-A-Glance

| Session | Day 1 | Day 2 | Day 3 | Day 4 | Day 5 |
|---------|-------|-------|-------|-------|-------|
| Morning Unit (4 hours) | Integrated Fraud & CyberCrime Protection - Best Practices | Security Fundamentals for Voice Networks | The Internet Ecosystem - A security perspective | Interconnect Simbox, Hack, Premium Rate & Injection Frauds | Cyber Security, Cloud, OTT, LTE & NextGen Services |
| Afternoon Unit (4 hours) | Fraud Management & Criminal Forensic Systems | Core Network & Radio Side Fraud Attacks & Defenses | Internet Cyber Crimes - Network Intrusion & Social Engineering | Roaming Fraud - IFRS, CAMEL & Credit Exploits | Assembling your Cyber-Protection Team t |

# GRAPA's 5-day Training Event for Voice, Data and Cyber-Fraud Professionals
## Certification Program Information



**Overview:**

GRAPA's Telco Fraud and Cyber-Crime Analyst Training is a 5-day certification and workshop event designed to provide attendees with a new, innovative, and comprehensive approach to the professional practice of combating fraud in Information, Communications, and Technology organizations as defined by the proposed GRAPA fraud standards, governance model, methodologies and framework. GRAPA's approach is exploit-library-driven, grounding fraud professionals in real-world risks and exposures.

**40-Hour Program Objectives:**

The 40-Hour Certification Program will meet the following student learning objectives:

• Provide students with a roadmap to understanding the new generation of cyber threats to the organization itself, your own I/T Systems, your service platforms and your customers

• Provide professionals with a comprehensive roadmap for understanding and anticipating these risks BEFORE THEY HAPPEN

• Learn how to integrate the activities of Fraud ANalysts, Auditors, I/T Security Teams, Network Engineers and product developers in order to assure the security and integrity of all of your service offerings , new and old.

• Learn how to decompose the many different layers of risk,and the development of a LAYERED APPROACH to detection and deterrence.

**Certification:**

Students who successfully complete the specified units (40 hours), pass certification tests, and have at least 6 months of verified work experience in telecoms will be awarded certification "Certified Anayst - Fraud Management."

**Who Should Attend:**

The primary audience for this certification training consists of telecoms fraud professionals. This includes those working with the fraud management system, internal auditors, forensic/investigative/law enforcement/legal professionals, logical and physical security specialists, finance, and business risk professionals as well as key operational managers in sensitive domains (billing, network, accounting, sales, supply chain, procurement, etc.).

**Our Promise:**

Students who take the training seriously, participate enthusiastically in activities, and pass the certification exams will be able to perform all practical applications listed under each course description.

# MORE THAN JUST TRAINING

## The GRAPA Experience !

### In the Classroom

**CHALLENGING CONTENT**

**DISCUSSION**

**CONFIDENCE BUILDING**

### Out of the Classroom

**SOCIALIZING**

**PARTICIPATION**

**NETWORKING**

# GRAPA CERTIFICATION

## Certified Analyst — Fraud Management (CA-FM)

GRAPA's intermediate level certification focuses on a practical, hands-on, standards-based approach to fraud management. For practitioners performing this function on a day to day basis, this is an essential program of training and credentialization. It provides fraud management team members with the framework and techniques, as well as the professional stature to be successful within their organizations – enabling and motivating them to effectively pursue revenue risk wherever it can be found.

Those who certify will not only have a firm and fundamental grasp of GRAPA's standards, as well as GRAPA's standard controls across all telco domains and lines of business, they will also be able to implement that understanding towards the effective containment of revenue risk. Achievement of this certification therefore presents a clear means of gaining professional status and confidence, allowing for accelerated professional development within your organization.

### Requirements for CA-FM Certification
Pre-requisites: None
Requirements:
- 40-50 hours clssroom participation
- 1 hour examination
- Verification of 6 months relevant work experience
- Pre-class preparation assignment  (Post-class follow up assignment)

## Certified Specialist (CS-xxx)

For the professional who is not interested in attaining the more broad-based Analyst, Expert, or Manager certification, GRAPA also offers a number of highly focused specialty certification programs.

These programs typically extend from 30-50 hours depending on the course, and allow the students access to regional public training events, on-site programs, and their own choice of online classes, to build a curriculum that allows them to cover a narrowly defined area in depth.

The certifications can be customized to the needs of the student or organization.

Programs offered include Certified Specialists in different lines of business and technology areas, specific fraud management practices and tools, and specific types of fraud.

### Requirements for CS-xxx Certification
Pre-requisites: none
Requirements:
- 30-50 hours of classroom participation
- 2 hour online exam (multiple choice and essay)
- Optional practicum (self-study – workplace or self-directed – research)

your photo here

*The GRAPA Certification program includes Training, Testing and Experience Verification.*

# Day 1- Voice, Data & Cyber Fraud - Overview

## Unit 1: Converged Fraud & Cyber Crime Standard Practices
### *Leveraging the best of both worlds*

**Unit Overview:**
This unit provides the student with a comprehensive overview of Telecommunications Fraud Management and Cyber Crime Prevention as unique disciplines that can be integrated into a synergistic approach that yields higher value to the organization. While most industries have a fraud management function and are vulnerable to cyber crime, the complex Information, Communications and Technology 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:  Incident Management Lifecycle, Situational Profiling, Fraudster Profiling, Behavior Profiling, Juristictional analysis and others methods are applied to the modern converged fraud landscape.

**Unit Learning Objectives** Students who have the following specific training objectives should participate in this unit

• I want a consistent approach to finding and preventing frauds for voice, data and internet scenarieos

• I want to perform fraud forensics in line with industry standard methods

• I want to improve my fraudster profiling techniques

• I want to better explain to management what it means to be a fraud professional and get more appreciation for the job I am doing

• I want to develop the skill set I need to be more successful at detecting and preventing frauds

## Unit 2: Fraud Management Systems & Criminal Forensic Systems
### *Maximizing your efforts with Best Practices in Forensics*

**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.

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.

**Unit Learning Objectives:**

 Students who have the following specific training objectives should participate in this unit:

• I want to learn about how to optimize my forensic capabilities with the latest tools and techniques in data analystics

• I want to optimize my current fraud management system and set more alarms to find more frauds

• I want to know what to look for/requirements for a new FMS

• I want to utilize a data warehouse to generate alarms that my FMS cannot do

# Day 2 - Voice Networks: Frauds and Phreaks

## Unit 3: Security Fundamentals for   Voice Networks
*(Pssst....You Cannot Secure Your Telco Without This Information)*

**Unit Overview:**
Get an overview of the OSS/Network environment specifically designed to meet the needs of fraud and cyber crime specialists. Students will learn to deal with the technical environment from a security perspective, focusing on Authentication, Authorization and Accounting - specifically the production of transaction records and CDRs, as well as guarding against exposures in the physical and logical architectures

**Unit Learning Objectives:**
Students who have the following specific training objectives should participate in this unit

• I want to stop theft of service on my voice network

   • I want to stop fraudsters from taking advantage of my voice network

      • I want to improve my techniques for finding the vulnerabilities in my network

         • I want to understand how my organization's network can become a playground for fraudsters and how to improve security

## Unit 4: Protection Strategies -
## Core Network & Radio Side Frauds
*Traditional Telecom Hacks & Modern Wireless Fraud Protection*

**Unit Overview:**
Learn how fraudsters perform theft of service, denial of service, and averse accessory fraud.  See how they can manipulate internal reference data/databases and compromise junctions/gateways, tee-ins, and signal intercepts.  Learn about breaking GSM encryption, SS7 traffic spoofing, SIM clones, handset attacks.

**Unit Learning Objectives** Students who have the following specific training objectives should participate in this unit:

•  I want to prevent theft of service and adverse accessory fraud in my organizations

•  I want to understand how fraudsters can take advantage of my radio network and what controls I can put in place to prevent this activity

•  I want to understand the details of the most costly Radio-side frauds and become my organization's expert for methods of detection and deterrence

# Day 3 - Cyber-Tech - Foundations for Internet Fraud Protection

## Unit 5:  The Internet Ecosystem - From a security perspective
*IP Fundamentals for the Fraud Analyst*

**Unit Overview:**
This unit provides the student with an overview of the fundamental principles of operation, security and protection of IP based and cloud services. This unit is prerequisite to anyone attempting to understand and secure Internet Services, GPRS, UMTS, LTE, IMS, Cable, Satellite, IPTV, VPN or any of the services based upon the IP architecture. This unit provides students with a comprehensive understanding of the practical implementation of AAA (authentication, authorization and accounting) controls for all IP environments.

**Unit Learning Objectives** Students who have the following specific training objectives should participate in this unit:

• I want to understand enough about the new Internet-based technology that I can secure the IP network from major frauds

•  I want to know the new fraud exposures that come with migrating to an Internet business model

• I want to secure the Internet network environments

## Unit 6: Internet-based Cyber Crimes - Network Intrusion & Social Engineering
*Protecting Customers, Society and The Operator*

**Unit Overview:**
See how Fraudsters break into IP-based and cloud environments and how you can protect against it. Learn about phishing, zero day vulnerability attacks, VPN hacks, SQL Injection, Denial of Service Attacks, (Windows, Linux, website, e-mail, methods of incursion and fraud). See how fraudsters hack a PC, break a WiFi encryption, and learn what you need to protect against it.

**Unit Learning Objectives:**
Students who have the following specific training objectives should participate in this unit

•     I want to stop fraudsters and hackers from taking advantage of my IP network

•     I want to feel confident in the security I have built into my organization's  Internet environment

•     I want to improve my forensics techniques for finding the vulnerabilities in my IP-network

# Day 4 - Partner Frauds, FMS & Data Mining

## Unit 7: Interconnect Settlement, Simbox, Bypass & Injection Frauds
*Securing the Interconnect Environment*

**Unit Overview:**
In this unit we examining key operational, commercial and technical security concerns in the interconnect/long distance/international calling environment. We review how partners, internal fraudsters, and professional criminal gangs exploit the complexity of the technical and commercial environment to defraud the telco, potentially leading to large cash losses within very short windows of time. Even more frightening, thse often go undetected for months or years.

**Unit Learning Objectives** Students who have the following specific training objectives should participate in this unit

• I want to stop my organization from getting hit with a major Interconnect Fraud

   • I want to make sure my interconnect environment has the controls in place to protect against major fraud exploits

      • I want to be confident that my organization has strong fraud defenses against PBX and Trunk Group Frauds



## Unit 8: Roaming Frauds - IRSF, CAMEL & Credit Exploits
*Securing the Roaming Environment*

**Unit Overview:**

In this unit we tackle frauds in the roaming environment. Often extremely costly, these are some of the most complicated frauds in one of the most complex telecoms Lines of Business - especially those that have to do with the use of premium rate numbers or International Revenue Share Fraud (IRSF). Extensive focus on other roaming frauds involving partner mis-conduct and evolving frauds exploiting vulnerabilities in the prepaid CAMEL roaming architecture.



**Unit Learning Objectives** Students who have the following specific training objectives should participate in this unit

• I want to make sure I am not missing large roaming frauds that could occur in my organization

• I want to understand how fraudsters commit IRSF and premium rate fraud so I can build a strategy to defend against these exploits

• I want to know how to leverage logical security around my camel roaming environment standards to add an additional layer of security around my CAMEL roaming environment

# Day 5 - Cyber Security, Cloud & Subscription Frauds

## Unit 9: Cyber Security and Cloud Protection
### *Securing the Internet Environment*

**Unit Overview:**
Given the incredible rate of change that operators are building into their networks, the only real surprise is that the fraudsters have not yet gotten around to really exploiting the environment. At this time the majority of cybercrimes are focusing on individual consumers, and large corporate I/T environments. But it is only a matter of time before hackers and freaks begin to exploit the vulnerabilities that these complex new business models create. In this unit we focus on the cybercrime exposures inherent in the next generation business models operators are building

**Unit Learning Objectives:**
Students who have the following specific training objectives should participate in this unit

- Fraud vulnerabilities and issues for LTE/4G and Hybrid 3G/4G environments
- GPRS Hacks and data roaming fraud exposures
- Cloud security profiling the DSSA security modeling methodology and the building of carrier protection for cloud partnerships
- Mobile-To-Mobile risk profiles and what to do about them

## Unit 10: Assembling your Cyber Protection Team
### *Hope for the best ... Prepare for the worst !*

**Unit Overview:**
Building and effective Fraud and CyberCrime strategy requires 2 things.

- First - you have to figure out how the fraudsters are going to convert their exploits into money
- Second - You have to assign the best from each of your security , fraud and controls teams to and be sure each is covering their part of the risk

Learn how fraudsters exploit customer identities, trick point of sale staff, generate false traffic, run premium rate exploits, perform call sells, and more. Learn the controls needed at the Point of Sale, in Network, at Billing, and over Marketing for new rate plans to prevent these fraudulent activities. Also, learn to utilize a fraud management system and fraud data warehouse to detect these frauds early. Learn the credit management lifecycle and the critical role of the FMS in containing credit risk and preventing bad debt (including leased line frauds).

**Unit Learning Objectives** Students who have the following specific training objectives should participate in this unit

- I want better organize my security and fraud management efforts to protect against the new generation of cyber frauds
- I want to understand how to leverage existing fraud and security controls to protect my company assets, my delivery network, my products and services and my customers
- I want to reduce my liability and risk of cyber fraud attack

# Why We are the Leaders in Training Telco Professionals Around the Globe

Join the leading provider of fraud-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 three 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 professionals who participate in "practices surveys," "strategy sessions," and other information-sharing events. Clear, specific deliverables are provided that apply to real-world situations. The material is never based on speculation, guesses, or unvalidated information.

☑ **Interactive** – The workshops are more than lecture sessions. RAA classes are participative and interactive and students are expected to proactively 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.

☑ **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.
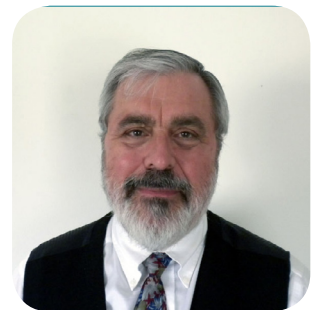
**Rob Mattison** is a world-renowned expert in telecommunications and the revenue assurance industry He has 20+ years of hands-on industry experience. He is President of GRAPA and author of *The Revenue Assurance Standards - 2009 Edition*, and of *The Telco Revenue Assurance Handbook*, which has become the authoritative guide for RA Managers at telecom firms around the world.

**Detecting and deterring fraud with proven techniques and strategies**

GRAPA

# About GRAPA

The Telco Fraud Academy is the exclusive fraud training organization of GRAPA. GRAPA has over 8000 registered members and has distributed more than 5000 copies of its 2009 standards book. The Data, Voice, and Cyber Faud Management curriculum is the Academy's latest offering, providing revolutionary and relevant material. By offering events that combine benchmark development, sharing of standard practices and approaches, as well as delivery of workshops, the Telco Fraud Academy provides a unique and powerful venue for deployment of standard practices and rapid integration of those practices into the participating telco environments.

We have conducted our training programs for dozens of carriers and services providers around the world. Our workshops are offered in public venues (attended by delegates from many operators and services providers, which promotes the sharing of practices), in live online sessions, as well as onsite for a private, more personalized and focused training for a company's staff.

All of our courses are based entirely on the GRAPA standards of professional practices and are focused heavily on practical experience, not theory.

Visit our website to read some great reviews from students who have attended our training:
http://telecom-fraud.org/telecom_fraud_academy_info/testimonials.html

Communications Industry Fraud Academy

"Being recognized and certified by a well-respected group like GRAPA is really something very inspiring to continue my endeavor and passion in the field of protecting telcos in revenue leaks and frauds. GRAPA training and certification is a MUST to ALL Revenue Assurance and Fraud Management Professionals working in the communications industry. This is, I think, the best organized body where professionals can acquire continuing learning in Revenue Assurance and Fraud Management."

Senior Specialist-Financial Audit, Philippines

Tel        +1- 847-930- 3610
Fax       +1- 707-276-7676
Email    info@grapatel.com