BECAUSE YOUR REPUTATION MATTERS

FORENSIC INVESTIGATIONS
DUE DILIGENCE
INFORMATION SECURITY
GDPR COMPLIANCE
SECURITY & RISK CONSULTING
BRAND PROTECTION
BACKGROUND CHECKS
TRAININGS & CERTIFICATIONS
OUR ASSOCIATIONS

OUR AWARDS

Business Protection Award
2019

Most Professional Consultant in Anti-counterfeiting Space
2019

Most Successful Company For Risk Consulting Services
2018

Fraud Investigator of The Year
2017

Outstanding contribution in the field of risk management, security & forensics
2016

Security Project Design of the Year
2015
FORENSIC INVESTIGATIONS

DO EVERYTHING THE RIGHT WAY

Due Diligence – may be for business partners, Senior hires, investors like by angel investors/venture capitalists/ institutional investors/ banks, etc who look for strategic investments, or who wish to acquire inorganic growth. The due diligence check is normally done to know the ethical behavior, financials, criminal background, court cases, media news, etc done through desktop searches through paid websites and publicly available information. In addition, site checks are carried out through market intelligence teams. Netrika Consulting India Pvt Ltd has experts who help customers in this domain with their expertise.

KNOW IT BEFORE YOU GET INTO IT

Having whistle blowers’ line for the employees and the business partners is very important for providing a channel to report unethical practices. In addition to the organizational culture it is very important to provide an avenue to the employees and the business partners for reporting. Netrika is well poised to manage this for the organizations independently and investigate these complaints. Typically, these complaints pertain to sexual harassment, conflict of interest cases, kickbacks, undue favoritism, etc.

EVIDENCE GATHERING

E-discovery is an important process of gathering the evidence may it be in support of investigations and disputes. Netrika has the requisite expertise for the same. We are in the process of setting up a lab for all forensic technology services including e-discovery.

REVIEW, LEARN, GROW

Proactively, companies constantly need to review and improve their policies and processes concerning security, ethics and compliance, sexual harassment, ABC, etc, in order to keep pace with the regulatory and market needs. These process reviews are done to assess the gaps which can be exploited by potential fraudsters to their advantage. Netrika’s team of multifunctional experts help carry out gap assessment while applying their knowledge gained through such work in the industry.

TRACING ASSETS

Banks, financial institutions, investors, venture capitalists need help in tracing assets when their investment/loans go bad and they need to find assets to recover their capital investments. It may be against individuals/companies. Netrika has the requisite expertise to assist assets tracing for clients either directly or through their legal advisors.

SKIP TRACING

Companies sometimes like to keep track of the promoters and key personnel of small brands who are providing strong competition in key markets. They could be a challenger to an established brand. A diverse team at Netrika works closely with CXO’s to keep close eye. As the market gets more competitive, several companies are demanding such services.

MYSTERY SHOPPING

Companies are often interested in testing if their processes are functional or not and often times, they need to report this requirement to the regulators as well. This can be done for retail sector, financial institutions, services/product companies. Netrika can assist clients in carrying out this very important function.

OUR OFFERINGS

<table>
<thead>
<tr>
<th>Proactive</th>
<th>Reactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Risk Management</td>
<td>Forensic Accounting and Corporate Fraud Investigation</td>
</tr>
<tr>
<td>Anti-bribery Health Check Ups</td>
<td>Anti-Bribery &amp; Corruption Investigations</td>
</tr>
<tr>
<td>Anti-Money Laundering Consulting</td>
<td>Forensic Technology Services</td>
</tr>
<tr>
<td>Business Intelligence Services</td>
<td>Forensic Data Analytics</td>
</tr>
<tr>
<td>Ethics and Compliance Review</td>
<td>Litigation Support</td>
</tr>
<tr>
<td></td>
<td>End Use Monitoring</td>
</tr>
</tbody>
</table>
WE HELP ORGANIZATIONS IN:

- Fraud Risk Assessment
- Forensic Accounting and Litigation Support
- Asset Tracing
- Mystery Shopping
- E-Discovery and Email Recovery
- Financial Frauds
  - NPA Frauds Investigations
  - Kisan Credit Card Frauds
  - Anti-Money Laundering (AML) / Know Your Customers (KYC)
- Fraud Investigations
- Anti-Bribery, Anti-Corruption and Regulatory Compliance Reviews
- Review of Policies, Processes and Procedures
- Training in ABC, Ethics & Compliance and Investigation
- Forensic Technology Services
- Due Diligence
  - Counter Party / Vendor Due Diligence
  - Integrity Due Diligence
  - Senior Management Due Diligence

OUR METHODOLOGY TO NAVIGATE THROUGH FORENSIC INVESTIGATIONS

01. E-discovery & email reviews
02. Review of policies, processes and procedures
03. Discussions with process owners
04. Transaction testing
05. Gathering of market intelligence
A. Through desktop searches
B. Site visits & neighborhood canvas
06. Subject interview
DUE DILIGENCE

OUR SERVICES
Counter Party Due Diligence (CDD)/ Vendor Due Diligence (VDD)

Integrity Due Diligence (IDD)  Senior Management Due Diligence (SMDD)

WHY IS IT CRITICAL TO MANAGE DUE DILIGENCE?

Regulatory
- Corruption and bribery
- Competition
- Sanctions
- Criminal cases

Fraud and Loss
- Grey market /piracy
- Conflicts of interest
- Collusion with employees
- Intellectual property Violations

Reputation
- Cultural risks
- Management risks
- Loss of trust and loyalty

OUR APPROACH & METHODOLOGY
COUNTER PARTY DUE DILIGENCE (CDD)

1. Identifying which risks really matter
2. Maintaining accurate and complete inventory of third parties
3. Selecting which third party to review
4. Limited Resources for Program
5. Inconsistent reporting on third party issues
6. Lack of internal skill set for effective program management
7. Gathering, integrating, analyzing, making use of third party data
8. Staying ahead of, & effectively complying with, changing regulatory requirements

Challenges of managing third party risks

Apply Netrika Consulting India Pvt Ltd’s intelligent framework for information collection and meaningful analysis & reporting

If gaps are identified, more information will be requested

Client → Provides questionnaire → Netrika Consulting India Pvt. Ltd → Conduct → Gap Analysis

if no gaps initiate due diligence

Client → Selects third party → Netrika Consulting India Pvt. Ltd → Conduct → Gap Analysis → Two levels of quality review

Due Diligence

Online Research
Involves conducting an intensive search on the third-party partner for any negative information in the public domain.

Market Intelligence
Conduct physical verification on the third party partner through site visits and market intelligence

Analysis
Analyse the qualitative and quantitative information on the third party partner to identify red flags.

Pre-Research
Research
Analysis and reporting
Summarise and finalise

General Report
SENIOR MANAGEMENT DUE DILIGENCE (SMDD)

Senior Management due diligence is the process of appraising a company's senior management about the new senior hires.

MANAGEMENT ASSESSMENT

While evaluating candidates for senior positions, management usually focuses on assessing the skills pertaining to leadership, people, targets, goals, etc.

IMPORTANCE OF SMDD

SMDD helps in assessing the senior hires of their abilities, skill sets, business acumen, drive, etc., before making a hiring decision.

- Identify the senior management person to be hired.
- Identify the people with whom he/she has served.
- Present the feedback along with ratings into report.
- Specially designed questionnaire-based feedback form.
- Speak with previous colleagues/reportees and obtain feedback.
- Obtain the ratings and feedback on scale to 0-5.

INTEGRITY DUE DILIGENCE (IDD)

In mergers and acquisitions/investments - Regulatory compliance and establishment and preservation of reputation is a primary concern for every organization. In the present era, investors like the PEs and the angel investors prefer to avoid getting embroiled in regulatory inquiries caused by illegal practices followed by a potential joint-venture partner.

IDD examines the target company's operations to identify issues that might pose major, unquantifiable financial or reputational risks to an acquirer. Examples of major focal points in this phase of the investigation include:

- The existence of any linkages with PEPs (Politically exposed persons) connections between the business and any of the directors
- Evaluation of the company and principals relating to bribery, corruption, money laundering, large-scale tax evasion, fraud or asset stripping, etc.
- Any alleged connections between the company and organized crime or terrorist groups/SDN (Specially designated nationals) or broader risk of exposure to such groups

WHY NETRIKA?

- Risk based framework
- Outstanding global network with international coverage
- Respected by regulators
- An experienced, multi-disciplinary team
- One stop solution for all your threat and risk mitigation requirements
- Industry leading standards and thought leader
- Tailored customized deliverables and technology-based solutions
- Efficient and timely delivery model

www.netrika.com    info@netrika.com    Toll free: 1800 121 300000, Board: +91 124 288 3000
Information Security

Data held on IT systems is valuable and critical to the business of every organization. We all rely on IT to store and process information, so it is essential that we maintain Information Security.

With every new application, newer vulnerabilities crop up, posing immense challenges to those who are mandated to protect the IT assets.

Netrika is CERT-In empaneled for providing Information Security Auditing Service

**CYBER ATTACK TRENDS**

Botnets events processed during 2017

(Source: CERT-In)

Type of breaches suffered by Corporates in 2017

(Source: Cyber Security Preparedness Survey Report, Netrika)
IS YOUR CORPORATE CYBER PREPARED?

Netrika gauged the increasing threat of cybercrime and conducted a detailed survey to understand awareness about cybercrime and security across the industries.

KEY FINDINGS

01

Majority of survey respondents have more than 25 people in IT teams but still it is noteworthy that 62% of participating companies have suffered a cyber-attack in the form of ransomware, phishing or malware attack.

02

The survey identified that most of the organization face challenges: to find qualified cyber security professional/vendors (27%), IT department loaded with other operational tasks (18%) and other challenges such as lack of funds (14%), senior management buying 11%) and emerging technologies (9%).

03

The survey captures the need for conducting self-examination or diagnosis to review the technology and processes to be prepared for any crisis situation. It also puts an emphasis on conducting a mock drill exercise to put ourselves in an imaginary crisis situation just to examine our response to handle the crisis.

04

The survey results demonstrated that 30% of the participant organizations does not have evidence of any systematic process with respect to IT security which is an area of concern.

(Source: Cyber Security Preparedness Survey Report, Netrika)

Download the survey Report at - https://www.netrika.in/survey/cyber-security-preparedness

OUR SERVICES

IT Security Audit (ISO 27001, ISO 20000)
- Process & Technology
  - IT internal Audit
  - Process and Technology Audit
  - Pre-Certification Assistance and certification advisory services

Cyber Security Implementation
- Cyber Security Products/Solution Selection
- Cyber Security product/Solution effectiveness review
- Cyber Security Solution Implementation
- SOC transformation

ISMS/BCMS Implementation & Certification

Web / Mobile Application Security

GDPR Project Management and Compliance

Vendor Risk Management

Information Security Awareness & Training

Vulnerability Assessment & Penetration Testing of
- Network Security
- Web Application Security Testing
- Database
- Security Products
- Wi-Fi Network Security
- Hardening of IT Infrastructure
- Mobile, Smart Phone Android, IOS etc

Cyber Security Framework, strategy and program Transformation

BCP Policy, Process and Plan along with Test Reports

Gap Assessment and Risk Assessment

Cyber Threat Assessment

WHY NETRIKA?

1. Get Secure
2. Get Sustainable
3. Elevate Your Security Posture
4. Drive Intelligence

www.netrika.com  info@netrika.com  Toll free: 1800 121 300000, Board: +91 124 288 3000
GDPR COMPLIANCE

A CUSTOMIZED PROACTIVE APPROACH.

WHAT IS GDPR?
The GDPR sets out the principles for data management and the right of the individuals, while also imposing fines that can be revenue-based. The General Data Protection Regulation covers all companies that deal with data of EU citizens, so it is a critical regulation for corporate compliance officers at banks, insurers, and other financial companies. It is a nuanced and complex regulation that impacts nearly all businesses.

The GDPR Challenge
- What Personal Data do you Process?
- What about Unstructured Data Sitting in PDF/word files, Images
- Can you pinpoint exactly How is it Processed?

Data Subject Rights (Doing it Correctly)
- Access
- Portability
- Prevent Marketing/Promotions
- Correction
- Deletion

HOW NETRIKA CAN HELP?
At Netrika, our team of experienced professionals is dedicated to helping our clients succeed, we start by helping them understand their GDPR compliance obligations, before creating and executing a remediation plan designed to minimize cost and disruption while meeting all requirements.

Key Activities
1. Our understanding of your requirement
2. Gap & Risk Assessment
3. Implement and Monitor
4. Process Design and Documentation

GDPR IMPLEMENTATION APPROACH

GAP ASSESSMENT
(We perform gap review against List of Compliance items)

POLICIES AND PROCEDURES
(Policies for Privacy Framework, Policies for Information Security Framework)

IMPLEMENTATION ASSISTANCE
(Data Inventory, DPIA, training answers to all your Questions)

COMPLIANCE AUDIT
(GDPR readiness Compliance Audit report that can be shared with the Client)

COMPLIANCE REQUIREMENT
Our main services are aligned to support the most common GDPR compliance requirements, including:
- GDPR Readiness
- Remediation and Implementation
- Outsourced / Virtual Data Protection Officer (DPO) Services (Articles 37-39)
- Incident Response

GDPR COMPLIANCE MODEL
43 GDPR Requirements
Netrika GDPR Checklist:
The European Union’s (EU) General Data Protection Regulation (GDPR) is far-reaching, with steep penalties for organizations that are not in compliance, ensure that your organization is taking proper precautions to protect your data.

1. Relevance & Responsibilities

2. Identify relevant business processes, systems and data sets likely to contain personal data.

3. Determine whether your company processes personal data belonging to EU “data subjects.”

4. Determine your responsibilities as a data “controller” or data “processor” - or in some cases, both.

SAMPLE LIST OF POLICIES
PROVIDED AS A PART OF GDPR CONSULTING

- Data Protection / Privacy Policy / GDPR policy
- Automated Processing and Profiling Policy
- Privacy by Design / Privacy by Default

- Third Party Vendors - Privacy Assessments
- Privacy Impact Assessment Guidelines
- Privacy Self-Assessment

- Data Inventory Procedures
- Cross Border Transfer Procedures
- Privacy Breach - Incident Response Plan

- Record Keeping Templates / Formats
- Important Privacy Notices
- Data Subject Access Rights Procedure

- Consent / Data request handling procedures
- All key forms, formats and templates to run the privacy program
- Important clauses in agreements, third party contracts.

www.netrika.com  info@netrika.com  Toll free: 1800 121 300000, Board: +91 124 288 3000
SECURITY AND RISK CONSULTING

We follow an Integrated Risk Management approach, providing value to businesses by accounting for enterprise-wide risks and empowering their decision-making at every level.

SECURITY ENGINEERING DESIGN

In the age of technology-based disruptions, businesses are operating in ‘VUCA’ (volatile, uncertain, complex, and ambiguous) environment, which makes a solid ground for organisations to holistically emphasize on their security setup (both physical and cyber security). It must be noted that “a poor physical security can even defeat the best in IT security controls and vice-versa”. Netrika follows an integrated risk management approach, and addresses risks across a variety of levels in an organisation, including strategy and tactics, covering both opportunities and threats.

SECURITY AUDITS

Security audits form an essential part of keeping tab of security preparedness and pay rich dividends in ensuring security when conducted on a regular basis. Physical security penetration testing forms an essential part of security audits. We have a team of professionals who undertake the security audits as well as physical security penetration testing. The security audit report gives a detailed breakdown of gaps and recommendations to plug the gaps.

EMBEDDED RESOURCES

It has always been the man behind the machine. Trained and experienced resources are always required for running the show. We provide embedded resources to meet the security requirements (other than security guards).
THREAT VULNERABILITY & RISK ASSESSMENT (TVRA)

TVRA forms the building block on which security solutions are based. We have a professional team that undertakes the TVRA following which we provide a detailed report highlighting the gaps and recommendations for mitigation of identified risks. The recommendations also include technology based solutions that may be deployed for risk mitigation.

Threat Vulnerability & Risk Assessment (TVRA)

Comm & Consultation

Asset Characterisation
Threat Assessment
Vulnerability Assessment
Risk Evaluation
Risk Treatment

Monitoring & Review

Threats / Risk Identification Frameworks (We follow ‘Outside to Inside’ approach)

EXTERNAL THREATS / RISKS: MACRO RISKS

INTERNAL THREATS / RISKS: MICRO RISKS

PESTEL ANALYSIS

P - Political
E - Economic
S - Social
T - Technological
E - Environmental
L - Legal

Crisis Management & Business Continuity Planning

Netrika helps its clients resolve crisis situations, that present a risk to the profitability and reputation of their business, safety of their personnel and security of their assets. We specialize in training, planning, response and recovery services for a wide range of crisis events to reduce the period of disruption.

How we can help:

- Crisis readiness assessment
- Crisis management planning
- Business continuity planning
- Post-crisis recovery services
- Crisis management plan capacity testing i.e simulation & training exercises

“BY FAILING TO PREPARE, YOU ARE PREPARING TO FAIL”

Technical Surveillance Counter Measures

TSCM | Debugging | Electronic Sweeping

Information is power! It is the life blood of any organization, business and Government. Post conduct of the TSCM we render a concise technical report of our findings, along with practical advice on how to further protect and defend your location from ‘eavesdropping’.

The TSCM services provided by NCIPPL cover following aspects:

- Analysis of Radio Frequency Transmission
- Detection of Telephone Bugs
- Detection of Infra-Red Transmission
- Passive Device Detection
- Acoustic Leakages

Executive Protection

Information Technology era has increased the risk of illicit surveillance, cyber-crimes, data breaches and thereby posing physical security risks to principal. Netrika Consulting India Pvt Ltd (NCIPPL) is specialised in providing close protection services to senior executives / HNIs of global corporations. We emphasize exclusively on providing professional security practitioners, who are trained to react to crisis situations and thus protect the interests of our clients at a wide range of commercial events, including sports events, corporate functions, conferences and AGMs.

Our Approach

- Risk Assessment
- Advance Operations
- Secured & Vetted Transport
- Contingency Planning

www.netrika.com  info@netrika.com  Toll free: 1800 121 300000,  Board: +91 124 288 3000
Intellectual Property is the exclusive right of a brand owner resulting from an original creative thought that has been translated into a copyright material or trademark. Hence, brand owners are the lawful owners of the copyright or trademark. However, there are some unscrupulous individuals who indulge in the manufacture and distribution of counterfeit products of well-known brands. The result of such illegal actions is the loss of sales, a tarnished brand image, and erosion of brand loyalty not to mention the ill effects of consumption by the consumer and the loss of revenue to the government.

Netrika is your ideal partner to be the eyes and ears of the brand across markets, offline and online. Our multidisciplinary experts regularly carry out reviews and scan the online marketplaces to keep a close eye on possible fake products.

From online surveillance to supply chain audits and real-time surveys on markets, brands will find Netrika as the ideal long-term partner to keep a close eye on all the markets. Companies, meanwhile, can focus on running the business and building the brands.

ANTI-PIRACY PROGRAM

- Comprehensive Protection Programs
- Anti-Counterfeiting / Anti-Piracy Programs
- Enforcement Actions
- Cyber Surveillance
- Online Investigations
- Site Take Downs
- Transshipment / Diversion
- Litigation Support
- Custom Trainings

HOW NETRIKA CAN HELP?

- We advise on designing and implementing strategies to prevent counterfeiting and piracy.
- We monitor the sale of your products on online platforms.
- We pinpoint the location of suspected counterfeits as well as backtrack the entire supply chain with the help of undercover operations and intelligence gathering/media screening.
- We engage your users by putting the power in their hands to report the fake products through Report Fake APP.

REPORT FAKE APP


WHEN IGNORING THE PROBLEM IS NO LONGER AN OPTION

WHY NETRIKA?

- Specialised online monitoring team
- Single point of contact
- Quick turnaround time on enforcement actions
- (In-house software) to reduce Cost
- Focus on manufacturing/warehouse/importers/printing units
- The system can also notify (DMCA notice) to the appropriate bodies
- Focus on conviction with backend team to follow cases regularly

Source: FICCI Report
Netrika’s reach and expertise help verify the background of professionals across industries. With regular verification, companies can eliminate part of the risk. Our expertise ensures rigorous processes for small as well as large companies. Banks and financial services, logistics, e-commerce, manufacturing, services and several other customer facing companies use our services.

TAILORED SOLUTIONS FOR YOUR BUSINESS NEEDS

BASIC CHECKS

- Employment History
- Address Verification
- Passport / Voter Card / Pan Validation
- Global Database Check
- Education Check
- Civil/Criminal Record
- Reference Check
- Gap Verification

ADVANCED CHECKS

- Biometric Checks
- Drug Testing
- Company Legitimacy Check
- Identity Verification
- Media Searches
- Form 16 Verification
HIRE THE BEST, WEED OUT THE REST.

Misleading/Incorrect/False Information Provided in the Resume

It has been estimated that resume fraud costs employers approximately $600 billion annually.

16% of executive resumes contain false academic claims and/or material omissions relating to educational experience.

White Collar Crime/Fraud Committed by Employees in the Workplace

Median losses caused by executive are 16 times those of their employees.

Employee theft is the cause of 30% of business failures.

DID YOU KNOW?

More than 75% of substance abusers are employed.

Up to 40% of industrial fatalities and 47% of industrial injuries can be linked to alcohol use and alcoholism.

Prevalence of Drug Abuse by Employees in the Workplace

Violence in the workplace accounts for 17 percent of all occupational fatalities, making it the second leading cause of job-related fatalities.

The most common effects of workplace violence incidents on employees include decreased morale, decreased sense of safety, decreased productivity, decreased trust among co-workers and increased stress and depression.

The Role of Workplace Violence in Disrupting the Functionality of an Organization

Why Do Corporates Need BGC?

- The average organization loses more than $9 per day per employee to fraud and abuse
- The average organization loses about 6% of its total annual revenue to fraud and abuse committed by its own employees
- Losses caused by key staff (manager, executive, supervisor, etc.) are four times those caused by employees

Risk of Not Conducting BGC

- Studies show that bad hires can cost up to 5 times their annual salary.
- 53% of all job applications contain some or other inaccurate information
- Drug and Alcohol Abusers are involved in approximately 20-25% of workplace accidents
- A Study of 2,410 cases of Occupational fraud reported a total loss of more than $6.3 billion and the median loss from a single case of occupational fraud was $150,000

Source: ACFE, SHRM, Work Safe, Business Week and Business Group Health

www.netrika.com  info@netrika.com  Toll free: 1800 121 300000,  Board: +91 124 288 3000
LEARNING & DEVELOPMENT

LEADERSHIP & LEARNING ARE INDISPENSABLE TO ONE ANOTHER

SECURITY CERTIFICATION TRAININGS

The certifications mentioned below provides an in-depth understanding into the strategic, operational and tactical security awareness and management.

- Certified Crime Prevention Specialist (CCPS)
- Certificate Corporate Security Management Specialist (CCSMS)
- Certified Anti-Terrorism Specialist (CATS)
- Certified Loss Prevention and Operations Specialist (CLPOS)
- Certified Asset and Personnel Security and Specialist (CAPSS)
- Certified Crisis and Risk Management Training
- First Responder Awareness Course (FRAC)

Aspects

- Fundamental Security Concepts: Do’s and Don’ts to raise the general awareness.
- Updates on Security Threats: Challenges and Trends.
- Security Best known Practices & Methods

Who All Should Attend?


ACFE (Association of Certified Fraud Examiners) Preparation Course

The ACFE is the world’s largest anti-fraud organization and premier provider of anti-fraud training and education. The Certified Fraud Examiner (CFE) credential denotes proven expertise in fraud prevention, detection and deterrence. CFEs around the world help protect the global economy by uncovering fraud and implementing processes to prevent fraud from occurring in the first place.

Get started preparing for the CFE Exam today, with live instructor-led event.

Aspects

- Structured Learning: Learn how to prepare for the CFE Exam
- Fast Track: Participate in an intense, 4-day preparation period
- Instructor-Led: Receive guidance from experienced instructors
- Interactive Sessions: Participate in open discussions on a variety of topics in fraud prevention
- Team Environment: Meet others preparing for the CFE Exam and practicing CFE instructors to help you organize study sessions, review materials, and provide you with tips and processes designed for the working professional’s busy schedule
- On-Site Testing: Take advantage of the option to test onsite. Go home knowing you’ve passed your CFE Exam.

Who All Should Attend?


SUPPLY CHAIN SECURITY TRAININGS

The Transported Asset Protection Association (TAPA) is a unique forum that unites global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. TAPA has developed Facility Security Requirements (FSR) and Truck Security Requirements (TSR) for the Supply Chain, which includes warehouse security, Air Cargo (TACSS) and Food & Drugs security (FDFSR).

- Facility Security Requirement (FSR)
- Trucking Security Requirement (TSR)

CIISC (Chartered International Institute Of Security & Crisis Management) is the first and only independent body representing security professionals. It has developed Certified Supply Chain Security Specialist (CSCSS) certification. It covers the essentials of Security Policies & Procedural Compliance which are the fundamental principles governing audits and assessments of supply chain facilities.

- Certified Supply Chain Security Specialist (CSCSS)
INVESTIGATION/INTERVIEWING TECHNIQUE

- PEACE Interviewing & Interrogation Technique by FIS (Forensic Interview Solution), Australia
  In this interactive workshop, Experts will largely focus on Types of Frauds, Detection and prevention through different investigation and interviewing Techniques. Twenty plus years of rigorous research has shown that employing the P.E.A.C.E. method dramatically increased the amount of facts gathered in interviews while simultaneously decreasing the possibility of false confessions.

- Investigative Interviewing Technique by CIISCM Singapore.
  Investigative interviewing is the last and most important step in the investigation process. It is a process of bridging gaps in the available evidence based on eliciting the facts as known to the target employee in order to help the authorities make a decision.

Aspects

- Corporate frauds in India - Trends and Threats Principles & legal aspects of investigative interview & statement recording
- Risk Mitigation, Contingencies and Counter Measures
- Proactive Investigation Techniques and Tools
- Statics on other corporate frauds
- Investigative interviewing techniques incorporating enhanced cognitive techniques to assist interviewees to recall more detailed & accurate information
- Principles & legal aspects of investigative interview & statement recording
- Behaviour Analysis and Detecting Deception; Question formulation & strategy; and Investigative Interviewing for suspects & accused persons.

INFORMATION SECURITY AWARENESS TRAINING

Majority of Information Security Breaches are caused not only by the insiders with malicious intent but also because of unintentional mistakes caused by unaware employees. We provide interactive classroom as well as web-based training program to improve the awareness of employees towards Information Security.

Aspects

- Fundamental information security concepts, Do’s and Don’ts to raise the general level of awareness
- News of significant information security breaches
- Relevant laws, regulations and best practice standards (e.g. ISO 27001, IT Act 2000)
- Information on Company Information Security Policy, Procedure, Standards and Guidelines

OTHER CORPORATE TRAININGS

For all your corporate training needs find below mentioned trainings
- Women Safety and Self Defense Training (WST)
- Prevention of Sexual harassment at workplace (POSH)
- Soft skill
- Behaviour based safety training
- Security Etiquettes Training
- Emergency and Evacuation Training.

Who All Should Attend?
All Employees

Who All Should Attend?

Who All Should Attend?

Who All Should Attend?
Company Employees, Vendors & Business Partners, IT / Non IT team.

www.netrika.com info@netrika.com Toll free: 1800 121 300000, Board: +91 124 288 3000