BROCHURE

SIVRIL

TRAINING INSTITUTE
AND CENTER FOR
DEVELOPMENT

TABLE OF CONTENTS

Table of Contents

3 About us

3 Our Vision

4 Crisis Management And Emergency Planning Course

6 Chief Security officer (CSO) Transition Program

9 Principles of Corporate and Homeland Security

12 COMMUNITY ENGAGEMENT FOR SECURITY PROFESSIONALS

Building Trust to Ensure Operational Continuity in Nigeria.

13 Security Management in Volatile Locations

Strategies for Risk Mitigation and Operational Continuity

SIVRIL

ABOUT US

About Us

SIVRIL is a world-class training institute offering globally relevant programs in security, forensics, crime Prevention, Business continuity, leadership, and Personal development.
SIVRIL provides world class practical based training that would create a significant impact for prospective students. We offer transformational trainings to address current professional
needs.

Our Vision

To raise a generation of ethical, skilled, and visionary professionals equipped to lead and solve Africa's most pressing Security, forensic, and leadership challenges.

SIVRIL

OUR SCHOOLS

1
SCHOOL OF SECURITY & INTELLIGENCE MANAGEMENT
2
SCHOOL OF FORENSICS & CRIME INVESTIGATION
3
LEADERSHIP & STRATEGY ACADEMY
4
PERSONAL & PROFESSIONAL DEVELOPMENT HUB

1. CRISIS MANAGEMENT AND EMERGENCY PLANNING COURSE

Category: Organizational Resilience | Emergency Management | Leadership

Duration: 3 Days (Modular / Executive Format Available)

Delivery: Classroom | Simulation-Based | Hybrid | In-Company

Certification: SIVRIL Professional Certificate in Crisis Management

CPE Alignment: ASIS Eligible

COURSE OBJECTIVE

To equip executives, security leaders, and operational managers with the skills to anticipate crises, develop effective emergency plans, lead under pressure, coordinate multi-agency response, protect lives and assets, preserve reputation, and restore operations quickly.

Participants learn how to move from reactive firefighting to structured, resilient crisis leadership.

TARGET AUDIENCE

- Chief Security Officers (CSOs)
- Executives and Senior Managers
- Business Continuity Managers
- Facility and Operations Managers
- Risk & Compliance Officers
- Emergency Response Coordinators
- NGO / Public Sector Leaders
- Law Enforcement transitioning to corporate security

LEARNING OUTCOMES

- Participants will be able to:
- Identify credible crisis scenarios
- Develop and validate emergency response plans
- Establish crisis management structures and roles
- Coordinate internal and external responders
- Make high-quality decisions under pressure
- Communicate effectively during crises
- Manage reputational, legal, and operational risk
- Lead recovery and business continuity

COURSE OUTLINE

1 UNDERSTANDING CRISIS & ORGANIZATIONAL RESILIENCE

- What defines a crisis vs incident
- Types of crises (security, safety, cyber, reputational, natural hazards)
- Organizational vulnerability analysis
- Cascading impacts
- Resilience vs response

2 EMERGENCY PLANNING FUNDAMENTALS

- Emergency risk assessment
- Emergency response plan structure
- Evacuation, shelter-in-place, lockdown
- Medical emergencies
- Fire and hazardous materials
- Utilities failure
- Natural disasters

3 CRISIS MANAGEMENT STRUCTURE & LEADERSHIP

- Incident Command System (ICS) principles
- Crisis Management Team roles
- Decision authority
- Escalation thresholds
- Legal and ethical considerations
- Documentation and accountability

4 CRISIS COMMUNICATION & STAKEHOLDER MANAGEMENT

- Internal communication protocols
- Media management
- Regulatory notifications
- Family liaison
- Social media risks
- Message consistency

5 BUSINESS CONTINUITY & OPERATIONAL RECOVERY

- Business impact analysis
- Critical function prioritization
- Alternate site planning
- IT recovery
- Supply chain continuity
- Workforce recovery

6 EXERCISES, DRILLS & CONTINUOUS IMPROVEMENT

- Tabletop vs functional vs full-scale exercises
- After-action reviews
- Corrective action tracking
- Performance metrics
- Audit readiness

7 EXECUTIVE DECISION-MAKING UNDER STRESS

- Cognitive bias in crisis
- Situational awareness
- Ethical dilemmas
- Resource prioritization
- Leadership presence

2. CHIEF SECURITY OFFICER (CSO) TRANSITION PROGRAM

From Law Enforcement Command to Industrial & Corporate Security Leadership

Format: Executive Classroom | Hybrid | In-Company

Duration: 5 Days (Modular)

Certification: SIVRIL Executive Certificate

CPE Alignment: ASIS Preferred Provider

COURSE OVERVIEW

The Certified CSO Transition Program is a high-impact executive training designed for security leaders transitioning from law enforcement, military, and public security roles into corporate, industrial, and private sector security leadership.

This program bridges the operational mindset gap between command-driven public security and governance-driven corporate security, equipping participants with the strategic, legal, financial, and leadership competencies required to operate at board and executive levels.

Participants gain practical mastery in enterprise risk management, compliance, industrial security systems, crisis leadership, investigations, cyber-physical convergence, and executive communication.

TARGET AUDIENCE

- Retired or transitioning law enforcement commanders
- Military officers moving into corporate security roles
- Government security executives entering private sector
- Newly appointed Chief Security Officers / Heads of Security
- Security directors managing large corporate portfolios

LEARNING OUTCOMES

- Participants will be able to:
- Shift from enforcement mindset to corporate governance leadership
- Design enterprise security strategies aligned with business objectives
- Conduct risk-based security planning and budgeting
- Navigate corporate legal, regulatory, and liability exposure
- Integrate physical, cyber, and operational security systems
- Lead crisis response and business continuity programs
- Deliver board-level reporting and executive briefings
- Manage vendors, contracts, and service-level accountability
- Build ethical, compliant, high-performance security teams

COURSE OUTLINE

1 FOUNDATIONS OF CORPORATE AND HOMELAND SECURITY

- Evolution of homeland security and corporate security
- National security architecture and critical infrastructure
- Role of private sector in national security
- Public vs private security mandates
- Security governance models
- Ethical responsibilities

2 THREAT LANDSCAPE AND RISK ENVIRONMENT

- Terrorism, insurgency, and violent extremism
- Organized crime and economic sabotage
- Cyber threats and insider risks
- Political instability and civil unrest
- Natural disasters and climate risk
- Supply chain disruptions

3 ENTERPRISE SECURITY RISK MANAGEMENT (ESRM)

- Risk identification and prioritization
- Vulnerability assessment techniques
- Asset criticality analysis
- Risk appetite and tolerance
- Risk mitigation strategies
- Cost-benefit analysis

4 LEGAL, REGULATORY AND POLICY FRAMEWORKS

- National security laws
- Private security regulations
- Data protection and privacy
- Human rights and use of force
- Evidence handling and reporting
- Compliance management

5 CRITICAL INFRASTRUCTURE PROTECTION

- Energy, telecoms, transport, finance, water
- Physical security architecture
- Access control and surveillance
- Perimeter security
- Redundancy and resilience
- Public-private coordination

6 INTELLIGENCE AND INFORMATION SHARING

- Intelligence cycle
- Open-source intelligence
- Threat reporting
- Information sharing protocols
- Fusion centers
- Confidentiality management

7 CRISIS MANAGEMENT AND EMERGENCY PREPAREDNESS

- Incident command systems
- Emergency response planning
- Evacuation and sheltering
- Media and reputation management
- Stakeholder coordination
- Business continuity integration

8 SECURITY LEADERSHIP AND GOVERNANCE

- Security strategy development
- Policy and SOP design
- Performance measurement
- Budgeting and procurement
- Vendor management
- Board reporting

VALUE TO PARTICIPANTS & ORGANIZATIONS

Strong security governance | Improved threat awareness | Better risk decision-making
Enhanced regulatory compliance | Improved crisis readiness | Stronger public-private coordination

3. PRINCIPLES OF CORPORATE & HOMELAND SECURITY

Category: Security Leadership | Risk Management | National Resilience

Delivery Mode: Classroom | Hybrid | Executive In-Company

Duration: 3 Days (or Modular)

Certification: SIVRIL Professional Certificate

CPE Alignment: ASIS (Eligible)

COURSE OVERVIEW

This course provides a comprehensive foundation in the principles, frameworks, and operational realities of corporate and homeland security. Participants will gain a strategic understanding of how public security systems interface with private sector security responsibilities, critical infrastructure protection, risk governance, threat management, and national resilience.

The program bridges the gap between government security mandates and corporate security governance, enabling participants to operate effectively within complex regulatory, operational, and threat environments.

TARGET AUDIENCE

- Chief Security Officers (CSOs)
- Executives and Senior Managers
- Business Continuity Managers
- Facility and Operations Managers
- Risk & Compliance Officers
- Emergency Response Coordinators
- NGO / Public Sector Leaders
- Law Enforcement transitioning to corporate security

LEARNING OUTCOMES

- Participants will be able to:
- Identify credible crisis scenarios
- Develop and validate emergency response plans
- Establish crisis management structures and roles
- Coordinate internal and external responders
- Make high-quality decisions under pressure
- Communicate effectively during crises
- Manage reputational, legal, and operational risk
- Lead recovery and business continuity

COURSE OUTLINE

1 LEADERSHIP TRANSITION & GOVERNANCE

- Public vs Corporate Security Mandates
- Accountability, Liability & Ethics
- Executive Decision Authority
- Security Governance Models

2 ENTERPRISE SECURITY RISK MANAGEMENT (ESRM)

- Threat, Vulnerability & Impact Analysis
- Risk Appetite & Business Alignment
- Asset Criticality Mapping
- Risk Treatment & ROI Justification

3 CORPORATE LEGAL, COMPLIANCE & REGULATORY FRAMEWORK

- Private Security Regulations
- Data Protection & Privacy
- Employment & Contractor Liability
- HSE Integration
- Evidence Handling & Reporting

4 INDUSTRIAL & CRITICAL INFRASTRUCTURE SECURITY

- Facility Design & Perimeter Security
- Access Control & Surveillance Systems
- Guard Force Optimization
- Supply Chain Security
- Oil & Gas / Telecom / Manufacturing Risks

5 CYBER–PHYSICAL CONVERGENCE

- Insider Threats
- OT/ICS Risk
- Incident Coordination with IT
- Digital Evidence Management

6 CRISIS MANAGEMENT & BUSINESS CONTINUITY

- Business Impact Analysis
- Emergency Response
- Executive Crisis Leadership
- Tabletop Simulations
- Reputation Protection

7 INTELLIGENCE, INVESTIGATIONS & CORPORATE MISCONDUCT

- Corporate Intelligence Cycle
- Fraud & Misconduct Investigations
- Surveillance Ethics
- Whistleblower Systems

8 BOARD ENGAGEMENT & EXECUTIVE COMMUNICATION

- Security KPIs & Dashboards
- Budgeting & Procurement
- Vendor Governance
- Board-Level Presentations

VALUE TO ORGANIZATIONS

Reduced liability exposure | Improved regulatory compliance | Stronger security governance
Better security ROI | Enhanced leadership maturity | Improved crisis readiness

4. COMMUNITY ENGAGEMENT FOR SECURITY PROFESSIONALS – BUILDING TRUST TO ENSURE OPERATIONAL CONTINUITY IN NIGERIA

Duration: 1 day

COURSE OBJECTIVE

Equip security professionals with the skills and strategies to engage effectively with local communities, build trust, prevent disruptions, and ensure operational continuity in Nigeria.

TARGET AUDIENCE

- Corporate security managers and officers
- Field security teams
- NGO and humanitarian security personnel
- Law enforcement liaisons
- Community liaison officers
- Risk managers and operations teams

LEARNING OUTCOMES

By the end of this training, participants will be able to:

1. Understand the socio-cultural, political, and economic factors affecting community relations in Nigeria.
2. Build positive engagement strategies with local communities and leaders.
3. Identify early warning signs of potential operational disruptions.
4. Develop communication and negotiation strategies for conflict prevention.
5. Integrate community engagement into operational security plans ethically and effectively.
6. Evaluate case studies and lessons learned from community-security interactions in Nigeria.

1 INTRODUCTION TO COMMUNITY ENGAGEMENT

- Definition and importance of community engagement in security operations
- Relationship between trust, cooperation, and operational continuity
- The Nigerian context: diversity, communal sensitivities, and socio-political factors

2 UNDERSTANDING LOCAL COMMUNITIES

- Identifying stakeholders: traditional leaders, youth groups, local associations, NGOs
- Mapping community power structures and influencers
- Cultural awareness and ethical considerations in engagement
- The impact of misinformation and rumors on operations

3 COMMUNICATION & ENGAGEMENT STRATEGIES

- Building rapport and trust through transparency and consistency
- Active listening and culturally sensitive communication
- Formal and informal engagement channels: town hall meetings, liaison officers, local partnerships
- Social media and digital engagement considerations

4 CONFLICT PREVENTION & EARLY WARNING

- Recognizing signs of potential disruptions: protests, strikes, or misinformation
- Reporting, escalation, and early intervention mechanisms
- Negotiation techniques and mediation strategies
- Integrating early warning systems into security operations

5 INTEGRATING COMMUNITY ENGAGEMENT INTO SECURITY OPERATIONS

- Developing a community engagement plan for operations
- Balancing security needs with community sensitivities
- Ethical considerations: human rights, cultural respect, and professional conduct
- Collaboration with authorities and NGOs for joint operational support

6 LESSONS LEARNED & CASE STUDIES

- Review of successful and failed community engagement initiatives in Nigeria
- Analysis of the impact of good engagement on operational continuity
- Discussion on adapting strategies for different regional and cultural contexts

5. SECURITY MANAGEMENT IN VOLATILE LOCATIONS – STRATEGIES FOR RISK MITIGATION AND OPERATIONAL CONTINUITY

Duration: 2 days

COURSE OBJECTIVE

Equip security professionals with the knowledge, strategies, and practical tools to operate safely and maintain operational continuity in volatile locations.

TARGET AUDIENCE

- Security managers and personnel operating in high-risk areas
- Corporate executives traveling to or operating in volatile regions
- NGO, humanitarian, and government field staff
- Risk managers and crisis response teams

LEARNING OUTCOMES

By the end of this training, participants will be able to:

1. Understand the nature of volatility in high-risk environments.
2. Conduct threat assessments and risk mapping tailored to volatile regions.
3. Implement proactive measures to prevent security incidents.
4. Plan for contingencies, including evacuation and crisis response.
5. Integrate operational continuity strategies with security planning.
6. Build and maintain relationships with local stakeholders and authorities for enhanced security.

1 UNDERSTANDING VOLATILITY & HIGH-RISK ENVIRONMENTS

- Definition and types of volatile locations: political unrest, social unrest, terrorism, crime-prone areas, natural disasters
- Key risk factors in high-risk environments
- The human, operational, and reputational impact of volatility
- Overview of volatile regions globally and in Africa.

2 THREAT ASSESSMENT & RISK MAPPING

- Conducting structured threat assessments
- Risk mapping: identifying hotspots, vulnerable assets, and critical operations
- Tools and frameworks for analyzing security threats
- Prioritizing risks for mitigation

3 PREVENTIVE SECURITY MEASURES

- Personal security protocols: situational awareness, travel security, and safe conduct
- Operational security measures: secure facilities, communication protocols, and access control
- Vehicle and transport security
- Technology for monitoring and threat detection

4 CONTINGENCY PLANNING & CRISIS MANAGEMENT

- Developing contingency plans: evacuation, shelter, and emergency response
- Crisis management team structure and roles
- Communication protocols during crises (internal and external)
- Coordination with authorities, local stakeholders, and security partners

5 OPERATIONAL CONTINUITY & RISK MITIGATION

- Ensuring mission-critical operations continue during volatile events
- Redundancy, alternative planning, and resource allocation
- Balancing operational goals with security requirements
- Post-event analysis and learning for continuous improvement

6 COMMUNITY & STAKEHOLDER ENGAGEMENT

- Importance of local relationships for operational safety
- Engaging local authorities, community leaders, and security partners
- Cultural awareness and sensitivity
- Managing perception and reducing friction with communities

6. PROTECTING BRANDS AND CONSUMERS – ANTI-COUNTERFEITING STRATEGIES FOR FMCG COMPANIES

Duration: 2 days

COURSE OBJECTIVE

Equip FMCG professionals with knowledge, tools, and practical strategies to prevent, detect, and respond to counterfeiting, protecting brand integrity, consumer safety, and revenue.

TARGET AUDIENCE

- FMCG brand managers and executives
- Supply chain and logistics managers
- Quality assurance and product safety teams
- Legal, compliance, and security personnel
- Anti-fraud and risk management professionals

LEARNING OUTCOMES

By the end of the training, participants will be able to:

1. Understand the scope, methods, and impact of counterfeiting in the FMCG sector.
2. Identify vulnerable points in the supply chain where counterfeiting occurs.
3. Apply technological and operational strategies for product authentication.
4. Develop monitoring, reporting, and enforcement procedures.
5. Educate and engage consumers to support anti-counterfeiting efforts.
6. Collaborate effectively with regulatory agencies and law enforcement.

COURSE OUTLINE

1 UNDERSTANDING COUNTERFEITING IN FMCG

- Definition, types, and methods of counterfeiting in FMCG
- Financial, legal, and reputational impact on brands
- Case studies of counterfeit FMCG incidents globally and in Nigeria/West Africa
- Emerging trends in counterfeiting

2 SUPPLY CHAIN VULNERABILITIES

- Identifying weak points in manufacturing, packaging, distribution, and retail
- Internal vs. external threats: employees, distributors, vendors
- Risk assessment frameworks for counterfeiting
- Importance of traceability and serialization

3 PRODUCT AUTHENTICATION & TECHNOLOGY SOLUTIONS

- Packaging solutions: holograms, QR codes, security inks
- Serialization and track-and-trace technologies
- Blockchain and digital authentication for FMCG
- Integrating technology into existing processes without disrupting operations

4 MONITORING, DETECTION & RESPONSE

- Market monitoring: retail, online marketplaces, and informal channels
- Reporting mechanisms for suspected counterfeits
- Legal action and collaboration with law enforcement
- Internal investigation procedures

5 CONSUMER ENGAGEMENT & AWARENESS

- Educating consumers on product authenticity
- Public awareness campaigns and communication strategies
- Leveraging social media and digital platforms to report counterfeit products
- Incentives and feedback loops for consumers

6 COLLABORATION & ENFORCEMENT

- Partnering with law enforcement, customs, and regulatory authorities
- Industry collaborations and information sharing
- Policy, compliance, and standard operating procedures for anti-counterfeiting
- Developing an internal anti-counterfeiting task force

7 DEVELOPING AN ANTI-COUNTERFEITING STRATEGY

- Integrating prevention, detection, and response into a single operational framework
- Metrics for measuring success (reduction of counterfeit incidents, revenue protection)
- Continuous improvement and audit of anti-counterfeiting measures

7. MITIGATING INSIDER THREATS – PROTECTING PEOPLE, DATA, AND OPERATIONS FROM INTERNAL RISKS

DURATION: 2 days

COURSE OBJECTIVE:

Enable participants to understand, detect, prevent, and respond to insider threats, protecting the organization's people, assets, and data.

TARGET AUDIENCE

- Security and risk managers
- HR and compliance officers
- IT and cybersecurity personnel
- Operations managers
- Executives responsible for safeguarding organizational assets

LEARNING OUTCOMES

By the end of the training, participants will be able to:

1. Define and categorize insider threats: malicious, negligent, or inadvertent.
2. Recognize behavioral, technical, and operational indicators of insider risk.
3. Apply policies, procedures, and controls to mitigate insider threats.
4. Integrate cybersecurity, physical security, and HR measures for holistic risk management.
5. Develop incident response strategies for insider threat scenarios.
6. Learn from case studies and implement best practices in their organizations.

COURSE OUTLINE

1 INTRODUCTION TO INSIDER THREATS

- Definition and scope of insider threats
- Types of insiders: malicious, negligent, accidental
- Motivations behind insider actions: financial, revenge, ideological, opportunistic
- Impact on operations, reputation, and finances

2 INDICATORS & RISK DETECTION

- Behavioral red flags: unexplained changes in work patterns, data access anomalies, disgruntlement
- Technical indicators: unusual system access, data transfers, bypassing security controls
- Organizational and environmental risk factors
- Early warning and monitoring techniques

3 POLICIES, PROCEDURES & PREVENTIVE MEASURES

- Background checks, screening, and vetting procedures
- Access controls: need-to-know, role-based access, and separation of duties
- Security policies: acceptable use, confidentiality, and whistleblower protocols
- Awareness programs and training for staff

4 CYBERSECURITY & PHYSICAL SECURITY INTEGRATION

- IT monitoring and anomaly detection
- Data protection measures and secure document handling
- Physical security: secure facilities, visitor control, and surveillance
- Combining human and technological controls for layered security

5 INCIDENT RESPONSE & INVESTIGATION

- Steps for detecting, reporting, and investigating insider incidents
- Evidence collection, chain of custody, and legal considerations
- Coordinating between HR, security, legal, and IT
- Communication and post-incident actions

6 CASE STUDIES & LESSONS LEARNED

- Review of real-world insider threat incidents
- Analysis of failures and successes in mitigation
- Identifying actionable lessons for participants' organizations

8. NATIONAL AND ORGANIZATIONAL SECURITY POLICIES

BUILDING POLICY FRAMEWORKS THAT PROTECT NATIONS, INSTITUTIONS & ASSETS

CATEGORY: Governance | Risk | Compliance | Security Leadership
DURATION: 3 Days (or Modular)
DELIVERY: Classroom | Executive | Hybrid
CERTIFICATION: SIVRIL Professional Certificate
CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

This course equips security leaders, policymakers, compliance officers, and CSOs with the knowledge and practical skills to understand, interpret, develop, implement, and evaluate national and organizational security policies.

Participants learn how policy translates into operational control, regulatory compliance, accountability, and institutional resilience.

TARGET AUDIENCE

- Chief Security Officers
- Corporate Risk & Compliance Leaders
- Government Security Officials
- Policy Analysts
- NGO Security Managers
- Law Enforcement Leaders transitioning into private sector
- Critical Infrastructure Operators

LEARNING OUTCOMES

Participants will:

- Understand the architecture of national security policy systems
- Interpret policy implications for organizations
- Draft and implement security policies and SOPs
- Align security policies with laws and regulations
- Establish governance and accountability mechanisms
- Monitor compliance and policy effectiveness
- Manage policy change and institutional adoption

COURSE OUTLINE

1 UNDERSTANDING SECURITY POLICY ARCHITECTURE

- National Security Policy hierarchy
- Homeland security doctrine
- Regulatory agencies and mandates
- Public-private policy interface
- Policy lifecycle

2 LEGAL AND REGULATORY FOUNDATIONS

- Constitution and security legislation
- Private security regulation
- Data protection laws
- Human rights and use of force
- Evidence governance
- Regulatory enforcement mechanisms.

3 ORGANIZATIONAL SECURITY POLICY DEVELOPMENT

- Policy structure and components
- Policy language and clarity
- Scope definition
- Authority and enforcement
- Version control and approval
- Documentation standards

4 TRANSLATING POLICY INTO OPERATIONS

- SOP development
- Training and awareness
- Performance indicators
- Audit mechanisms
- Incident reporting
- Continuous improvement

5 POLICY GOVERNANCE AND OVERSIGHT

- Policy committees
- Risk ownership
- Compliance monitoring
- Audit trails
- Board oversight
- Regulatory reporting

6 MANAGING POLICY CHANGE AND CRISIS ADAPTATION

- Policy review cycles
- Incident-driven updates
- Technology impact
- Stakeholder engagement
- Communication strategies

7 ETHICS, HUMAN RIGHTS AND SAFEGUARDING

- Use of force governance
- Data privacy
- Survivor protection
- Whistleblower protection
- Anti-corruption controls

9. SECURITY OPERATIONS & CPTED: DESIGNING, OPERATING AND PROTECTING SECURE ENVIRONMENTS

CATEGORY: Physical Security | Facility Protection | Environmental Design
DURATION: 3Days (Modular / Executive Format Available)
DELIVERY: Classroom | Site-Based Practicals | Hybrid
CERTIFICATION: SIVRIL Professional Certificate
CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

To equip security professionals, facility leaders, and infrastructure managers with the ability to design, operate, and manage secure environments using operational security principles and CPTED methodologies to reduce crime, improve safety, enhance usability, and strengthen resilience.

Participants learn how to integrate people, process, technology, and environment into a cohesive protection strategy.

TARGET AUDIENCE

- Chief Security Officers
- Facility & Property Managers
- Industrial Security Managers
- Project Managers
- Architects & Engineers
- Urban Planners
- Government Infrastructure Managers
- Real Estate Developers
- Law Enforcement transitioning to private sector

LEARNING OUTCOMES

Participants will:

- Design secure facilities using CPTED principles
- Conduct security surveys and vulnerability assessments
- Optimize access control and perimeter protection
- Integrate lighting, landscaping, and visibility controls
- Manage guard force and patrol operations
- Implement technology effectively
- Balance security with usability and aesthetics
- Reduce operational risk and incident rates

COURSE OUTLINE

1 FOUNDATIONS OF SECURITY OPERATIONS

Topics

- Physical security fundamentals
- Threat environment analysis
- Asset protection principles
- Risk-based security planning
- Security governance and compliance
- KPIs and performance management

2 PRINCIPLES OF CPTED

- Natural surveillance
- Natural access control
- Territorial reinforcement
- Maintenance and image management
- Activity support
- 2nd and 3rd generation CPTED
- Cultural and urban considerations

3 SITE ASSESSMENT & VULNERABILITY ANALYSIS

- Security surveys
- CPTED audits
- Crime pattern analysis
- Lighting assessment
- Sightline mapping
- Environmental risk mapping

4 ACCESS CONTROL, PERIMETER & FLOW MANAGEMENT

- Gates, fencing, barriers
- Visitor management
- Vehicle screening
- Pedestrian flow
- Emergency egress
- Crowd management

5 SECURITY OPERATIONS MANAGEMENT

- Guard force deployment
- Patrol strategies
- Post orders
- Incident reporting
- Command and control
- Shift management

6 SECURITY TECHNOLOGY INTEGRATION

- CCTV systems
- Access control systems
- Intrusion detection
- Lighting systems
- Analytics and AI
- Control rooms

7 HUMAN BEHAVIOR, DESIGN & RISK REDUCTION

- Behavioral patterns
- Crime displacement
- Public psychology
- Inclusivity and safety
- Gender-sensitive design

8 TESTING, AUDITING & CONTINUOUS IMPROVEMENT

- Penetration testing
- CPTED audits
- Incident trend analysis
- Maintenance programs
- Continuous improvement

10. SECURITY MANAGEMENT & OPERATIONS

CATEGORY: Security Leadership | Operations | Governance
DURATION: 5 Days (Modular / Executive Format Available)
DELIVERY: Classroom | Simulation | Hybrid | In-Company
CERTIFICATION: SIVRIL Professional Certificate in Security Management & Operations
CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

To develop competent security leaders who can design, manage, govern, and continuously improve integrated security operations that protect people, assets, reputation, and business continuity.

Participants transition from operational execution to strategic management.

TARGET AUDIENCE

- Chief Security Officers (CSOs)
- Security Managers & Supervisors
- Law Enforcement transitioning to corporate security
- Risk & Compliance Managers
- Facility Managers
- Operations Managers
- NGO Security Coordinators
- Government Security Leaders

LEARNING OUTCOMES

Participants will be able to:

- Build enterprise security strategies
- Manage security operations professionally
- Lead people and vendors
- Control budgets and resources
- Measure performance
- Manage risk and compliance
- Respond to incidents and crises
- Communicate with executives

COURSE OUTLINE

1 FOUNDATIONS OF SECURITY MANAGEMENT

- Role of modern security leadership
- Enterprise Security Risk Management (ESRM)
- Governance frameworks
- Legal and regulatory compliance
- Ethics and accountability

2 RISK ASSESSMENT & SECURITY PLANNING

- Threat, vulnerability and risk assessment
- Asset criticality analysis
- Risk appetite
- Security master planning
- Program maturity models

3 SECURITY OPERATIONS MANAGEMENT

- Guard force management
- SOP development
- Patrol strategies
- Command centers
- Incident management
- Technology integration

4 PHYSICAL SECURITY & INFRASTRUCTURE PROTECTION

- Perimeter security
- Access control
- CCTV systems
- CPTED principles
- Facility hardening

5 INFORMATION, CYBER & CONVERGED SECURITY

- Cyber-physical convergence
- Data protection
- Insider threats
- Access governance
- Digital investigations

6 PERFORMANCE MANAGEMENT & QUALITY ASSURANCE

- KPIs
- Audits and inspections
- Continuous improvement
- Compliance reporting
- Benchmarking

7 BUDGETING, PROCUREMENT & VENDOR MANAGEMENT

- Budget development
- Cost-benefit analysis
- Contract management
- SLA governance
- Fraud prevention

8 INCIDENT & CRISIS MANAGEMENT

- Emergency planning
- Crisis leadership
- Business continuity
- Investigations
- Post-incident review

9 LEADERSHIP, COMMUNICATION & STAKEHOLDER MANAGEMENT

- Executive reporting
- Influence skills
- Change management
- Ethics
- Cultural intelligence

11. INTELLIGENCE GATHERING & RISK ANALYSIS

CATEGORY: Intelligence | Risk Management | Decision Support
DURATION: 2–3 Days (Modular / Executive Format Available)
DELIVERY: Classroom | Practical Labs | Simulation | Hybrid
CERTIFICATION: SIVRIL Professional Certificate Course
CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

To equip security professionals with the skills to collect, analyze, interpret, and convert intelligence into actionable risk decisions that protect people, assets, and business operations.

Participants learn how to move from information overload to structured intelligence-led security management.

TARGET AUDIENCE

- Chief Security Officers
- Intelligence & Security Analysts
- Corporate Security Managers
- Risk & Compliance Officers
- Investigations Teams
- Law Enforcement transitioning to private sector
- NGO Security Managers
- Government Security Officers

LEARNING OUTCOMES

Participants will be able to:

- Identify intelligence requirements
- Collect information legally and ethically
- Evaluate source reliability and data credibility
- Analyze threats, vulnerabilities and impacts
- Develop risk intelligence products
- Forecast emerging risks
- Support executive decision-making
- Integrate intelligence into operation

COURSE OUTLINE

1 FOUNDATIONS OF INTELLIGENCE IN SECURITY

- Intelligence cycle
- Tactical vs operational vs strategic intelligence
- Intelligence ethics and legality
- Corporate intelligence vs law enforcement intelligence
- Information security

2 INTELLIGENCE COLLECTION TECHNIQUES

- Open-source intelligence (OSINT)
- Human intelligence (HUMINT)
- Internal reporting systems
- Liaison networks
- Digital monitoring
- Surveillance principles
- Ethical boundaries

3 INFORMATION EVALUATION & VALIDATION

- Source grading
- Bias identification
- Data triangulation
- Deception detection
- Information quality control
- Chain of custody

4 RISK ANALYSIS & THREAT ASSESSMENT

- Threat intent, capability and opportunity
- Vulnerability assessment
- Consequence analysis
- Risk scoring
- Bow-tie analysis
- Scenario modelling

5 INTELLIGENCE PRODUCTS & REPORTING

- Intelligence briefs
- Threat bulletins
- Executive dashboards
- Visualization
- Writing for decision-makers
- Confidentiality controls

6 PREDICTIVE ANALYSIS & EARLY WARNING

- Trend analysis
- Indicators and warnings
- Horizon scanning
- Geopolitical risk
- Insider threat detection
- Business impact forecasting

7 INTELLIGENCE INTEGRATION INTO OPERATIONS

- Patrol deployment
- Resource prioritization
- Budget justification
- Crisis readiness
- Executive governance

12. EMERGENCY PREPAREDNESS – PLANNING, RESPONDING, AND ENSURING SAFETY

CATEGORY: Intelligence | Risk Management | Decision Support

DURATION: 2 Days (Modular / Executive Format Available)

DELIVERY: Classroom | Practical Labs | Simulation | Hybrid

CERTIFICATION: SIVRIL Professional Certificate Course

CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

Enable participants to understand potential emergencies, prepare proactively, respond effectively, and recover safely, ensuring organizational and personal resilience.

TARGET AUDIENCE

- Security personnel and managers
- Facility managers and operations teams
- Corporate staff and executives

- Crisis management teams
- Health, safety, and emergency response coordinators

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

- Identify types of emergencies and potential threats.
- Develop preparedness plans and procedures for their organization or team.
- Understand roles and responsibilities during an emergency.
- Execute effective emergency response and evacuation procedures.
- Communicate efficiently and coordinate with internal teams, authorities, and stakeholders.
- Conduct post-emergency review and continuous improvement.

COURSE OUTLINE

1 INTRODUCTION TO EMERGENCY PREPAREDNESS

- Definition and importance of emergency preparedness
- Types of emergencies: natural disasters, human-made incidents, technical failures
- The consequences of unpreparedness on people, operations, and reputation
- Overview of emergency preparedness cycle: plan, respond, recover, improve

2 RISK ASSESSMENT & THREAT ANALYSIS

- Identifying hazards and vulnerabilities in workplaces and operational environments
- Probability vs. impact analysis
- Prioritizing emergency risks
- Mapping high-risk areas and critical assets

3 EMERGENCY PLANNING & PREPAREDNESS

- Developing emergency response plans and procedures
- Roles and responsibilities of staff during emergencies
- Resource planning: first aid, emergency kits, communication systems
- Coordination with external stakeholders: fire services, medical teams, law enforcement

4 RESPONSE & EVACUATION PROCEDURES

- Emergency alert and notification systems
- Evacuation procedures and assembly points
- Crowd management and safe exit strategies
- First response actions: fire, medical, or security emergencies

5 COMMUNICATION & COORDINATION DURING EMERGENCIES

- Internal communication channels
- External communication with authorities and media
- Incident reporting and documentation
- Crisis management team coordination

6 POST-EMERGENCY REVIEW & CONTINUOUS IMPROVEMENT

- Debriefing and lessons learned
- Evaluating response effectiveness
- Updating emergency plans and procedures
- Training and continuous awareness programs

13. BUSINESS CONTINUITY & CONTINGENCY MANAGEMENT FOR SECURITY PROFESSIONALS

CATEGORY: Intelligence | Risk Management | Decision Support

DURATION: 2 Days (Modular / Executive Format Available)

DELIVERY: Classroom | Practical Labs | Simulation | Hybrid

CERTIFICATION: SIVRIL Professional Certificate Course

CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

Enable security professionals to plan, implement, and maintain business continuity and contingency strategies that protect people, assets, and operations during disruptions.

TARGET AUDIENCE

- Security managers and officers
- Risk and compliance managers
- Operations managers and continuity planners
- Crisis management teams
- Facility and corporate security personnel

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

- Understand the principles of business continuity and contingency management.
- Identify risks and threats that could disrupt operations.
- Develop and implement business continuity plans (BCPs) and contingency measures.
- Conduct impact assessments and prioritize critical functions.
- Coordinate emergency response and recovery efforts effectively.
- Test, evaluate, and improve continuity and contingency plans.

COURSE OUTLINE

1 INTRODUCTION TO EMERGENCY PREPAREDNESS

- Definition and importance of emergency preparedness
- Types of emergencies: natural disasters, human-made incidents, technical failures
- The consequences of unpreparedness on people, operations, and reputation
- Overview of emergency preparedness cycle: plan, respond, recover, improve

2 RISK ASSESSMENT & THREAT ANALYSIS

- Identifying hazards and vulnerabilities in workplaces and operational environments
- Probability vs. impact analysis
- Prioritizing emergency risks
- Mapping high-risk areas and critical assets

3 DEVELOPING BUSINESS CONTINUITY PLANS

- Components of an effective BCP: policies, procedures, roles, and responsibilities
- Contingency strategies for security, operations, IT, and communications
- Redundancy and alternative arrangements for critical functions
- Integration with existing security and operational procedures

4 EMERGENCY RESPONSE & CRISIS MANAGEMENT

- Response protocols for different types of crises
- Security team roles during emergencies
- Coordination with internal departments, authorities, and stakeholders
- Communication strategies during disruption

5 RECOVERY & RESUMPTION STRATEGIES

- Restoring operations after an incident
- Post-incident evaluation and corrective measures
- Lessons learned and continuous improvement
- Documentation and reporting for future reference

6 TESTING, TRAINING & CONTINUOUS IMPROVEMENT

- Conducting drills, simulations, and exercises
- Staff training and awareness programs
- Updating plans based on feedback, incidents, and evolving threats
- Benchmarking and best practices

14. UPSCALING A SECURITY TEAM – BUILDING CAPABILITY, CAPACITY, AND EFFECTIVENESS

CATEGORY: Intelligence | Risk Management | Decision Support

DURATION: 2 Days (Modular / Executive Format Available)

DELIVERY: Classroom | Practical Labs | Simulation | Hybrid

CERTIFICATION: SIVRIL Professional Certificate Course

CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

Enable organizations to strategically grow their security teams by developing capability, improving efficiency, and integrating best practices in recruitment, training, and operational management..

TARGET AUDIENCE

- Security managers and directors
- Operations managers
- HR and recruitment personnel for security roles
- Risk and compliance officers
- Team leaders in corporate, government, or private security sectors

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

- Assess the current structure, capacity, and capability of their security team.
- Identify operational gaps and requirements for upscaling.
- Develop recruitment, training, and retention strategies for security personnel.
- Implement standard operating procedures and performance management systems.
- Integrate technology, analytics, and tools to support a larger team.
- Maintain operational efficiency and resilience during expansion.

COURSE OUTLINE

1 ASSESSING CURRENT SECURITY TEAM CAPABILITIES

- Reviewing current roles, responsibilities, and competencies
- Identifying gaps in skill, coverage, and leadership
- Analyzing operational performance and incident response capabilities

2 STRATEGIC PLANNING FOR UPSCALING

- Defining objectives for team expansion: risk mitigation, operational needs, coverage
- Resource planning: human, financial, and technological
- Aligning team growth with organizational goals
- Risk-based approach to scaling security operations

3 RECRUITMENT & TALENT DEVELOPMENT

- Identifying required skills, qualifications, and certifications
- Recruitment strategies: sourcing, vetting, and selection
- Onboarding and induction programs for security staff
- Continuous professional development and career progression

4 STANDARD OPERATING PROCEDURES & PERFORMANCE MANAGEMENT

- Developing SOPs for daily operations, incident response, and reporting
- Key performance indicators and metrics for security teams
- Accountability and reporting structures
- Monitoring and evaluating team effectiveness.

5 TECHNOLOGY & TOOLS TO SUPPORT EXPANSION

- Leveraging security technology for surveillance, access control, and communication
- Integrating analytics for threat monitoring and performance tracking
- Automating routine processes to free resources for strategic tasks

6 LEADERSHIP, TEAM COHESION & CULTURE

- Building a cohesive, motivated, and resilient security team
- Leadership styles for large teams
- Conflict resolution, mentorship, and team engagement
- Promoting a culture of accountability and excellence

15. CYBERSECURITY & THREAT MITIGATION

CATEGORY: Cyber Risk | Converged Security | Digital Resilience
DURATION: 2–3 Days (Modular / Executive Format Available)
DELIVERY: Classroom | Labs | Simulation | Hybrid
CERTIFICATION: SIVRIL Professional Certificate Course
CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

To equip security leaders and operational managers with the skills to understand cyber threats, assess digital risk, implement effective mitigation controls, manage cyber incidents, and integrate cybersecurity into enterprise security governance.

Participants gain practical decision-making capability, not just technical theory.

TARGET AUDIENCE

- Chief Security Officers
- Security Managers
- IT Managers
- Risk & Compliance Officers
- Operations Managers
- Investigations Teams
- Law Enforcement transitioning to corporate roles
- NGO Security Managers

LEARNING OUTCOMES

Participants will be able to:

- Understand the cyber threat landscape
- Identify digital vulnerabilities
- Assess cyber risk
- Implement layered cyber controls
- Respond to cyber incidents
- Protect sensitive data
- Manage vendors and third parties
- Report cyber risk to leadership

COURSE OUTLINE

1 CYBER THREAT LANDSCAPE

- Types of cyber threats
- Attack vectors
- Threat actors
- Emerging risks
- Cybercrime economics
- Regional threat trends

2 DIGITAL ASSETS & VULNERABILITY IDENTIFICATION

- Asset inventory
- Network basics
- Cloud risks
- Mobile device risks
- OT and IoT exposure
- Insider threats

3 CYBER RISK ASSESSMENT

- Threat modeling
- Vulnerability scanning concepts
- Likelihood and impact analysis
- Data classification
- Risk acceptance

4 CYBERSECURITY CONTROLS & MITIGATION

- Access control
- Endpoint security
- Network segmentation
- Encryption
- Backup strategies
- Security awareness
- Vendor controls

5 CYBER INCIDENT RESPONSE & RECOVERY

- Incident response lifecycle
- Breach containment
- Forensics basics
- Legal obligations
- Communications
- Business continuity

6 GOVERNANCE, COMPLIANCE & ETHICS

- ISO 27001
- Data protection laws
- Privacy principles
- Cyber policies
- Audit readiness
- Reporting

7 CYBER-PHYSICAL CONVERGENCE

- CCTV network security
- Access control cyber risks
- Smart building vulnerabilities
- SCADA risks
- Integrated command centres

16. BUILDING ORGANIZATIONAL RESPECT FOR SECURITY DEPARTMENTS – INFLUENCE, CREDIBILITY AND LEADERSHIP

DURATION: 2 days

COURSE OBJECTIVES

Enable security departments to establish credibility, gain trust, and earn respect across the organization, positioning security as a strategic partner rather than just a rule enforcer.

TARGET AUDIENCE

- Security managers and teams
- Risk and compliance officers
- Facility and operations managers

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

- Understand why some security teams struggle to gain respect.
- Communicate the value of security to all employees and management.
- Build professional relationships across departments.
- Demonstrate operational excellence, consistency, and integrity.
- Influence organizational culture toward safety and security awareness.

COURSE OUTLINE

1 UNDERSTANDING RESPECT & CREDIBILITY IN ORGANIZATIONS

- Why respect is critical for security departments
- Common pitfalls: over-enforcement, lack of communication, low visibility
- Differentiating authority from influence

2 COMMUNICATING SECURITY'S VALUE

- Articulating security objectives in business language
- Linking security to operational continuity, productivity, and risk mitigation
- Developing clear internal messaging and awareness campaigns

3 PROFESSIONALISM & OPERATIONAL EXCELLENCE

- Consistent application of policies and procedures
- Demonstrating competence in risk management and incident response
- Building confidence through reliability and preparedness

4 BUILDING RELATIONSHIPS & COLLABORATION

- Engaging other departments without being confrontational
- Collaborative problem-solving with HR, operations, IT, and management
- Networking and mentorship within the organization

5 SECURITY AS A STRATEGIC PARTNER

- Shifting from "enforcement" to "advisor" role
- Participation in corporate planning, risk assessment, and decision-making
- Influencing company culture toward proactive security awareness

6 PERSONAL & TEAM DEVELOPMENT

- Developing soft skills: communication, conflict resolution, leadership
- Visibility through training, briefings, and corporate engagement
- Continuous improvement and feedback loops

17. ASSET PROTECTION & PROACTIVE SECURITY SYSTEMS

DURATION: 2–3 Days (Modular / Executive Format Available)
DELIVERY: Classroom | Site Practicals | Simulation | Hybrid
CERTIFICATION: SIVRIL Professional Certificate Course
CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

To equip security professionals with the capability to identify, prioritize, protect, and sustain critical assets using proactive, intelligence-led, and risk-based security systems that prevent loss, disruption, and reputational damage.

Participants learn how to shift from reactive guarding to value-driven protection.

TARGET AUDIENCE

- Chief Security Officers
- Asset Protection Managers
- Operations Managers
- Facility Managers
- Supply Chain Managers
- Retail & Industrial Security Leaders
- Risk & Compliance Officers
- Law Enforcement transitioning to private sector

LEARNING OUTCOMES

Participants will be able to:

- Identify and classify critical assets
- Conduct asset risk assessments
- Design layered protection strategies
- Implement proactive detection systems
- Reduce theft, fraud, sabotage and downtime
- Integrate people, process, and technology
- Measure asset protection performance
- Align protection with business objectives

COURSE OUTLINE

1 UNDERSTANDING ASSETS & BUSINESS VALUE

- Tangible vs intangible assets
- Criticality ranking
- Business dependency mapping
- Asset lifecycle risk
- Regulatory implications

2 ASSET RISK ASSESSMENT & VULNERABILITY ANALYSIS

- Threat identification
- Vulnerability mapping
- Impact analysis
- Risk prioritization
- Insider threats
- Environmental threats

3 PROACTIVE SECURITY SYSTEM DESIGN

- Layered security architecture
- Deterrence strategies
- Early detection systems
- Delay mechanisms
- Response integration
- Redundancy planning

4 TECHNOLOGY-ENABLED ASSET PROTECTION

- CCTV analytics
- Access control systems
- Asset tracking
- Intrusion detection
- Command centers
- Data integration

5 HUMAN SYSTEMS & OPERATIONAL CONTROLS

- Guard force optimization
- Insider threat programs
- Training and competence
- SOPs
- Ethics and accountability

6 LOSS PREVENTION & INVESTIGATIONS

- Theft and fraud patterns
- Evidence preservation
- Root cause analysis
- Case management
- Prosecution support

7 PERFORMANCE MANAGEMENT & CONTINUOUS IMPROVEMENT

- KPIs
- Audits
- Trend analysis
- ROI measurement
- Improvement cycles

18. EFFECTIVE KIDNAP MANAGEMENT STRATEGY – WEST AFRICA

Duration: 2 Days

COURSE OBJECTIVES

To prevent, prepare for, respond to, and recover from kidnap incidents in West Africa, while minimizing risk to life, reputation, and operations.

TARGET AUDIENCE

- Corporate executives, expatriates, and high-net-worth individuals
- NGO workers, journalists, and field personnel
- Drivers, security teams, and logistics personnel

COURSE OUTLINE

1 THREAT ASSESSMENT & INTELLIGENCE GATHERING

2 PREVENTION & PERSONAL SECURITY MEASURES

3 KIDNAP RESPONSE & CRISIS MANAGEMENT

- Crisis Team Activation
- Immediate Actions
- Negotiation Protocol

4 COMMUNICATION & MEDIA MANAGEMENT

- CCTV analytics
- Access control systems
- Asset tracking
- Intrusion detection
- Command centers
- Data integration

5 RECOVERY & REINTEGRATION

- Victim Support
- Operational Review
- Legal & Insurance Considerations

19. CORPORATE INVESTIGATION STRATEGY & GOVERNANCE

CATEGORY: Investigations | Compliance | Risk | Governance
DURATION: 3–5 Days (Executive / Professional Format Available)
DELIVERY: Classroom | Case Labs | Simulation | Hybrid
CERTIFICATION: SIVRIL Executive Certificate
CPE ALIGNMENT: ASIS Eligible

COURSE OBJECTIVES

To equip security, compliance, and executive leaders with the ability to design, govern, and execute defensible corporate investigation programs that prevent fraud, misconduct, corruption, data breaches, workplace abuse, and regulatory exposure.

Participants learn how to move from ad-hoc investigations to structured, legally defensible investigative systems.

TARGET AUDIENCE

- Chief Security Officers
- Compliance & Ethics Officers
- Internal Audit Leaders
- Legal Counsel
- HR Directors
- Risk Managers
- Investigations Managers
- Regulators
- NGO Governance Leaders

LEARNING OUTCOMES

Participants will be able to:

- Design corporate investigation frameworks
- Establish governance and reporting structures
- Conduct legally defensible investigations
- Manage evidence and digital data
- Protect whistleblowers and victims
- Coordinate with regulators and law enforcement
- Mitigate organizational risk
- Strengthen ethics culture

COURSE CONTENT

1 FOUNDATIONS OF CORPORATE INVESTIGATIONS

- Purpose of corporate investigations
- Legal frameworks
- Regulatory exposure
- Corporate liability
- Ethics and privacy
- Cross-border issues

2 INVESTIGATION GOVERNANCE & STRATEGY

- Investigation policy design
- Intake mechanisms
- Triage systems
- Escalation thresholds
- Independence and oversight
- Budgeting

3 INVESTIGATION PLANNING & CASE MANAGEMENT

- Case scoping
- Risk assessment
- Evidence mapping
- Investigation plans
- Documentation standards
- Chain of custody

4 DIGITAL & PHYSICAL EVIDENCE MANAGEMENT

- Email and device forensics
- CCTV evidence
- Access logs
- Data integrity
- Secure storage
- Disclosure obligations

5 INTERVIEWING & STATEMENT ANALYSIS

- Interview planning
- Cognitive interviewing
- Deception indicators
- Trauma-informed approaches
- Cultural sensitivity
- Documentation

6 LEGAL INTERFACE & REGULATORY ENGAGEMENT

- Attorney privilege
- Reporting obligations
- Law enforcement referral
- Regulatory cooperation
- Cross-border compliance

7 REPORTING, REMEDIATION & GOVERNANCE

- Investigation reports
- Root cause analysis
- Control remediation
- Disciplinary processes
- Board reporting
- ESG impact

8 ETHICS, WHISTLEBLOWER PROTECTION & SAFEGUARDING

- Whistleblower systems
- Retaliation prevention
- Survivor protection
- Data privacy
- Cultural risks

20. PROFESSIONAL INVESTIGATION SKILLS AND TECHNIQUES

DURATION: 3days

COURSE OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the principles and ethics of investigations.
2. Conduct systematic investigations using proper methodologies.
3. Gather, preserve, and analyze physical and digital evidence.
4. Conduct effective interviews and interrogations.
5. Prepare comprehensive investigation reports.
6. Avoid common investigative pitfalls and legal issues.

TARGET AUDIENCE

- Investigators,
- Security personnel
- Compliance officers
- Forensic practitioners

COURSE OUTLINE

1 INTRODUCTION & PRINCIPLES
- Fundamentals of Investigation
- Legal and Ethical Considerations
- Nigerian labour law

2 INVESTIGATION PLANNING & EVIDENCE HANDLING
- Investigation Planning
- Evidence Identification and Preservation

3 INTERVIEWING & INTERROGATION TECHNIQUES
- Interview Techniques
- Interrogation Methods
- Legal boundaries
- Psychological approaches

4 ANALYSIS & REPORTING
- Evidence Analysis
- Report Writing

5 ADVANCED INVESTIGATIONS & REVIEW
- Special Investigations
- Review and Assessment

21. SITUATIONAL AWARENESS TRAINING COURSE FOR SECURITY PROFESSIONALS

DURATION: 2 days

TARGET AUDIENCE

- Security guards
- Corporate security officers
- Event security personnel
- Law enforcement support staff

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand the concept and levels of situational awareness.
2. Recognize potential threats and suspicious behavior in various environments.
3. Apply observational techniques and improve memory recall.
4. Anticipate potential security risks and prepare appropriate responses.
5. Integrate situational awareness into daily security operations and emergency scenarios.

COURSE OUTLINE

1 INTRODUCTION TO SITUATIONAL AWARENESS

- Definition: Perception + Comprehension + Projection
- Why situational awareness is crucial in security operations
- Real-life examples of security breaches prevented through awareness
- Levels of awareness (from relaxed alertness to high alert)

2 OBSERVATION SKILLS

- Key observation techniques:
  Systematic scanning
  Noticing unusual behavior, objects, or environmental changes
  Pattern recognition (daily routines, crowd behavior)
- Using all senses effectively
- Recording observations accurately

3 THREAT RECOGNITION & RISK ASSESSMENT

- Recognizing suspicious behavior (loitering, nervous actions, concealed objects)
- Environmental threats (structural hazards, exits, lighting, crowd density)
- Assessing risk levels and prioritizing responses
- Common security blind spots

4 SITUATIONAL AWARENESS IN PRACTICE

- Applying situational awareness in:
  Patrols and access control
  Event security
  Surveillance operations
  Emergency response (fire, medical, active threats)
- Maintaining awareness under stress or fatigue
- Communication protocols for reporting risks

5 COGNITIVE SKILLS & DECISION MAKING

- Avoiding tunnel vision and confirmation bias
- Situational prioritization: what to respond to first
- Maintaining calm and clarity in high-pressure situations
- Using technology to support awareness (CCTV, alarms, drones, mobile apps)

22. MANAGING SECURITY AMID KIDNAPPING AND HOSTAGE THREATS IN NIGERIA

DURATION: 1 day

TARGET AUDIENCE

- Security managers
- Corporate staff in high-risk zones
- Risk officers

LEARNING OUTCOMES

- Understand kidnap-for-ransom trends in Nigeria
- Conduct risk assessment for personnel and assets
- Develop prevention strategies and SOPs
- Coordinate crisis response and negotiation procedures

COURSE OUTLINE

1 OVERVIEW OF KIDNAP THREATS IN NIGERIA

Patterns
Motives
and high-risk zones

2 RISK ASSESSMENT & PREVENTION

Travel risk
Residential security
and SOPs

3 CRISIS RESPONSE & HOSTAGE NEGOTIATION

Incident command,
communication, and
law enforcement coordination

4 CASE STUDIES

- Nigerian incidents, lessons learned

5 ACTION PLANNING & DRILLS

Developing response plans and simulations

23. COMMUNITY-CENTRIC SECURITY: PREVENTING DISRUPTIONS IN NIGERIA'S VOLATILE REGIONS

DURATION: 1 day

TARGET AUDIENCE

- Security managers,
- Field operations teams,
- Corporate social responsibility officers

LEARNING OUTCOMES

- Build trust and rapport with local communities
- Identify early warning signs of communal unrest
- Integrate local intelligence into security planning
- Maintain operational continuity during tensions

COURSE OUTLINE

1 UNDERSTANDING LOCAL DYNAMICS

Ethnic, religious, and political tensions

2 COMMUNITY ENGAGEMENT STRATEGIES

Communication, negotiation, and collaboration

3 CONFLICT MITIGATION & OPERATIONAL CONTINUITY

Risk mapping and contingency planning

4 CASE STUDIES

Successful corporate-community collaborations

24. SECURITY MANAGEMENT FOR CRITICAL INFRASTRUCTURE IN NIGERIA

DURATION: 2 days

TARGET AUDIENCE

Security managers in oil & gas, telecoms,

Energy, transport, and corporate facilities

LEARNING OUTCOMES

- Understand threats to critical infrastructure
- Conduct vulnerability assessments
- Design protective measures and SOPs
- Coordinate emergency response and recovery

COURSE OUTLINE

1 CRITICAL INFRASTRUCTURE LANDSCAPE IN NIGERIA

Sectors, threats, and regulatory requirements

2 RISK ASSESSMENT & VULNERABILITY ANALYSIS

Physical and cyber risks

3 SECURITY PLANNING & OPERATIONAL CONTROLS

SOPs, surveillance, access control

4 EMERGENCY PREPAREDNESS & RESPONSE

Drills, communication, and coordination

5 CASE STUDIES

Nigerian infrastructure security successes and failures

25. INSIDER THREATS AND CORRUPTION RISK MANAGEMENT IN NIGERIAN ORGANIZATIONS

DURATION: 1 day

TARGET AUDIENCE

Security, HR, compliance,
and operations managers

LEARNING OUTCOMES

- Recognize insider threat indicators
- Assess corruption and fraud risk
- Implement monitoring, reporting, and mitigation strategies
- Respond to internal security incidents

COURSE OUTLINE

1 UNDERSTANDING INSIDER THREATS & CORRUPTION

Motivations and impact

2 DETECTION & MONITORING TECHNIQUES

Behavioral and operational red flags

3 POLICIES & CONTROLS

Screening, SOPs, and whistleblower programs

4 INCIDENT RESPONSE & INVESTIGATION

Internal audits and reporting

5 CASE STUDIES & LESSONS LEARNED

Nigerian corporate and government incidents

26. SECURITY TRAINING COURSE FOR BEGINNERS

DURATION: 3–5 days (can be adjusted based on organization needs)

TARGET AUDIENCE

New security guards or officers

Entry-level corporate security personnel

Event security staff

LEARNING OUTCOMES

By the end of this course, participants will be able to:

- Understand the role and responsibilities of a security professional.
- Apply basic situational awareness and observation techniques.
- Handle access control, patrolling, and reporting procedures.
- Respond appropriately to emergencies and minor security incidents.
- Demonstrate professional conduct and communication skills.

COURSE OUTLINE

1 INTRODUCTION TO SECURITY

- Role of a Security Professional
- Legal & Ethical Basics

2 BASIC OBSERVATION & SITUATIONAL AWARENESS

- Introduction to Situational Awareness
- Observation Skills for Beginners

3 SECURITY PROCEDURES & TOOLS

- Access Control
- Patrolling & Monitoring
- Communication Skills

4 RESPONDING TO EMERGENCIES

Fire safety, medical emergencies, and evacuation procedures.
Handling aggressive or suspicious individuals safely

5 PERSONAL SAFETY & RISK AWARENESS

- Protecting oneself while protecting others
- Identifying hazards in the environment

27. PRESENTING SECURITY TO THE BOARDROOM

DURATION: 1 day

TARGET AUDIENCE

- Security managers
- Corporate security officers
- Risk and compliance officers
- Anyone responsible for communicating security matters to executives

LEARNING OUTCOMES

By the end of this training, participants will be able to:

1. Understand the expectations and priorities of board members regarding security.
2. Translate technical security issues into business risk language.
3. Prepare structured, clear, and persuasive security presentations.
4. Use data and visuals effectively to support recommendations.
5. Handle boardroom questions and discussions confidently.

COURSE OUTLINE

1 UNDERSTANDING THE BOARDROOM PERSPECTIVE

- Difference between operational security and strategic security.
- What executives care about: risk exposure, cost, compliance, reputation.
- Aligning security reporting with business objectives.

2 COMMUNICATING SECURITY AS RISK

- Translating technical issues into business risk language.
- Using the “Impact vs Likelihood” approach for security threats.
- Highlighting consequences for the organization: financial, reputational, legal.

3 STRUCTURING YOUR PRESENTATION

Key elements of an effective boardroom presentation:

1. Executive summary (focus on key risks)
2. Threat landscape (high-level overview)
3. Current security posture and gaps
4. Recommended actions and business impact
5. Cost vs benefit and risk mitigation options

- Best practices: keep slides simple, focus on visuals, avoid jargon.

4 DATA VISUALIZATION & SUPPORTING MATERIALS

- Using charts, heat maps, dashboards, and tables to illustrate risk.
- Highlighting trends and patterns clearly.
- Providing backup data in appendices for board reference.

5 BOARDROOM DELIVERY & CONFIDENCE

- Professional presence: tone, posture, and pacing.
- Managing Q&A with executives: anticipating difficult questions.
- Using storytelling to make security relatable.
- Handling pushback or skepticism effectively.

28. DATA ANALYTICS FOR SECURITY PROFESSIONALS

DURATION: 2–3 days (can be condensed into 1 full day for overview)

TARGET AUDIENCE

- Security analysts
- Security managers
- Corporate security officers
- Risk and compliance personnel

LEARNING OUTCOMES

By the end of this training, participants will be able to:

1. Understand the role of data analytics in modern security operations.
2. Collect, organize, and interpret security data effectively.
3. Identify trends, anomalies, and potential threats from data sets.
4. Use analytics tools and visualization techniques to support decision-making.
5. Communicate analytical findings in a clear and actionable way.

COURSE OUTLINE

1 INTRODUCTION TO SECURITY DATA ANALYTICS

- Definition and importance of data analytics in security.
- Types of data in security operations:
  Physical security: access logs, CCTV footage, patrol records
  Cybersecurity: network logs, intrusion attempts
  Incident reports and case files
- How analytics improves decision-making, resource allocation, and risk mitigation.

2 DATA COLLECTION & ORGANIZATION

- Principles of accurate data collection: consistency, completeness, and timeliness.
- Structuring data for analysis: spreadsheets, databases, and logs.
- Data privacy and security compliance considerations.

3 BASIC ANALYTICAL TECHNIQUES

- Descriptive analytics: summarizing past incidents and trends
- Diagnostic analytics: identifying patterns and correlations
- Predictive analytics: anticipating threats and vulnerabilities
- Key metrics for security operations: incident frequency, response times, access anomalies

4 DATA VISUALIZATION FOR SECURITY INSIGHTS

- Using charts, heatmaps, dashboards, and graphs to communicate insights.
- Highlighting trends, anomalies, and priority risks visually.
- Tools overview: Excel, Power BI, Tableau, or security-specific platforms

5 DECISION-MAKING AND REPORTING

- Translating analytical findings into actionable recommendations.
- Preparing executive-friendly security reports.
- Aligning data insights with organizational risk priorities.

6 ADVANCED TOPICS & EMERGING TOOLS

- AI and machine learning applications in security analytics
- Real-time analytics for CCTV, intrusion detection, and access control
- Predictive risk modelling.

29. INTERVIEW & INTERROGATION TECHNIQUES

DURATION: 2 days

TARGET AUDIENCE

Investigators

HR managers

Security personnel

LEARNING OUTCOMES

- Conduct effective witness and suspect interviews
- Identify deception and assess credibility
- Maintain ethical and legal compliance during interrogations

COURSE OUTLINE

1 INTRODUCTION TO INVESTIGATIVE INTERVIEWING

- Purpose and legal considerations

2 QUESTIONING TECHNIQUES

- Open-ended, closed, probing, and leading questions

3 BEHAVIORAL ANALYSIS & DECEPTION DETECTION

- Verbal and non-verbal cues

4 HANDLING DIFFICULT INTERVIEWS

Resistance, hostility, or uncooperative subjects

5 ROLE-PLAY EXERCISES

- Conducting interviews in simulated scenarios

6 DOCUMENTATION & REPORTING

- Recording interviews for legal and organizational purposes

1. CRIME SCENE & FORENSIC INVESTIGATION FUNDAMENTALS

DURATION: 2 days

TARGET AUDIENCE

Security professionals

Forensic officers,

Corporate investigators

LEARNING OUTCOMES

- Secure and manage crime scenes
- Collect and document forensic evidence
- Maintain chain of custody and ensure legal admissibility

COURSE OUTLINE

CRIME SCENE MANAGEMENT 1

Securing, documenting, and controlling access

EVIDENCE COLLECTION & PRESERVATION 2

Physical, digital, and trace evidence

CHAIN OF CUSTODY 3

Documentation and integrity of evidence

FORENSIC PRINCIPLES 4

Introduction to forensic analysis methods

PRACTICAL EXERCISE 5

Simulated crime scene management and evidence collection

REPORTING & COURT PREPARATION 6

Structuring evidence for legal proceedings

2. INVESTIGATION REPORT WRITING FOR LEGAL & CORPORATE USE

DURATION: 2 days

TARGET AUDIENCE

Investigators

Security officers

Compliance managers

LEARNING OUTCOMES

- Produce clear, accurate, and admissible investigation reports
- Present findings in legal and organizational contexts
- Structure reports for management and courtroom use

COURSE OUTLINE

1 INTRODUCTION TO INVESTIGATION REPORTING

Purpose, audience, and standards

2 STRUCTURING REPORTS

Executive summary, findings, evidence, conclusions

3 WRITING TECHNIQUES

Clarity, accuracy, and professionalism

4 LEGAL CONSIDERATIONS

Admissibility and chain of custody

5 PRACTICAL EXERCISES

Drafting sample investigation reports

6 PEER REVIEW & FEEDBACK

Improving report quality and credibility

3. INTRODUCTION TO FORENSICS & CRIME SCENE MANAGEMENT

DURATION: 3 days

TARGET AUDIENCE

- Security personnel
- Law enforcement recruits
- Investigators-in-training
- Forensic science students

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand the fundamentals of forensic science and its role in criminal investigations.
2. Recognize different types of evidence and their significance.
3. Apply proper procedures for securing and managing a crime scene.
4. Document and preserve evidence in compliance with legal standards.
5. Avoid common mistakes that compromise investigations.

COURSE OUTLINE

1 INTRODUCTION TO FORENSICS

- Definition and scope of forensic science.
- Key disciplines within forensics:
  Crime scene investigation (CSI)
  Fingerprint analysis
  Forensic biology (blood, DNA)
  Forensic chemistry (drugs, toxins)
  Digital forensics
- The role of forensic evidence in the justice system.

2 TYPES OF EVIDENCE & THEIR IMPORTANCE

- Physical evidence: weapons, clothing, fingerprints, trace materials
- Biological evidence: blood, hair, bodily fluids
- Digital evidence: computers, phones, CCTV
- Documentary evidence: notes, logs, contracts
- Demonstrative evidence: reconstructions, diagrams
- Principles of evidence integrity and chain of custody

3 CRIME SCENE MANAGEMENT

Steps for managing a crime scene:

1. First responder duties
2. Securing the scene to prevent contamination
3. Initial assessment and documentation
4. Systematic evidence search and collection
5. Evidence packaging, labeling, and transport

- Crime scene photography and sketching
- Using checklists and standard operating procedures (SOPs)

4 LEGAL & ETHICAL CONSIDERATIONS

- Understanding admissibility of evidence
- Maintaining chain of custody
- Avoiding contamination and procedural errors
- Ethics in forensic investigations

5 DOCUMENTATION & REPORTING

- Preparing professional crime scene reports
- Photograph logs, sketches, and evidence inventory
- Clear and concise reporting for law enforcement and courts

4. FORENSIC PSYCHOLOGY & CRIMINAL PROFILING

DURATION: 1–2 days (can be expanded with practical exercises or case studies)

TARGET AUDIENCE

- Security professionals
- Investigators and law enforcement personnel
- Forensic science students
- Anyone interested in understanding criminal behavior

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand the principles of forensic psychology and its role in criminal investigations.
2. Recognize behavioral patterns associated with different types of offenders.
3. Apply basic techniques of criminal profiling to assist investigations.
4. Analyze crime scenes, victimology, and evidence from a psychological perspective.
5. Communicate findings effectively to investigative teams and law enforcement.

COURSE OUTLINE

1 INTRODUCTION TO FORENSIC PSYCHOLOGY

- Definition and scope of forensic psychology
- Role of forensic psychologists in criminal investigations
- Key areas: assessment, criminal behavior analysis, courtroom testimony
- Differences between clinical psychology and forensic psychology

2 UNDERSTANDING CRIMINAL BEHAVIOR

- Factors influencing criminal behavior:
  Biological, psychological, and sociological influences
  Personality traits and disorders (antisocial behavior, psychopathy)
  Motivations behind criminal acts
- Types of offenders: organized vs. disorganized, impulsive vs. planned

3 CRIMINAL PROFILING BASICS

Definition and objectives of profiling

- Types of profiles:
  Crime scene profiles (linking behavior to psychological traits)
  Suspect profiles (predicting age, gender, occupation, habits)
- Components of profiling:
  Crime scene analysis
  Victimology
  Modus operandi (MO) and signature behaviors
  Geographic profiling

4 PSYCHOLOGICAL ASSESSMENT IN INVESTIGATIONS

- Interviewing techniques: detecting deception, eliciting information
- Behavioral observation and interpretation
- Using psychological insights to prioritize suspects or investigative leads

5 CASE STUDIES & PRACTICAL APPLICATION

- Real-life cases demonstrating effective profiling and forensic psychology
- Lessons learned from profiling successes and failures
- Group exercise: develop a mini-profile from provided case data

6 REPORTING & COMMUNICATION

- Documenting psychological insights for investigative teams
- Presenting profiling findings clearly and concisely
- Ethical considerations in profiling and reporting

5. TRAINING COURSE: DIGITAL FORENSICS & CYBERCRIME

DURATION: 3 days (can be condensed to 1 day for an overview or extended with hands-on labs)

TARGET AUDIENCE

- Security professionals
- Law enforcement officers
- Corporate investigators
- IT/security personne

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand the fundamentals of digital forensics and cybercrime.
2. Identify and preserve digital evidence according to legal standards.
3. Investigate cyber incidents using structured forensic methodologies.
4. Analyze digital evidence from computers, mobile devices, and networks.
5. Communicate findings effectively for investigations, reports, and legal proceedings.

COURSE OUTLINE

1 INTRODUCTION TO DIGITAL FORENSICS & CYBERCRIME

- Definition and scope of digital forensics
- Types of cybercrime:
- Hacking, phishing, malware attacks
  Insider threats
  Financial fraud and identity theft
  Cyberstalking and harassment
- The role of digital forensics in modern investigations
- Legal and ethical considerations

2 DIGITAL EVIDENCE & PRESERVATION

- Types of digital evidence: computers, servers, mobile devices, cloud storage, network logs
- Principles of evidence preservation:
  Integrity and chain of custody
  Avoiding alteration or deletion of data
- Imaging, hashing, and documenting digital evidence

3 CYBERCRIME INVESTIGATION METHODOLOGY

- Investigation phases:
  1. Identification
  2. Collection
  3. Preservation
  4. Analysis
  5. Presentation
- Using logs, metadata, and digital footprints to trace activity
- Introduction to common forensic tools: EnCase, FTK, Autopsy, Cellebrite (overview)

4 ANALYSIS OF DIGITAL EVIDENCE

- File and data analysis: recovered files, deleted items, timestamps
- Network forensics: IP tracing, packet analysis, identifying breaches
- Mobile forensics: SMS, call logs, GPS, app data
- Understanding malware behavior and digital signatures

5 REPORTING & LEGAL CONSIDERATIONS

- Writing clear and concise digital forensics reports
- Presenting findings for investigators, executives, or in court
- Maintaining chain of custody and admissibility of evidence
- Privacy and compliance issues in cyber investigations

6 EMERGING THREATS & ADVANCED TOPICS

- Cloud computing and IoT security threats
- Ransomware, phishing, and social engineering
- Cybercrime trends and predictive analytics in cybersecurity
- Future tools and AI applications in digital forensics.

6. TRAINING COURSE: FORENSIC EVIDENCE IN COURT

DURATION: 1 Day

TARGET AUDIENCE

- Security professionals
- Investigators and law enforcement officers
- Forensic examiners
- Legal support staff involved in investigations

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand the role of forensic evidence in legal proceedings.
2. Explain the rules and standards governing the admissibility of forensic evidence.
3. Prepare forensic reports suitable for court presentation.
4. Testify effectively as an expert witness or supporting investigator.
5. Handle challenges and cross-examination of forensic evidence

COURSE OUTLINE

1 INTRODUCTION TO FORENSIC EVIDENCE IN COURT

- Role of forensic evidence in criminal and civil cases
- Types of evidence commonly presented:
  Physical, biological, digital, trace, and documentary evidence
- Importance of accuracy, integrity, and chain of custody
- Understanding how judges and juries perceive forensic evidence

2 ADMISSIBILITY OF EVIDENCE

- Legal standards for admissibility:
  Daubert standard (scientific validity)
  Frye standard (general acceptance)
  Local and national legislation on forensic evidence
  Ensuring forensic procedures meet legal and ethical standards
- Common pitfalls that lead to evidence being challenged or rejected

3 FORENSIC REPORTS & DOCUMENTATION

- Structure of a court-ready forensic report:
  Executive summary
  Methods and procedures used
  Findings and conclusions
  References and appendices
- Clarity, conciseness, and avoidance of jargon
- Linking evidence to investigative findings or charges

4 EXPERT WITNESS TESTIMONY

- Role of the forensic expert in court
- Preparing for testimony:
  Reviewing reports and evidence
  Anticipating questions and cross-examination
- Communicating findings clearly to judges, juries, and lawyers
- Handling challenging or misleading questions professionally

5 HANDLING CHALLENGES & OBJECTIONS

- Responding to challenges regarding:
  Methodology
  Chain of custody
  Accuracy and interpretation of results
- Maintaining professionalism under pressure
- Strategies for reinforcing credibility in court

7. EXPERT WITNESS IN COURT

DURATION: 1 Day

TARGET AUDIENCE

- Security professionals
- Forensic examiners and investigators
- Law enforcement personnel
- Professionals likely to present evidence in court

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand the role and responsibilities of an expert witness.
2. Prepare forensic or investigative findings for court presentation.
3. Communicate complex technical information clearly to judges and juries.
4. Respond confidently to direct examination and cross-examination.
5. Maintain professionalism, credibility, and impartiality during testimony.

COURSE OUTLINE

1 ROLE OF THE EXPERT WITNESS

- Definition and purpose of an expert witness
- Difference between expert witnesses and fact witnesses
- Duties and responsibilities in legal proceedings
- Legal and ethical considerations for expert testimony

2 PREPARATION FOR COURT TESTIMONY

- Reviewing case materials and evidence thoroughly
- Understanding the questions you may be asked
- Preparing concise, factual, and non-biased statements
- Using reports, diagrams, and visual aids effectively

3 COMMUNICATING COMPLEX INFORMATION

- Translating technical or forensic findings into clear, understandable language
- Avoiding jargon and overly technical terms
- Using visuals (charts, diagrams, timelines) to support explanations
- Adjusting communication style for judges, juries, and lawyers

4 TESTIMONY & COURTROOM CONDUCT

- Direct examination: presenting findings confidently and accurately
- Cross-examination: handling challenging or leading questions
- Maintaining impartiality and professionalism under pressure
- Body language, tone, and demeanor for credibility

5 HANDLING CHALLENGES & OBJECTIONS

- Common tactics used in cross-examination
- Responding to credibility challenges, contradictions, or technical questions
- Staying composed and avoiding argumentative responses
- Reinforcing credibility with facts, methodology, and clarity

8. FORENSIC EVIDENCE IN THE COURTROOM: UNDERSTANDING SCIENCE, PRACTICE, AND ADMISSIBILITY

DURATION: 1 Day

TARGET AUDIENCE

- Judges
- Lawyers (prosecutors and defense attorneys)
- Legal scholars and practitioners
- Court staff involved in evidence evaluation

LEARNING OUTCOMES

By the end of this training, participants will be able to:

1. Understand the fundamental principles of forensic science relevant to legal proceedings.
2. Recognize the types of forensic evidence commonly presented in court.
3. Evaluate the reliability, validity, and limitations of forensic evidence.
4. Understand legal standards for admissibility (e.g., Daubert, Frye, local jurisdiction rules).
5. Question and interpret expert witness testimony effectively.
6. Apply best practices in handling forensic evidence in legal decision-making.

COURSE OUTLINE

1 INTRODUCTION TO FORENSIC EVIDENCE

- What is forensic evidence and why it matters in legal proceedings
- The intersection of science and law: objectivity vs. legal interpretation
- Types of evidence: DNA, fingerprints, digital forensics, trace evidence, ballistic evidence

2 SCIENCE BEHIND FORENSIC EVIDENCE

- How forensic techniques generate evidence
- Understanding accuracy, error rates, and uncertainty
- Strengths and limitations of different forensic disciplines
- Avoiding misconceptions (forensic "myths" vs. reality)

3 LEGAL STANDARDS AND ADMISSIBILITY

- Overview of admissibility standards:
  Daubert standard – reliability and scientific validity
  Frye standard – general acceptance in the relevant scientific community
  Local jurisdiction-specific rules
- Challenges in court: cross-examination, conflicting expert opinions
- Importance of chain of custody, documentation, and ethical practice

4 EVALUATING EXPERT WITNESS TESTIMONY

- Understanding the role of the expert witness in court
- Evaluating credibility, methodology, and conclusions
- Asking appropriate questions to clarify evidence without leading
- Handling conflicting expert opinions

5 INTERPRETING AND APPLYING FORENSIC EVIDENCE

- Translating scientific evidence into legal arguments
- Weighing evidence in case preparation and judicial decisions
- Recognizing when forensic evidence is corroborative vs. conclusive
- Ethical considerations in presenting or evaluating forensic evidence

6 EMERGING TRENDS AND CHALLENGES

- Advances in forensic science (digital forensics, AI-assisted analysis)
- New legal challenges and considerations
- Case law trends regarding forensic evidence
- Best practices for courts and legal practitioners

1. STRATEGIC LEADERSHIP & DECISION MAKING

DURATION: 2 Days

TARGET AUDIENCE

- Professionals at all levels
- Students or early-career individuals
- Team leaders or aspiring leaders
- Anyone interested in improving personal or organizational decision-making skills

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand what strategic leadership means and why it matters in personal and professional contexts.
2. Apply effective decision-making frameworks to everyday challenges.
3. Recognize personal biases and barriers to good decision-making.
4. Lead themselves and others toward achieving goals strategically.
5. Reflect, evaluate, and improve decisions over time.

COURSE OUTLINE

1 UNDERSTANDING STRATEGIC LEADERSHIP

- What leadership is and why it matters for everyone
- Difference between reactive (tactical) and strategic thinking
- Key traits of effective leaders: vision, integrity, resilience, empathy
- Leadership at work, in community, and personal life

2 FUNDAMENTALS OF DECISION MAKING

- Types of decisions: everyday, important, strategic
- Decision-making steps: define, analyze, choose, act, review
- Common cognitive biases and how they affect choices
- Balancing logic and intuition in decisions

3 STRATEGIC THINKING MADE SIMPLE

- Understanding goals: short-term vs long-term
- Prioritization and planning
- Using basic SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) in life and work
- Scenario thinking anticipating consequences before acting

4 RISK AWARENESS & PROBLEM SOLVING

- Identifying potential risks and opportunities in choices
- Simple tools: pros and cons list, risk-reward analysis
- Thinking creatively to solve challenges
- Learning from past mistakes

5 LEADING YOURSELF AND OTHERS

- Personal accountability: taking ownership of decisions
- Influencing and motivating others without authority
- Communication and collaboration in decision-making
- Dealing with conflict constructively

6 REFLECTING, EVALUATING AND IMPROVING DECISIONS

- How to review outcomes: what worked, what didn't
- Adjusting strategies for continuous improvement
- Building confidence and resilience in decision-making

2. EMOTIONAL INTELLIGENCE & INFLUENCE

DURATION: 2 Days

TARGET AUDIENCE

- Professionals at all levels
- Leaders and aspiring leaders
- Team members who interact with colleagues, clients, or stakeholders
- Anyone seeking to improve self-awareness and interpersonal effectiveness

LEARNING OUTCOMES

By the end of this Course, participants will be able to:

1. Understand the concept and components of emotional intelligence (EI).
2. Recognize the role of EI in personal and professional success.
3. Manage their own emotions and respond effectively to others.
4. Build strong relationships through empathy and effective communication.
5. Apply influence techniques ethically to motivate and guide others.

COURSE OUTLINE

1 INTRODUCTION TO EMOTIONAL INTELLIGENCE

- Definition and importance of EI
- Four core components of EI (Daniel Goleman model):
  1. Self-awareness
  2. Self-management
  3. Social awareness (empathy)
  4. Relationship management
- How EI impacts personal effectiveness, teamwork, and leadership

2 SELF-AWARENESS & SELF-MANAGEMENT

- Recognizing emotions and triggers
- Techniques for regulating emotions under pressure
- Building resilience and stress management
- Aligning actions with values and goals

3 SOCIAL AWARENESS & EMPATHY

- Understanding and interpreting others' emotions
- Active listening and effective questioning
- Reading verbal and non-verbal cues
- Cultural and situational empathy

4 RELATIONSHIP MANAGEMENT & INFLUENCE

- Building trust and rapport
- Conflict resolution and negotiation
- Collaborative problem-solving
- Ethical influence techniques: persuasion, motivation, and coaching

5 APPLYING EI IN LEADERSHIP AND EVERYDAY LIFE

- Using EI to improve decision-making and leadership
- Leading diverse teams effectively
- Managing difficult conversations with confidence
- Enhancing personal and organizational performance through EI

3. PUBLIC SPEAKING FOR PROFESSIONALS

DURATION: 2 Days

TARGET AUDIENCE

- Professionals at all levels
- Team leaders, managers, and executives
- Security professionals, investigators, or anyone presenting findings
- Anyone looking to improve confidence and impact in public speaking

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the fundamentals of effective public speaking.
2. Structure and deliver clear, engaging presentations.
3. Manage nerves and project confidence.
4. Engage and influence audiences through verbal and non-verbal communication.
5. Handle questions and challenging situations professionally.

COURSE OUTLINE

1 INTRODUCTION TO PUBLIC SPEAKING

- Importance of effective communication in professional settings
- Overcoming fear and anxiety in public speaking
- Identifying your personal speaking style
- Elements of a strong presentation: clarity, structure, and engagement

2 STRUCTURING YOUR PRESENTATION

- The 3-part structure: Introduction, Body, Conclusion
- Crafting a clear message or objective
- Using storytelling and examples to illustrate points
- Creating logical flow and transitions

3 VOICE, TONE & BODY LANGUAGE

- Using vocal variety for emphasis and engagement
- Controlling pace, volume, and clarity
- Positive body language: gestures, posture, and eye contact
- Avoiding distracting habits

4 ENGAGING THE AUDIENCE

- Techniques to capture and maintain attention
- Asking questions and encouraging participation
- Reading audience reactions and adapting accordingly
- Using visual aids effectively: slides, charts, props

5 HANDLING QUESTIONS & CHALLENGING SITUATIONS

- Responding to questions confidently and professionally
- Handling interruptions or disagreements
- Staying composed under pressure
- Strategies for difficult audiences

4. ETHICAL LEADERSHIP

DURATION: 2 Days

TARGET AUDIENCE

- Corporate leaders and managers
- Security and investigative professionals
- Team leaders and supervisors
- Professionals in governance, compliance, or HR
- Anyone seeking to enhance ethical decision-making and leadership impact

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the principles and importance of ethical leadership.
2. Recognize ethical dilemmas and navigate them effectively.
3. Apply integrity and transparency in decision-making.
4. Foster an ethical culture within teams and organizations.
5. Balance competing interests and pressures while maintaining ethical standards.

COURSE OUTLINE

1 INTRODUCTION TO ETHICAL LEADERSHIP

- Definition and significance of ethical leadership
- The difference between leadership and ethical leadership
- Core values and principles: integrity, accountability, transparency, fairness
- Benefits of ethical leadership for individuals and organizations

2 ETHICS IN DECISION-MAKING

- Understanding ethical dilemmas and conflicts of interest
- Decision-making frameworks for ethical challenges
- Balancing personal, organizational, and societal responsibilities
- Consequences of unethical decisions on reputation and operations

3 BUILDING AN ETHICAL CULTURE

- The leader's role in shaping organizational culture
- Establishing codes of conduct, policies, and accountability mechanisms
- Encouraging open communication and ethical reporting
- Leading by example: walking the talk

4 ETHICAL LEADERSHIP IN PRACTICE

- Handling pressure, conflicts, and competing interests ethically
- Communicating decisions transparently
- Promoting fairness and equity in team management
- Building trust and credibility with stakeholders

5 PERSONAL DEVELOPMENT AS AN ETHICAL LEADER

- Self-awareness and reflection on values
- Continuous learning and feedback
- Accountability and personal responsibility
- Mentoring and developing ethical leaders within the organization

5. MANAGING GEN Z IN THE WORKPLACE – ENGAGING, MOTIVATING, AND LEADING THE NEXT GENERATION

COURSE OBJECTIVE:

Equip managers and leaders with strategies to understand, engage, motivate, and retain Gen Z employees, while balancing multi-generational team dynamics.

TARGET AUDIENCE

- Managers and team leaders
- HR professionals
- Executives and department heads
- Project leads supervising multi-generational teams

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the characteristics, values, and expectations of Gen Z.
2. Adapt management and communication styles to fit Gen Z needs.
3. Develop engagement, motivation, and retention strategies for younger employees.
4. Manage conflicts and expectations between Gen Z and other generations.
5. Leverage Gen Z's digital skills and innovation potential for organizational success.

COURSE OUTLINE

1 UNDERSTANDING GEN Z

- Who Gen Z are and what defines them: digital natives, diversity-minded, purpose driven
- Work values: flexibility, technology, recognition, career growth
- Generational differences and stereotypes in the workplace

2 COMMUNICATION & LEADERSHIP STYLES

- Effective communication with Gen Z: direct, transparent, digital-friendly
- Leadership approaches: coaching, mentoring, and feedback-driven management
- Adapting management styles to bridge generational gaps

3 ENGAGEMENT & MOTIVATION STRATEGIES

- Motivators for Gen Z: purpose, autonomy, skill development, recognition
- Creating a workplace culture that attracts and retains young talent
- Leveraging flexibility, technology, and innovation opportunities

4 PERFORMANCE MANAGEMENT & CAREER DEVELOPMENT

- Setting goals, providing feedback, and performance evaluations
- Career development paths and growth opportunities
- Reward systems that resonate with Gen Z

5 MULTI-GENERATIONAL TEAM MANAGEMENT

- Understanding differences between Baby Boomers, Gen X, Millennials, and Gen Z
- Managing conflicts and expectations across generations
- Creating collaborative, high-performing multi-generational teams

6 ACTION PLANNING & IMPLEMENTATION

- Developing personal leadership strategies for managing Gen Z
- Creating policies, communication plans, and engagement initiatives
- Monitoring and adapting strategies over time

6. ADAPTIVE LEADERSHIP IN COMPLEX ENVIRONMENTS

DURATION: 1 Day

TARGET AUDIENCE

- Leaders in volatile
- Uncertain, or high-risk environments

LEARNING OUTCOMES

- Lead effectively in complex, unpredictable situations
- Make decisions under pressure with incomplete information
- Motivate teams during change or uncertainty
- Develop resilience and agility as a leader

COURSE OUTLINE

1 INTRODUCTION TO ADAPTIVE LEADERSHIP
- Principles, traits, and relevance

2 UNDERSTANDING COMPLEXITY AND UNCERTAINTY
- VUCA environments, systemic thinking

3 DECISION-MAKING UNDER PRESSURE
- Rapid analysis, prioritization, and risk tolerance

4 LEADING TEAMS THROUGH CHANGE
- Engagement, communication, and accountability

5 BUILDING PERSONAL AND ORGANIZATIONAL RESILIENCE
- Stress management, adaptability

6 CASE STUDIES & SCENARIO EXERCISES
- Nigerian or security-related crises

7 ACTION PLANNING
- Developing an adaptive leadership roadmap

7. TRANSFORMATIONAL LEADERSHIP

DURATION: 2 Days

TARGET AUDIENCE

- Managers
- Executives and
- Team leaders

LEARNING OUTCOMES

- Inspire and motivate teams toward a shared vision
- Drive performance and innovation through influence
- Foster a culture of continuous improvement
- Coach and develop emerging leaders

COURSE OUTLINE

1 INTRODUCTION TO TRANSFORMATIONAL LEADERSHIP
- Core principles and traits

2 VISION AND STRATEGY ALIGNMENT
- Creating purpose-driven goals

3 INFLUENCE AND MOTIVATION
- Emotional intelligence and engagement

4 COACHING AND MENTORSHIP
- Developing talent and succession planning

5 CREATING HIGH-PERFORMANCE CULTURE
- Values, accountability, and recognition

6 CASE STUDIES & ROLE-PLAY EXERCISES
- Transformational leadership in action

7 PERSONAL ACTION PLANNING
- Applying strategies to own team/organization

8. CRISIS LEADERSHIP AND DECISION MAKING

DURATION: 1 Day

TARGET AUDIENCE

- Executives
- Security professionals,
- Operations managers

LEARNING OUTCOMES

- Lead effectively during crises, emergencies, and high-stakes scenarios
- Make rapid, informed decisions under pressure
- Communicate clearly and maintain credibility in critical situations
- Coordinate teams and resources for effective crisis response

COURSE OUTLINE

1 INTRODUCTION TO CRISIS LEADERSHIP
- Principles, traits, and responsibilities

2 UNDERSTANDING CRISIS TYPES & IMPACT
- Operational, reputational, and human risks

3 DECISION-MAKING IN HIGH-PRESSURE ENVIRONMENTS
- Prioritization, rapid analysis

4 TEAM COORDINATION & COMMUNICATION
- Incident command, stakeholder management

5 SCENARIO-BASED EXERCISES
- Simulations of Nigerian or security-related crises

6 POST-CRISIS REVIEW & LEARNING
- Continuous improvement and resilience

7 ACTION PLAN
- Preparing personally and organizationally for crises

9. LEADING HIGH-PERFORMANCE TEAMS

DURATION: 1 Day

TARGET AUDIENCE

- Team leaders
- Managers, and
- Security supervisors

LEARNING OUTCOMES

- Build and sustain high-functioning teams
- Motivate, align, and engage team members
- Resolve conflicts and improve collaboration
- Monitor performance and drive results

COURSE OUTLINE

1 INTRODUCTION TO HIGH-PERFORMANCE TEAMS
- Traits, dynamics, and outcomes

2 TEAM BUILDING & ROLE CLARITY
- Roles, responsibilities, and accountability

3 MOTIVATION & ENGAGEMENT
- Recognition, feedback, and reward systems

4 CONFLICT RESOLUTION & COLLABORATION
- Techniques and interventions

5 PERFORMANCE MONITORING & CONTINUOUS IMPROVEMENT
- KPIs and team metrics

6 CASE STUDIES & TEAM EXERCISES
- Practical application

7 ACTION PLANNING
- Implementing strategies for team performance

10. INCLUSIVE LEADERSHIP & DIVERSITY MANAGEMENT

DURATION: 1 Day

TARGET AUDIENCE

- Executives,
- HR managers,
- Team leaders

LEARNING OUTCOMES

- Lead inclusively and leverage diverse perspectives
- Recognize and mitigate unconscious bias
- Promote collaboration and innovation through diversity
- Build culturally intelligent teams

COURSE OUTLINE

1 INTRODUCTION TO INCLUSIVE LEADERSHIP
- Principles and benefits

2 UNDERSTANDING DIVERSITY & BIAS
- Types, awareness, and mitigation

3 CULTURAL INTELLIGENCE IN LEADERSHIP
- Leading across backgrounds and experiences

4 COLLABORATION & INNOVATION
- Leveraging differences for results

5 CASE STUDIES & EXERCISES
- Inclusive leadership challenges in Nigeria

6 ACTION PLAN
- Strategies to lead inclusively in own team

11. LEADERSHIP IN VUCA (VOLATILE, UNCERTAIN, COMPLEX, AMBIGUOUS) ENVIRONMENTS

DURATION: 1 Day

TARGET AUDIENCE

- Executives,
- Operations Managers
- Security leaders

LEARNING OUTCOMES

- Navigate and lead in volatile and complex environments
- Make strategic decisions amid uncertainty
- Build resilient teams and adaptive processes
- Manage risk while maintaining performance

COURSE OUTLINE

1 UNDERSTANDING VUCA ENVIRONMENTS
- Context and challenges

2 STRATEGIC DECISION-MAKING UNDER UNCERTAINTY
- Risk analysis, scenario planning

3 LEADING RESILIENT TEAMS
- Adaptability, engagement, and empowerment

4 INNOVATION AND AGILITY
- Leveraging uncertainty for opportunity

5 CASE STUDIES & SIMULATIONS
- Nigerian operational or security contexts

6 ACTION PLAN
- Building personal and team resilience strategies

12. TRAINING COURSE: EFFECTIVE COMMUNICATION – ENHANCING CLARITY, INFLUENCE, AND IMPACT

DURATION: 1 Day

COURSE ONJECTIVE

Equip participants with the skills to communicate clearly, confidently, and persuasively, improving collaboration, decision-making, and professional influence.

TARGET AUDIENCE

- Professionals at all levels
- Team leaders, managers, and executives
- Security and investigative professionals
- Customer-facing staff and corporate communicators

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the principles of effective communication.
2. Adapt communication style to audience and context.
3. Communicate ideas clearly and concisely, both verbally and in writing.
4. Listen actively and respond empathetically.
5. Use persuasion and influence ethically to achieve outcomes.
6. Manage difficult conversations and conflicts professionally.

COURSE OUTLINE

1 FUNDAMENTALS OF COMMUNICATION

- Definition and components: verbal, non-verbal, and written communication
- Communication barriers and how to overcome them
- The communication process: sender, message, receiver, feedback
- Importance of clarity, tone, and context

2 AUDIENCE ANALYSIS & ADAPTATION

- Understanding your audience: expectations, knowledge, and perspective
- Adapting style for senior executives, peers, or teams
- Formal vs. informal communication channels
- Cultural and organizational considerations

3 ACTIVE LISTENING & EMPATHY

- Principles of active listening
- Empathetic communication and emotional intelligence
- Asking questions and giving feedback effectively
- Avoiding misunderstandings and assumptions

4 PERSUASION & INFLUENCE

- Principles of persuasion: credibility, logic, and emotion
- Storytelling and structuring persuasive messages
- Influencing without authority
- Negotiation and collaborative communication techniques

5 DIFFICULT CONVERSATIONS & CONFLICT MANAGEMENT

- Handling disagreements professionally
- Giving constructive feedback
- Managing emotions and maintaining professionalism
- Techniques for de-escalation and resolution

6 WRITTEN COMMUNICATION EXCELLENCE

- Clear, concise, and professional writing
- Email etiquette and effective reporting
- Structuring documents and presentations for maximum impact
- Avoiding ambiguity and misinterpretation

1. TIME MANAGEMENT & PRODUCTIVITY

DURATION: 1 Day

TARGET AUDIENCE

- Professionals at all levels
- Students or early-career individuals
- Team leaders and managers
- Anyone seeking to improve personal and professional productivity

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the principles of effective time management.
2. Identify personal productivity patterns and time-wasting habits.
3. Plan, prioritize, and schedule tasks efficiently.
4. Apply strategies and tools to increase focus and reduce procrastination.
5. Balance workload, deadlines, and personal goals for sustainable productivity.

COURSE OUTLINE

1 INTRODUCTION TO TIME MANAGEMENT

- Definition and importance of time management
- Common challenges and barriers: procrastination, distractions, poor planning
- The relationship between time management and productivity
- Self-assessment: understanding current time use and habits

2 PRIORITIZATION & GOAL SETTING

- Setting SMART goals (Specific, Measurable, Achievable, Relevant, Time-bound)
- Prioritization frameworks:
  - Eisenhower Matrix (urgent vs. important)
  - ABCDE method
- Aligning daily tasks with long-term goals

3 PLANNING & SCHEDULING TECHNIQUES

- Daily, weekly, and monthly planning methods
- Time-blocking and batching tasks
- Tools for planning: calendars, planners, digital apps
- Managing interruptions and maintaining focus

4 INCREASING FOCUS & MANAGING DISTRACTIONS

- Techniques to boost concentration: Pomodoro technique, single-tasking
- Handling digital distractions (emails, notifications, social media)
- Mindfulness and mental clarity practices for productivity
- Work environment optimization

5 DELEGATION & EFFECTIVE WORKLOAD MANAGEMENT

- Identifying tasks that can be delegated
- Principles of effective delegation
- Balancing workload to prevent burnout
- Collaborating with teams for shared productivity

6 REVIEWING & IMPROVING PRODUCTIVITY

- Measuring productivity and tracking progress
- Reflecting on time management effectiveness
- Continuous improvement: adjusting strategies based on outcomes
- Building sustainable productivity habits

2. CRISIS & CONFLICT RESOLUTION

DURATION: 2 Days

TARGET AUDIENCE

- Security personnel and crisis managers
- Corporate managers and team leaders
- HR professionals and organizational mediators
- Law enforcement and emergency response teams
- Professionals dealing with high-stakes negotiations or sensitive stakeholders

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the nature and types of crises and conflicts.
2. Identify early warning signs and potential escalation triggers.
3. Apply structured frameworks for resolving conflicts effectively.
4. Make informed decisions under pressure and manage high-stress situations.
5. Communicate clearly and empathetically during crises.
6. Develop proactive strategies to prevent recurrence of conflict.

COURSE OUTLINE

1 UNDERSTANDING CRISIS & CONFLICT

- Definition of crisis and conflict
- Types of crises: operational, reputational, security, financial, and natural
- Types of conflicts: interpersonal, organizational, community, and political
- The impact of unresolved conflicts on organizations and teams

2 CONFLICT ANALYSIS & EARLY DETECTION

- Understanding the root causes of conflict
- Recognizing escalation patterns and triggers
- Tools for conflict assessment: conflict mapping, stakeholder analysis
- The role of perception, emotion, and communication in conflict escalation

3 CRISIS MANAGEMENT FRAMEWORKS

- Crisis response cycle: preparation, response, recovery, and review
- Establishing a crisis management team and clear chain of command
- Decision-making under pressure
- Risk assessment and mitigation strategies

4 CONFLICT RESOLUTION STRATEGIES

- Communication skills: active listening, assertiveness, empathy
- Negotiation and mediation techniques
- Collaborative problem-solving
- De-escalation strategies for high-tension situations
- Ethical considerations in conflict resolution

5 CRISIS COMMUNICATION & STAKEHOLDER MANAGEMENT

- Internal and external communication during a crisis
- Managing rumors, misinformation, and stakeholder expectations
- Social media and media handling protocols
- Maintaining trust and credibility

6 POST-CRISIS EVALUATION & LEARNING

- Reviewing the response: what worked and what didn't
- Lessons learned and knowledge management
- Preventing recurrence: policy updates, training, and culture development
- Personal resilience and stress management

3. NAVIGATING WORKPLACE POLITICS

DURATION: 2 Days

TARGET AUDIENCE

- Professionals and team members at all levels
- Managers, supervisors, and leaders
- HR personnel and organizational development specialists
- Anyone seeking to manage workplace dynamics more effectively

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the nature and impact of workplace politics.
2. Identify informal networks, power structures, and influence dynamics.
3. Develop strategies to navigate politics ethically and strategically.
4. Communicate and collaborate effectively in politically charged environments.
5. Protect personal and team interests while maintaining credibility and professionalism.

COURSE OUTLINE

1 UNDERSTANDING WORKPLACE POLITICS

- Definition and common types of workplace politics
- The difference between negative and positive politics
- Sources of power: positional, personal, informational, relational
- Recognizing political behaviors and motives

2 MAPPING ORGANIZATIONAL DYNAMICS

- Identifying formal and informal networks
- Understanding stakeholders and influencers
- Recognizing power relationships and alliances
- Detecting “hidden agendas” without jumping to assumptions

3 STRATEGIES FOR ETHICAL NAVIGATION

- Building credibility and trust across teams
- Developing alliances and supportive networks ethically
- Managing conflicts and competing interests
- Avoiding pitfalls: gossip, manipulation, and reactive behaviors

4 COMMUNICATION & INFLUENCE

- Effective verbal and non-verbal communication in political environments
- Negotiation and persuasion techniques
- Managing sensitive conversations diplomatically
- Listening, observing, and adapting to organizational culture

5 PERSONAL RESILIENCE & CAREER PROTECTION

- Maintaining focus on personal goals and performance
- Stress management in politically charged environments
- Ethical self-advocacy
- Navigating promotions, assignments, and organizational change

4. SELF-MASTERY FOR HIGH PERFORMANCE

DURATION: 2 Days

TARGET AUDIENCE

- Professionals and corporate leaders
- Entrepreneurs and executives
- High-potential employees and team leaders
- Security and investigative professionals
- Anyone seeking to improve personal discipline, focus, and results

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the principles of self-mastery and high performance.
2. Manage time, energy, and focus for optimal results.
3. Develop emotional regulation and resilience under pressure.
4. Set and achieve meaningful goals consistently.
5. Build habits and mindsets that sustain long-term high performance.

COURSE OUTLINE

1 INTRODUCTION TO SELF-MASTERY

- Definition and importance of self-mastery
- Key traits of high performers: discipline, focus, resilience, emotional intelligence
- The relationship between mindset, behavior, and results

2 GOAL SETTING & PERSONAL VISION

- The role of vision and purpose in high performance
- SMART goals and stretch goals
- Aligning daily actions with long-term objectives
- Prioritization frameworks to maximize impact

3 MANAGING ENERGY, FOCUS & TIME

- Techniques to improve focus and reduce distractions
- Energy management: physical, mental, and emotional
- Time management strategies for peak performance
- Overcoming procrastination and decision fatigue

4 EMOTIONAL REGULATION & RESILIENCE

- Recognizing triggers and managing stress
- Techniques for emotional regulation under pressure
- Developing a resilient mindset to navigate setbacks
- Mindfulness, visualization, and reflective practices

5 BUILDING HIGH-PERFORMANCE HABITS

- Habit formation and reinforcement strategies
- Daily routines and rituals for success
- Accountability and tracking progress
- Self-motivation and sustaining momentum

6 REVIEW & PERSONAL ACTION PLAN

- Recap of key concepts and strategies
- Developing a personalized self-mastery roadmap
- Peer discussion and sharing actionable commitments

5. THE 7 HABITS OF HIGHLY EFFECTIVE PEOPLE: APPLICATION FOR PERSONAL DEVELOPMENT

DURATION: 2 Days

TARGET AUDIENCE

- Professionals at all levels
- Managers, team leaders, and executives
- Students and emerging leaders
- Anyone seeking personal growth, productivity, and leadership skills

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the 7 habits and their principles.
2. Apply these habits to increase personal effectiveness and productivity.
3. Improve relationships and communication through empathy and collaboration.
4. Develop proactive, goal-oriented, and principle-centered behaviors.
5. Create a personal action plan to integrate these habits into daily life.

COURSE OUTLINE

INTRODUCTION TO THE 7 HABITS 1

-Overview of the habits and the philosophy of effectiveness

-Character vs. personality ethics

-The Maturity Continuum: dependence → independence → interdependence

-The importance of principles and values

HABIT 1 – BE PROACTIVE 2

-Taking responsibility for actions, responses, and decisions

-Focus on circle of influence vs. circle of concern

-Choosing responses instead of reacting to circumstances

HABIT 2 – BEGIN WITH THE END IN MIND 3

-Defining personal and professional vision

-Goal setting aligned with values and mission

-Visualization and mental rehearsal of desired outcomes

HABIT 3 – PUT FIRST THINGS FIRST 4

-Time management and prioritization

-Quadrant II focus: urgent vs. important

-Planning and execution strategies to align actions with goals

HABIT 4 – THINK WIN-WIN 5

-Developing an abundance mindset

-Seeking mutually beneficial solutions in work and relationships

-Balancing courage and consideration in negotiations

HABIT 5 – SEEK FIRST TO UNDERSTAND, THEN TO BE UNDERSTOOD 6

-Active listening and empathy

-Improving communication by understanding perspectives

-Managing disagreements constructively

HABIT 6 – SYNERGIZE 7

- Value of teamwork and collaboration

- Leveraging differences to create better solutions

- Creative problem-solving through synergy

HABIT 7 – SHARPEN THE SAW 8

- Continuous self-improvement in four dimensions: physical, mental, emotional/social, spiritual

- Work-life balance, stress management, and lifelong learning

- Building habits for sustainability and resilience

6. NAVIGATING A COMPLEX TEAM FOR EFFECTIVE DELIVERY

DURATION: 2 Days

TARGET AUDIENCE

- Team leaders and managers
- Project managers and coordinators
- Leaders of cross-functional or remote teams
- Professionals managing diverse teams or multi-stakeholder projects

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the dynamics and challenges of complex teams.
2. Identify individual and group strengths, roles, and motivations.
3. Build cohesion, trust, and effective collaboration.
4. Manage conflicts, competing priorities, and organizational politics.
5. Drive team performance and achieve project objectives efficiently.

COURSE OUTLINE

1 UNDERSTANDING COMPLEX TEAMS

- Definition of a complex team: diversity, structure, and interdependencies
- Challenges in complex teams: communication, conflicting priorities, cultural differences
- The importance of psychological safety and trust for effective delivery
- Identifying key stakeholders, roles, and influencers within the team

2 BUILDING TEAM COHESION & TRUST

- Principles of high-performing teams
- Trust-building strategies: transparency, reliability, and accountability
- Encouraging open communication and mutual respect
- Understanding and leveraging team diversity (skills, experience, culture)

3 COMMUNICATION & COLLABORATION STRATEGIES

- Clear and consistent communication in complex environments
- Active listening and feedback mechanisms
- Collaboration tools and processes for cross-functional teams
- Managing remote, hybrid, and multi-location teams

4 CONFLICT MANAGEMENT & PROBLEM-SOLVING

- Recognizing sources of conflict: role ambiguity, resource competition, personality differences
- Conflict resolution frameworks and negotiation techniques
- Collaborative problem-solving and consensus-building
- Turning conflict into opportunity for innovation

5 DRIVING TEAM PERFORMANCE & ACCOUNTABILITY

- Setting clear goals, KPIs, and expectations
- Delegation and task alignment according to skills and capacity
- Monitoring progress, providing feedback, and course correction
- Celebrating wins and reinforcing team motivation

6 LEADING COMPLEX TEAMS IN PRACTICE

- Adaptive leadership and decision-making
- Managing stakeholders' expectations
- Balancing short-term delivery pressure with long-term team development
- Continuous improvement and learning culture

7. PERSONAL MASTERY – UNLOCKING YOUR POTENTIAL FOR PEAK PERFORMANCE

DURATION: 2 Days

COURSE OBJECTIVE:

Enable participants to develop self-awareness, discipline, emotional intelligence, and intentional habits that drive personal and professional growth.

TARGET AUDIENCE

- Professionals and corporate leaders
- Entrepreneurs and high-potential employees
- Security and investigative professionals
- Anyone seeking self-improvement, focus, and personal effectivenesss

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the principles and importance of personal mastery.
2. Develop self-awareness to identify strengths, weaknesses, and limiting beliefs.
3. Cultivate focus, discipline, and self-regulation.
4. Set meaningful personal and professional goals aligned with values.
5. Create habits and routines that reinforce continuous growth.
6. Build resilience, adaptability, and a growth mindset.

COURSE OUTLINE

1 INTRODUCTION TO PERSONAL MASTERY

- Definition and importance of personal mastery
- The link between self-mastery, personal growth, and professional success
- Core areas: mindset, habits, focus, and emotional intelligence

2 SELF-AWARENESS & MINDSET

- Principles of high-performing teams
- Trust-building strategies: transparency, reliability, and accountability
- Encouraging open communication and mutual respect
- Understanding and leveraging team diversity (skills, experience, culture)

3 GOAL SETTING & FOCUS

- Clarifying purpose and personal vision
- SMART and stretch goals
- Prioritization and focus strategies
- Time and energy management for high performance

4 HABIT FORMATION & DISCIPLINE

- The science of habit formation
- Daily routines and rituals for success
- Overcoming procrastination and distractions
- Accountability and tracking progress

5 RESILIENCE, ADAPTABILITY & GROWTH

- Developing adaptability and problem-solving skills
- Learning from failure and continuous improvement
- Strategies for long-term growth and sustainability

6 INTEGRATION & ACTION PLANNING

- Recap of principles and practices
- Developing a personal action plan for ongoing mastery
- Commitment to continuous reflection and self-improvement

8. CONFIDENCE BUILDING FOR PERSONAL DEVELOPMENT

DURATION: 2 Days

COURSE OBJECTIVE:

Enable participants to develop self-confidence, overcome limiting beliefs, and leverage personal strengths for professional and personal growth.

TARGET AUDIENCE

- Professionals and corporate leaders
- Entrepreneurs and high-potential employees
- Security, investigative, and field professionals
- Anyone seeking to improve self-confidence and personal growth

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the role of confidence in personal and professional development.
2. Identify internal and external barriers to self-confidence.
3. Develop strategies to enhance self-belief and assertiveness.
4. Practice techniques for public speaking, decision-making, and interpersonal interactions.
5. Build resilience and manage self-doubt effectively.
6. Apply confidence-building strategies to achieve personal and career goals

COURSE OUTLINE

1 UNDERSTANDING CONFIDENCE

- Definition and importance of self-confidence
- The relationship between confidence, self-esteem, and personal growth
- Differentiating authentic confidence from arrogance
- Common barriers to confidence: fear, negative self-talk, and past experiences

2 SELF-AWARENESS & STRENGTH IDENTIFICATION

- Understanding your strengths, talents, and achievements
- Recognizing skills and capabilities that enhance confidence
- The role of mindset in self-belief: fixed vs. growth mindset

3 OVERCOMING SELF-DOUBT & LIMITING BELIEFS

- Identifying negative thoughts and cognitive distortions
- Techniques for reframing and positive self-talk
- Visualization and mental rehearsal for confidence
- Managing fear of failure and fear of judgment

4 BUILDING ASSERTIVENESS & EFFECTIVE COMMUNICATION

- The difference between assertive, passive, and aggressive behavior
- Techniques for expressing ideas and opinions confidently
- Non-verbal communication, body language, and voice modulation
- Handling difficult conversations with composure

5 PUBLIC PRESENCE & PRESENTATION SKILLS

- Overcoming nervousness in public speaking
- Structuring clear and confident presentations
- Engaging the audience with authenticity
- Using storytelling and examples to strengthen credibility

6 RESILIENCE & SUSTAINING CONFIDENCE

- Building emotional resilience to setbacks
- Maintaining confidence during challenges and high-pressure situations
- Continuous learning and skill development to reinforce self-belief
- Accountability and habit formation for ongoing growth

9. PRE-RETIREMENT PLANNING – PREPARING FOR A SECURE AND FULFILLING FUTURE

DURATION: 2 Days

COURSE OBJECTIVE:

Enable participants to plan effectively for retirement by addressing financial, emotional, health, and lifestyle aspects, ensuring a smooth transition and continued personal fulfillment.

TARGET AUDIENCE

- Employees approaching retirement (typically 5–10 years before planned retirement)
- Middle and senior-level professionals
- HR managers and corporate wellness coordinators
- Anyone seeking a structured approach to retirement planning

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the key aspects of retirement planning: financial, emotional, health, and lifestyle.
2. Assess their current financial situation and retirement readiness.
3. Develop strategies to secure income and manage finances post-retirement.
4. Explore lifestyle, health, and personal development options for retirement.
5. Plan for emotional and social adjustments during the transition.
6. Create a personalized pre-retirement action plan.

COURSE OUTLINE

1 INTRODUCTION TO RETIREMENT PLANNING

- Understanding retirement and its significance
- Common challenges during retirement: financial, social, and emotional
- Planning horizon and the importance of starting early
- Overview of retirement planning components: finance, health, lifestyle, and personal growth

2 FINANCIAL PLANNING FOR RETIREMENT

- Assessing current financial status: assets, liabilities, savings, and investments
- Retirement income planning: pensions, savings, investments, and other income streams
- Budgeting for retirement and managing expenses
- Risk management: inflation, healthcare costs, and unforeseen emergencies

3 HEALTH & WELLNESS PLANNING

- Importance of physical and mental health for a fulfilling retirement
- Preventive healthcare and regular check-ups
- Stress management and maintaining cognitive function
- Lifestyle changes to enhance longevity and quality of life

4 EMOTIONAL & SOCIAL PREPARATION

- Coping with identity changes and loss of work structure
- Maintaining social connections and building community networks
- Volunteerism, hobbies, and personal growth opportunities
- Planning for purposeful and fulfilling activities post-retirement

5 LEGAL AND ADMINISTRATIVE CONSIDERATIONS

- Wills, trusts, and estate planning
- Health directives and power of attorney
- Retirement benefits and entitlements
- Tax considerations for retirees

6 DEVELOPING A PERSONAL PRE-RETIREMENT PLAN

- Integrating financial, health, emotional, and lifestyle components
- Setting short-term and long-term goals
- Creating milestones and action steps
- Accountability and review mechanisms

10. SITUATIONAL AWARENESS FOR DRIVERS

DURATION: 1 Days

TARGET AUDIENCE

- Professional drivers (chauffeurs, delivery drivers, security drivers)
- Corporate drivers and fleet operators
- Law enforcement and security personnel
- Anyone who wants to improve driving safety and awareness

LEARNING OBJECTIVES

By the end of this Course, participants will be able to:

1. Understand the principles of situational awareness (SA) and its importance for driving safety.
2. Recognize common hazards and risk factors on the road.
3. Apply techniques to anticipate, identify, and respond to potential threats or hazards.
4. Maintain focus and attention under varying driving conditions.
5. Integrate situational awareness into daily driving routines for accident prevention.

COURSE OUTLINE

1 INTRODUCTION TO SITUATIONAL AWARENESS

- Definition of situational awareness in driving
- Levels of SA: perception, comprehension, projection
- Importance of SA in preventing accidents and reacting to emergencies
- Human factors affecting SA: fatigue, stress, distractions

2 HAZARD RECOGNITION & RISK ASSESSMENT

- Identifying static and dynamic hazards:
  - o Road conditions, weather, traffic patterns
  - o Pedestrians, cyclists, other drivers
  - o Unexpected events: accidents, roadblocks, animals
- Risk assessment techniques: probability, severity, and exposure
- Understanding common accident causes: speed, distraction, misjudgment

3 OBSERVATION & ATTENTION TECHNIQUES

- Using mirrors, scanning, and peripheral vision effectively
- Maintaining proper distance and speed management
- Anticipating the actions of other road users
- Avoiding tunnel vision and distractions

4 DEFENSIVE DRIVING & THREAT RESPONSE

- Principles of defensive driving: anticipation, space management, and braking techniques
- Responding to threats: sudden stops, evasive maneuvers, aggressive drivers
- Maintaining composure and decision-making under stress
- Vehicle checks and pre-driving routines for safety

5 INTEGRATING SITUATIONAL AWARENESS INTO DAILY DRIVING

- Creating personal routines and checklists for SA
- Maintaining alertness during long drives or night driving
- Using technology effectively without distraction (GPS, cameras, sensors)
- Continuous improvement: reflection, feedback, and practice

SIVRIL

SPECIAL PROGRAMS

- Executive Coaching & Corporate Retreats
- Goal Setting & Vision Board Workshops
- Customized Security & Forensic Training
- Staff orientation Programs for organizations
- Fire Fighting & Fire Awareness Programs
- Defensive & Offensive Driving
- First Aid & Emergency Response Program
- Youth Mentorship Programs
- Customized Team Bonding for Security Departments
- Conference presentation

Diploma Courses in collaboration with the University of Lagos, Akoka

1. Diploma in Crime Scene Management
2. Diploma in Security Governance and crisis management
3. Diploma in Private Investigation.

FACULTY

ELITE FACULTY | GLOBAL PERSPECTIVE | OPERATIONAL EXCELLENCE

SIVRIL's facilitators represent a distinguished network of senior professionals with proven expertise in security operations, forensic investigations, intelligence analysis, leadership development, and organizational resilience.

With experience spanning international agencies, critical infrastructure protection, corporate governance, and complex investigations, our faculty delivers instruction rooted in real-world decision-making and contemporary global challenges.

Every program is facilitated by practitioners who understand operational pressure, ethical responsibility, and strategic leadership, ensuring participants develop competence, confidence, and credibility in their professional roles.

CERTIFICATION & RECOGNITION

- All participants are awarded a certificate upon completion of each program.
- Selected courses attract ASIS CPE points and professional development credits.
- Designated programs also offer an additional joint certification in collaboration with the
- University of Lagos (UNILAG), Akoka.

MODE OF LEARNING

- Virtual Delivery – Interactive live online instruction
- Onsite Classroom Delivery – Facilitated in-person learning experience
- Hybrid Delivery – Blended virtual and physical learning mode

TRAINING VENUE

Trainings may be conducted at:

- **SIVRIL Facilities –** Mainland or Island, Lagos
- **Offsite Venues** – Within or outside Lagos and Nigeria, sourced by SIVRIL or the client
- **Client Premises** – On-site corporate delivery
- **Virtual Platforms** – Live online training sessions

WHY CHOOSE SIVRIL

INDUSTRY-LED FACULTY – Programs are delivered by seasoned practitioners with real-world operational and leadership experience across security, investigations, intelligence, and risk management.

GLOBAL STANDARDS, LOCAL RELEVANCE – Our curriculum aligns with international best practices while addressing regional realities and operational challenges.

PRACTICAL, HANDS-ON LEARNING – Scenario-based training, case studies, simulations, and applied exercises ensure immediate workplace impact.

PROFESSIONAL RECOGNITION – Selected programs attract ASIS CPE points and co-issued certifications with the University of Lagos (UNILAG), Akoka.

FLEXIBLE DELIVERY MODELS – Virtual, classroom, hybrid, onsite, and international delivery options tailored to organizational needs.

CUSTOMIZED CORPORATE SOLUTIONS – Bespoke training designed around your operational risks, organizational objectives, and industry environment.

INVESTMENT COST

Program Fees:

Fees vary based on course type, duration, delivery mode (in-person / virtual), customization level, and participant volume.

- Individual Courses
- Corporate & Group Training
- Executive & Specialized Programs
- Custom Training Solutions

For detailed pricing, group discounts, and corporate packages, please contact: info@sivrilinstitute.com or sivrilinstitute@gmail.com

EARLY REGISTRATION DISCOUNTS AND CORPORATE PARTNERSHIP RATES AVAILABLE

CONTACT US

SIVRIL TRAINING INSTITUTE & CENTRE FOR LEADERSHIP DEVELOPMENT

Lagos, Nigeria | Online Worldwide

+2348137412120, +2349062072117 **@SIVRIL.institute**

Email: info@sivrilinstitute.org, sivrilinstitute@gmail.com

M O T T O : L E A R N . L E A D . S U C C E E D .