

Information Security & Cyber Security Fundamentals Course

2027 0000 5 - 1
Paris (France)

UK Traininig

PARTNER





Day 2: Network and Infrastructure Security

- Network security architecture and protocols
- Firewalls, IDS/IPS, and VPN implementation
- Cloud security and virtualization considerations
- Securing wireless networks and remote access

Day 3: Application and Data Security

- Secure software development lifecycle SDLC
- Web application security best practices
- Cryptography, encryption, and key management
- Database protection and data privacy measures

Day 4: Identity and Access Management

- Authentication methods, including multi-factor authentication
- Access control models and implementation strategies
- Privileged access management PAM
- Identity governance and compliance frameworks

Day 5: Security Operations and Incident Response

- Security information and event management SIEM tools
- Incident detection, response, and reporting processes
- Digital forensics and investigative techniques
- Business continuity and disaster recovery planning

Individual Impact

Participants will leave the program with:

- Practical skills to conduct security assessments and risk analysis
- Ability to implement fundamental security controls in diverse IT environments
- Knowledge to develop and execute incident response and continuity plans
- Enhanced understanding of cybersecurity best practices to protect organizational assets

Organizational Impact

Organizations will benefit through:

- Strengthened information security posture and reduced risk exposure
- Improved preparedness for cyber incidents and operational disruptions
- Enhanced compliance with legal, regulatory, and ethical standards
- Greater confidence in managing and protecting critical IT assets

A graphic of a chessboard with several chess pieces (king, queen, rook, knight, and pawns) in gold and silver. The word 'PARTNER' is written in large, bold, black letters across the board, with 'UK Training' in smaller text above it.

UK Training
PARTNER

Training Methodology

This course emphasizes practical, hands-on learning through:

- Real-world cybersecurity scenarios and simulations
- Exercises in risk assessment and security control implementation
- Incident response and digital forensics workshops
- Group discussions on ethical, legal, and regulatory challenges

Beyond the Course

Upon completion, participants will be able to:

- Identify and mitigate cyber threats proactively
- Implement effective security controls across the organization
- Develop and maintain incident response and business continuity plans
- Contribute to building a culture of cyber awareness and resilience

This program provides a practical pathway for IT professionals and managers to enhance cyber security capabilities, safeguard organizational assets, and respond confidently to the challenges of today's digital landscape.

A graphic of a chessboard with several chess pieces (a king, a queen, and a pawn) on it, set against a background of concentric circles.

UK Training
PARTNER