Global Leaders in Cyber, Intelligence and Training.

EXCEPTIONAL PEOPLE. CUTTING-EDGE CAPABILITIES.
Welcome to the PGI Cyber Academy

In 2014, we launched PGI’s world class Cyber Academy to complement our Cyber Security service delivery capabilities. Our cyber solutions for government and corporate clients had to acknowledge the critical roles that knowledge, skills and research play in countering the breadth of the malign activity that represents the “Cyber Threat.” We understood that helping our clients develop their own staff to respond to the threat would play as vital a role in managing it as the provision of services.

Our 15,000 square foot state of the art ‘flagship’ facility in Bristol was specifically designed to create an environment to reduce the cyber skills shortage among industry professionals. Alongside PGI’s exceptional UK Cyber Academy, its capabilities encompass advanced training courses and scenario exercises that can be delivered internationally, fulfilling the demands of a global skills gap. Our aim is to create awareness, understanding, provide education to those that need it, and to preserve the UK’s international reputation as a leading Cyber Security nation.
Brian Lord OBE
Managing Director, PGI Cyber

Brian joined PGI in September 2013, after 21 years with GCHQ as their Deputy Director for Intelligence and Cyber Operations. Brian served in a wide range of roles for GCHQ, at home and abroad, and has deep understanding drawn from many years’ experience across the breadth of Intelligence and Cyber Operations. He is a leading thinker in the area of Cyber Warfare.
The modern world faces a variety of evolutionary threats which outstrip the capability of nations and corporations. The PGI Cyber Academy is playing a major role in reversing this trend by helping its clients understand the threats and respond at the same speed by:

- Building the knowledge of leaders – government and corporate to enable them to build manageable, affordable strategies and policies supported by the right levels of investment in the right capabilities at the right time
- Building national capability development and transfer programmes for several of the UK’s closest allies
- Developing global enterprise risk management programmes for blue-chip corporations and small to medium sized enterprises
- Transforming and growing national and organisational workforces that can operate safely, effectively and efficiently in the networked world
- Training and certifying new and existing specialists working in the cyber security field alongside senior executives, management and IT staff
- Continuing to grow the numbers of skilled people within the UK’s national defence and security organisations
- Developing specialist cybercrime training for UK and other law enforcement agencies
- Providing new entrants with multiple routes into a recognised, sustainable Cyber Security profession that grows and adapts to the nature of the threat; keeping the public and private institutions of the UK and its allies safe
- Educating and advising to help the public and small businesses live and trade securely in a digital world.
PGI Cyber Academy offers its clients:

• A world class training environment – the only one of its kind in Europe
• Operational trainers who continue to work in cyber operations teams alongside their training roles and ‘practicing what they teach’
• A fully immersive ‘sandboxed’ training and research environment: making the impossible possible
• Rigorous industry recognised certification under GCHQ’s Certified Training scheme
• A PGI Cyber Academy network, connecting alumni with peers across the industry.

“I am proud to introduce you to the Cyber Academy, which is always achieving remarkable things.”

Brian Lord OBE
Managing Director, PGI Cyber
Professor Brian Brivati  
**Academic Director, PGI Cyber Academy**

Brian joined the PGI Cyber Academy in 2014 and was formerly the Academic Director of the John Smith Trust and Beyond Borders, Scotland. He is a specialist in designing and delivering professional development, leadership, policy transformation and bespoke training programmes for government, NGOs, the private sector and overseas clients. Brian has been a senior policy adviser to politicians and civil servants from a range of countries across the Middle East and Eastern Europe. He has written or edited fourteen books on contemporary historical and political themes. Previously, he was Professor of Human Rights at Kingston University.
Teaching and Learning Strategy

Technology enabled crime represents a threat to virtually all aspects of the way we live today. Think about the layers of dependency on technology our lives entail:

- **Daily Life** – from our mobile phones to online shopping, from travel to the internet of things, we use technology from morning to night
- **Economic Life** – our jobs and livelihoods are dependent on the protection of our information systems either directly, because of what we do for a living, or indirectly through the banking and welfare systems
- **Community Life** – the critical infrastructure of our towns and cities, and the way we live together in communities, are technologically enabled
- **States** – the organisation of our countries, government, tax, health, education and the defence of our strategic critical infrastructure are all targets because they all function through, with and in cyberspace.

All of these threats are constantly changing and evolving. Cyber Crime amounts to a new criminal superpower on the world stage. The gap between the structural threats from this superpower and our capacity to defend ourselves is the Cyber Gap. It is this gap that the Cyber Academy is working hard to fill for our UK and international clients. Given the nature of the threat and the demand for experts, the teaching and learning strategy of the Academy has to allow for continuous adaptation to new threats based on new knowledge and thinking.
Teaching that is Experiential and Research Based

PGI’s Cyber Academy courses are designed and delivered by experienced and qualified operational staff. Our trainers are widely regarded as some of the most respected cyber trainers in the UK. They are drawn from backgrounds including UK Government, law enforcement and military alongside commercial colleagues with backgrounds in central government, telecommunications and finance. All have actively managed research time to allow them to keep ahead of the fast changing cybercrime environment. Our teaching model is based on experiential delivery derived from our active research and our practice-based team. Everything that happens in the classroom is based on the training team’s direct experience of delivering cyber security solutions for our clients.
Technology that is the Best in the World

The learning environment in the Academy is immersive. We offer a powerful virtual network to support a hands-on approach to the learning process. It is a vast electronic sandbox for real-time application of learning to reality.
We teach the actions that are necessary to achieve the results our clients require. The single loop learning cycle informs many of the courses that we run; learning that is needed to raise awareness of the threats that exist and that we know about, and to influence behaviour in ways that produce better protection. These courses allow us to use the tools we have better, and to meet the key performance indicators that allow greater protection and understanding of the threat environment. In our more advanced courses, we aim for double loop learning. This entails working with the trainers to explore what we do not know, to think through what the next threat might look like, and question the assumptions on which our approach is based. Single loop learning is based on learning through doing on our state of the art network. The double loop learning takes this one stage further and encourages experimentation in the application of knowledge.
Certified as the Best

PGI’s Cyber Academy works closely with the GCHQ Certified Training (GCT) scheme which provides an industry recognised benchmark for cyber security training by assuring the course content quality and delivery. The majority of our courses are accredited under the GCT scheme. We also work with our University partners to provide academic qualifications and routes to higher degrees through credit transfer schemes where these are desired by students.

Professor Brian Brivati
Academic Director, PGI Cyber Academy
Building National Capability

Providing countries with the cyber skills and training infrastructure to meet their own national cyber security priorities.

To combat proliferating cyber threats, governments are creating and expanding cyber units in their security, intelligence, defence and law enforcement agencies. The PGI Cyber Academy has been developed to support this activity. We have a proven track record of delivering training for UK and international law enforcement agencies, security services, armed forces, and other government departments. We are currently working for multiple government clients in four continents to help build their national capabilities.

“The UK offers unrivalled training and education to build long-term cyber security capability.”

UK Government’s ‘Your security in safe hands brochure’, featuring PGI as the training provider.

The large team of senior and experienced PGI Cyber Academy staff has been recruited from UK government, intelligence, defence and critical national infrastructure backgrounds. They have deep and extensive experience of creating national cyber structures, teams, career plans and exercises. Our training infrastructure was designed for and has been extensively used by, some of the world’s largest and most advanced cyber agencies.
This allows us to support our clients in:

- Building national cyber leaders and strategy development capability
- Running cyber exercises
- Building the capability and capacity of national cyber units at speed and scale
- Designing bespoke programmes, tuned to address current national requirements and priorities
- Realising the benefits of technology investment through developing skilled operators.
Capability Transfer

Building national cyber security capability is too important a role to be left indefinitely to an external provider. Designing capability transfer to the client country into all of our long-term programmes is a fundamental principle for PGI.

We do this through a combination of:

- Design and delivery of training environments
- Trainer training
- Developing national curriculums and accreditations.

PGI’s approach is flexible. We will provide training in the UK or in the host country as required. Our preferred model, however, is to work with our government clients – and their existing partners – to replicate the successful PGI Cyber Academy model and infrastructure locally. We create training programmes – by identifying the most appropriate training courses that are available on the commercial market, and combining them with purpose-built courses that fill specific gaps – build the training infrastructure and train the trainers to deliver them. In this way, we create national cyber training assets with the technical and academic capability to meet government and critical national infrastructure requirements.
Recent Examples of our Work

Building a Cyber Policy Fellowship to combine cyber leaders and individuals with leadership potential from across the Middle East into a regional network. The fellowship aims to understand and connect best practice, and work on white papers covering legal frameworks, organisational roles and national skills development.

Developing cyber security professionals for a new national unit; we designed and delivered a 15-week modular training programme which included a combination of theory, hands-on exercises and practical experience across the core cyber skills, which identified trainees with special aptitude for specialist extension classes.

An intensive training programme for police officers in a newly formed cybercrime unit to supplement existing police academy training with modules on current cybercrime trends and how to investigate them.

Bespoke cyber intelligence training for an intelligence unit which had invested in a cyber intelligence toolset from a 3rd party provider and needed officers to be trained in new investigative techniques before they could use it effectively.

Running a national-level cyber exercise with government agencies and critical infrastructure providers. This measured current cyber response mechanisms against international best practice, identified gaps and informed the national strategy development process.
Corporate Cyber Education

Normalising the threat, and managing it alongside other corporate risks.

PGI’s qualified trainers and certified training provide the clarity and balanced approach that allow companies to manage cyber risks alongside every other corporate risk as part of their risk management approach. PGI’s approach recognises that managing the cyber security risk is simply an on-going cost of doing business in the 21st century.

PGI delivers the three fundamental components of corporate cyber training and education:

- A leadership that understands cyber risk, sets the right organisational culture and invests proportionately
- A workforce and supply chain that applies their understanding of the threat into day to day behaviours and responsibilities
- A technical workforce that operates technological business tools securely and effectively.

“Industry’s perception of the cyber risk remains extremely variable. Companies struggle to interpret what the real business risks are when the threat is poorly explained by government, exaggerated or rendered unintelligible by the information security and risk industry, and complicated by sensationalist and inconsistent media reporting. Increasing levels of governance and regulation add to the churn of awareness. Education, knowledge and skills are the most effective defence to countering the cyber threat.”

Brian Lord OBE
Managing Director, PGI Cyber
Cyber risks and training needs vary considerably according to an organisation’s size, sector and geographical distribution. Training an organisation to react or manage cyber vandalism is very different to educating boards in avoiding falling victim to corporate espionage. The PGI Cyber Academy trains organisations of all sizes – from international corporations to small and medium-sized businesses – and ensures that the training time for each is used as efficiently as possible. We select and tailor course material to ensure that it focuses only on risks and methodologies that are relevant to the client’s needs.
Leadership Education

We educate business leaders to make the correct investment decisions to effectively manage the risk and develop embedded cyber-aware cultures. By implementing this philosophy, businesses have been shown to reduce the threat by as much as 80%. PGI’s certified leadership training has been used by the global boards of banks, critical national infrastructure and defence providers, as well as retail and insurance clients.

PGI’s Board Training is designed for a desired duration and delivered in an environment stipulated by our client. This bespoke training is designed using jargon-busting content that includes:

• Material tailored specifically to the client’s sector and nationality
• Distinction between reality and hyperbole – facilitating sensible and relevant risk management dialogue
• Language and style appropriate to business or department, not technology – allowing identified risk to be quantified
• Context around sociological and geopolitical aspects of the threat – informing both international business engagement, as well as varying workforce demographics.

“Probably the most informative, easy to understand, business-relevant and balanced education on any type of threat I have ever experienced”

Head of UK Defence Company
In addition to Board level education, PGI also delivers Cyber Awareness Courses for Executives and Managers. These provide the same levels of comprehension as the Board Training, supplemented by specific training on tools and policies that manage cyber risks, and guidance on implementing cyber security cultural awareness within a workforce, and on developing tools and policies to manage the risk and legal accountabilities in the different areas of business.

Each of these courses carries the level of UK Government certification that provides assurance that the training and education has been delivered to the appropriate, contemporary standards.

“All UK Cyber Security businesses certified by CESG have been rigorously assessed and independently evaluated by the UK Government”

UK Government’s ‘Your security in safe hands brochure’
Workforce Education

For most organisations, users represent the greatest cyber security risk yet, typically, mass security training is either neglected or ineffective. To address this, the PGI Cyber Academy has developed a range of workforce training based on best practice techniques identified through decades of scientific study by our partners at University College, London. These have identified that security training is only effective if it is both highly realistic and relevant to the audience. We, therefore, design our courses for targeted groups of recipients and focus on threats and vulnerabilities that are relevant to them – either in their role at work or in their personal life – so that the courses have immediate, measurable, impact and drive behavioural change. These courses are delivered using a combination of interactive tools and corporate communications vehicles.
Building a Specialist Technical Workforce

The PGI Cyber Academy specialises in building its clients a cyber security workforce. This includes:

- The education and upskilling of an existing cyber security workforce
- Identifying and creating additional cyber security professionals from elsewhere within the business
- The recruitment, retention and management of cyber professionals.

Our workforce solutions are flexible and designed to reflect the needs of each client’s organisation. Our courses and programmes allow businesses to use training models that best reflects their business objectives and the corporate and risk environment in which they operate.

Throughout PGI’s Cyber Academy work, our courses and training facilities have been designed to provide the most effective learning environment. While the majority of our courses are delivered at the Academy, we can also deliver training wherever requested by our clients.

All PGI Cyber Academy Courses have bespoke elements that can be tailored to specific business objectives and deliverables. Our teaching methods include e-learning packages, board briefings and immersive ‘war gaming’ exercises. All our courses are designed and delivered in line with the specific nature of the threat to the industry or business in question.
Creating and Developing Cyber Professionals

“The evolution of the Cyber Threat has far outstripped the normal demographic trends in education”

Professor Brian Brivati
Academic Director, PGI Cyber Academy

Traditional academia and professional education are struggling to keep up with the fast paced developments in the cyber threat. This has resulted in a significant skills shortage – it is now estimated that there are up to two million unfilled cyber security roles globally.
The PGI Cyber Academy is helping to close this skills gap by identifying and building cyber security professionals at scale and equipping them with the skills, experience and credentials that they need to fill cyber security roles in government, industry and academia.

It does this through:

• Supporting initiatives such as The Cyber Security Challenge that are designed to attract people into cyber security careers
• Assessing individuals for potential and aptitude in cyber security roles and advising them on suitable career streams
• Providing entry level training for people changing career into cyber security
• Developing structured career pathways for cyber security professionals
• Providing continuing professional development training for staff in technical assurance and policy roles.
PGI’s training for cyber security professionals is created and delivered on an evolutionary basis. This recognises the constantly changing threats, vulnerabilities and societal attitudes to risk and security as well as the needs of the market, individual and industry. It is underpinned by PGI’s innovative models for learning and course development ensure that course materials and trainers are continually kept current and reflect this in their training.

The PGI Cyber Academy gives its alumni the competitive advantage they need in a fast paced industry. Our course accreditations ensure that our graduates are recognised and rewarded as the best in their profession and ensures that their careers can survive and thrive in the digital age.

Recent Examples of our Work

- Helping individuals seeking to move into cyber security roles develop their careers through our cyber security education pathways

- Assisting employees in technical assurance and related roles grow their skills to support business objectives and new service lines

- Giving graduates, who are looking to take their first steps in their chosen career, real world knowledge from trainers with current operational experience.
“Our goal is for PGI Cyber to employ the best trainers, and offer the best courses – whether PGI’s own or from other world-leading cyber training companies – from the best training facilities in the world. To support this, we require our trainers, our course materials and our facilities to meet the highest standards of external validation from both Government bodies and academia.”

Brian Lord OBE
Managing Director, PGI Cyber
Cyber Academy Training Courses

The following is a selection of our current courses that are regularly scheduled to be taught at the Cyber Academy and can be booked on an individual or group basis. For organisations seeking bespoke, closed or specialist courses please contact us.

AWAIRENESS

EXECUTIVE CYBER AWARENESS | 30
CYBER SECURITY FUNDAMENTALS | 31
CYBER SECURITY AWARENESS | 32
MALWARE AWARENESS | 33
CYBER SECURITY AWARENESS FOR GOVERNMENT OFFICIALS | 34
INTRODUCTION TO CYBER RISK FOR CRITICAL NATIONAL INFRASTRUCTURE | 35

FILLING THE KNOWLEDGE GAP

BESPOKE PROGRAMME MODULES | 36

CONVERSION

CERTIFICATE IN INFORMATION SECURITY MANAGEMENT PRINCIPLES (CISMP) | 38
ISO 27001 LEAD AUDITOR CONVERSION | 39
COMPTIA A+ | 40
COMPTIA NETWORK+ | 41
COMPTIA SECURITY+ | 42
INCIDENT RESPONSE FOR IT STAFF | 43
ADVANCED THREAT METHODOLOGY | 44
PGI PENETRATION TESTING ASSOCIATE | 45
SOC ANALYST | 46
OPERATIONAL DIGITAL FORENSICS | 47
CONTINUING PROFESSIONAL DEVELOPMENT

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP®) | 48
PRACTITIONER CERTIFICATE IN INFORMATION ASSURANCE ARCHITECTURE | 50
SOLUTIONS ARCHITECTURE SECURITY PRACTITIONER | 52
ISO 27001 LEAD IMPLEMENTER | 53
ISO 27001 LEAD AUDITOR | 54
QUALIFIED SECURITY TEAM MEMBER (QSTM) | 56
OPEN SOURCE INTELLIGENCE | 57
MALWARE AWARENESS | 58
DDOS SIMULATION FOR INVESTIGATORS | 59
ADVANCED THREAT METHODOLOGY FOR POLICE | 60
OPERATIONAL DIGITAL FORENSICS FOR POLICE | 62
INTRODUCTION TO CYBER TECHNOLOGY FOR SENIOR INVESTIGATING OFFICERS | 63
LEAD INCIDENT MANAGER | 64
SOC INCIDENT RESPONDER | 65

LEADERSHIP

EXECUTIVE CYBER AWARENESS TRAINING | 66
CYBER SECURITY FUNDAMENTALS | 67
CERTIFIED INFORMATION SECURITY MANAGER (CISM) | 68

PROGRAMMES | 70
Executive Cyber Awareness

Our **bespoke duration** Executive Cyber Awareness training allows you, as a leader or a manager of your organisation, to grasp the business critical issues of cyber security. This will enable you to understand the security measures that need to be implemented to mitigate risks and ensure that appropriate investment plans are proportionate to the risks your company faces. As leaders you will need to develop your cyber threat landscape awareness and will do so by experiencing a variety of demonstrations, discussions and case studies.

**Aim**

Gain insight of the cyber threat landscape and real-world consequences of ignoring the risk to business by learning the methodologies that an attacker will adopt to breach security and to expand access within a compromised network.

**Who Should Attend?**

This course is designed for executives and senior managers from both the public and commercial sector organisations, allowing them to appreciate how the many and various issues of cyber security in a digitally enabled environment applies to them, their roles, their reputation and ultimately their organisational survival.

Designed specifically for executives from a non-IT or information security background but who have the opportunity to shape and determine their organisation’s working culture, strategy and investment in this area.

**Learning Objectives**

- Effectively understand and discuss real-world hacking events
- Understand exploitation techniques used by hackers
- Mitigate risk by demystifying cyber security jargon
- Assess the damage malware can cause
- Understand cyber defence operations.

A **one day** GCHQ Certified Executive Cyber Awareness course is also available.
Cyber Security Fundamentals

Our **two day** GCHQ Certified Cyber Security Fundamentals course is an introduction to cyber awareness for those managing or leading teams who need to identify cyber risk within typical business operations. The course provides a broad overview of the cyber threat landscape, risks and associated vulnerabilities with ‘cyber’ and the impact of a breach to businesses and individuals. It provides a fundamental level of knowledge required to inform and positively affect behaviours of end users, reducing the risk of losing or mismanaging sensitive information.

**Aim**

Develop a well-informed, positive mindset towards cyber security to be able to design and implement a strategic cyber security plan with significant relevance to business risk.

**Who Should Attend?**

Trainees who use systems to interact with data and should understand who their behaviour affects the overall security of their organisation, or those responsible for cyber awareness and IT security training for the workforce. Key decision makers within an organisation will benefit from becoming more aware of the risks present by both human and technical vulnerabilities.

**Learning Objectives**

- Increase the understanding of the cyber threat landscape
- Identify measures to secure your organisation’s digital footprint
- Analyse cybercrime case studies to demonstrate real-world consequences
- Identify techniques to drive a cyber security culture in an organisation
- Understand why organisational behaviour must adopt safe cyber practices
- Understand techniques used by adversaries and how to protect against them
- Increase knowledge of safe and responsible use of information technology
- Understand the risks associated with information sharing using social media
- Gain insight into how to explain to executives the importance of cyber security in an organisation.
Cyber Security Awareness

Our **one day** GCHQ Certified Cyber Security Awareness course will provide you with a thorough understanding of cyber security as well as the associated threats, risks and different mitigation strategies for managing relevant issues. Cyber security concepts are demystified and the risks are normalised using live demonstrations, relevant and contemporary case studies and explanations of jargon used by media and industry talking about cyber security.

**Aim**

Develop a well-informed and positive mind-set towards cyber security by becoming cyber security aware and understand how to discuss and manage security vulnerabilities appropriately in relation to business and personal risks.

**Who Should Attend?**

This course is for staff at all technical or non-technical levels who interact with a computer system on a daily basis. There is no pre-reading required for this course but trainees are likely to fully benefit from this course if they are familiar with recent hacks and data breaches in the national and international media, as these may be used as case studies or help form discussions on the course.

**Learning Objectives**

- Become aware of the cyber threat landscape
- Identify who conducts cyber-attacks, how, and why
- Learn how to drive a security aware culture within an organisation
- Analyse and explain relevant and contemporary case studies of data breach
- Understand threat actors and explain their differences in methods and objectives
- Demonstrate what 2FA and secure passphrases are and what they offer
- Explain the three pillars of information security defined in current, real-world context
- Understand how hackers exploit open source information to create an attack plan
- Create core messages for a cyber security awareness campaign within their workforce
- Identify steps to directly improve personal and departmental or divisional cyber security.
Malware Awareness

Our **one day** Malware Awareness course will teach you how an attacker uses malware with common attack tools such as Metasploit and Remote Access Tools (RAT), such as Dark Comet. This will help you develop strategies, system management techniques and user policies to defend your network and critical information.

**Aim**

Understand current cyber-attack methods employed by attackers by demonstrating the process of an attack and delving deeper into the hacker mind-set.

**Who Should Attend?**

This course is for IT professionals involved in operating and administering networks, websites and databases, and people who are responsible for protecting their organisation's networks from threats. The course also benefits investigators who require an understanding of malware and attacker technique for the purpose of working in and around crime prevention.

**Learning Objectives**

Trainees will gain a comprehensive understanding of:

- Attacker tools and terminology
- How these tools are used to attack victim's systems
- The capabilities of some of these tools
- How an incident responder may go about searching for signs of these tools
- Steps for handling infected computers
- Possible lines of inquiry for investigation
- Notable technical data points which will be useful for analysis
- Undertake fully immersive live training on how an attacker gains access.
Cyber Security Awareness for Government Officials

Our one day GCHQ Certified Cyber Security Awareness course for Government Officials will give you an increased understanding of cyber security as well as the associated threats, risks and different mitigation strategies for managing these issues. Cyber security concepts are demystified and the risks are normalised using live demonstrations, relevant and contemporary case studies and explanations of jargon used by media and industry talking about cyber security.

Aim
Develop a well-informed and positive mind-set towards cyber security by becoming cyber security aware and understand how to discuss and manage security vulnerabilities appropriately in relation to operational risks.

Who Should Attend?
Senior government officials, specifically those that are from a non-technical background. There is no pre-reading required for this course but trainees are likely to fully benefit from this course if they are familiar with recent hacks or data breaches in the national and international media, as these may be used as case studies or discussions on the course. If you are in a position of leadership and “cyber” is on your radar, PGI will explain jargon, demystify concepts and normalise the threats allowing you to treat cyber as any other operational risk.

Learning Objectives
- Be able to explain relevant and contemporary case studies of data breach
- Understand threat actors and explain their differences in methods and objectives in the context of government
- Demonstrate what 2FA and secure passphrases are and what they offer
- Explain the three pillars of information security defined in current, real-world context
- Understand how hackers exploit open source information to create an attack plan
- Create core messages for a cyber-security awareness campaign within their department
- Become aware of the current cyber threat landscape
- Identify who conducts cyber-attacks, how, and why
- Learn how to drive a security aware culture within a department.
Introduction to Cyber Risk for Critical National Infrastructure

Our two day Introduction to Cyber Risk for CNI course allows you, as a leader or a manager of your organisation, to understand the risks involved when designing and building a cyber security strategy that involves critical national infrastructure. An effective strategy will ensure that staff are adequately aware and prepared to defend the organisation in the event of a cyber-attack.

Aim
Gain specialist insight into critical national infrastructure protection and how measures can be included to prevent or mitigate cyber-attacks on an organisation effectively.

Who Should Attend?
This course is designed for trainees who need to understand risk associated with managing or operating functions within a Critical National Infrastructure environment, with a background in administering controls or CNI.

Learning Objectives
• The nature of a cyber threat landscape from a CNI perspective
• How CNI is built together
• The impact of an attack on CNI
• Reviewing known Industrial Control System attacks
• The ease of breaking into systems with known vulnerabilities
• How to gain access to CNI through people and then how to sustain access
• Open source frameworks and how they are applicable to CNI
• CNI profiles and their extended establishments (crossover of corporate & operational technology networks)
• Updates and downtime (patching of systems and minimising downtime)
• Vendor support (to include PLCs and associated systems)
• Supply chain and vetting within CNI
• CNI architecture and design
• The use of big data as an enabler within cyber security
• An introduction to Incident Response and Incident Handling
• How to manage an incident
• A CNI perspective – lessons learnt from Incident Response.
Bespoke Programme Modules

PGI design and build bespoke modules to benefit those with technical skills in other domains, to transfer these existing skills into new capability. Listed, are examples of modules created to help fill the knowledge gaps for trainees partaking in skills transformation programmes:

**Managing Data with Excel**

Learn and complete a range of practical exercises within Excel, each building in complexity, by creating, manipulating and analysing data through Excel. Explore data types and logic which extend into practical examples with Macros. By the end of the module, efficiently and effectively manage large datasets using Microsoft Excel.

**Operating System Fundamentals**

An understanding of various operating systems, the technologies they employ and how they differ. Exploring the key design concepts of a modern operating system, gaining the practical skills to manage and interact with a variety of different operating systems and their vendor specific technologies.

**Cookies**

Cookies are a fundamental part of the World Wide Web, and are required to allow stateful transactions to take place, as well as to greatly extend the functionality of the HTTP protocol. Cookies are explored in depth, as well as common mistakes in this context. Hands on activities allow trainees to understand the real world implications of cookie usage.

**Communications Foundations**

An introduction to the history and modern implementations of common communications systems. Understand the fundamental implementations of popular communication technologies.

**Geolocation**

Understand the core concepts behind mapping and Graphical Information Systems (GIS). Use newly acquired skills to understand the different co-ordinate systems, analysis techniques and conduct common tasks with ArcGIS.

**Open Source Intelligence**

Open Source Intelligence (OSINT) is taking information from the public domain to support an operational mission. There is a wealth of information available in open sources, but locating and extracting this information can prove difficult and time consuming due to the sheer volume of data available to draw upon. Extract information from public sources, as well as understanding technical information such as Domain Registration details to further an investigation. Use the newly acquired skills required to conduct independent online open source investigations while understanding the impact of an online footprint.
Operational Forensics

An understanding of various operating systems, the technologies they employ and how they differ. Exploring the key design concepts of a modern operating system, gaining the practical skills to manage and interact with a variety of different operating systems and their vendor specific technologies.

Cryptographic Foundations

Encryption is used throughout our connected world to enable private communications and transactions. This is particularly pertinent within computer systems due to their ability to automate mathematics. Address the history of cryptography and move through the theory behind both symmetrical and asymmetrical cryptography. Follow theory with practical sessions within the PGP suite, as well as a discussion of cryptanalysis. Use The Onion Router (TOR) and understand the privacy offered by the system and how it is utilised to perform attacks.
Certificate in Information Security Management Principles (CISMP)

Our five day BCS accredited Certificate in Information Security Management Principles (CISMP) course will help you develop your knowledge of the core concepts relating to information security which can be used to gain an internationally recognised qualification. Upon completion of this course, you will be able to apply the practical principles you have learned to further enhance and secure business processes. You will also receive access to an online resource that includes content, exercises, model answers, topical quizzes with feedback, module tests and a mock exam to prepare you for taking and successfully completing the BCS CISMP exam on the final day of the course.

Aim

Gain an understanding of the principles of information security management and to equip you with the necessary knowledge to complete the exam and achieve the CISMP qualification.

Who Should Attend?

This course is for trainees interested in the information security domain, a manager who is responsible for information security as part of their day-to-day role, or for those thinking of moving into an information security position. Knowledge of IT systems would be advantageous, but is not essential.

Learning Objectives

Trainees will gain a comprehensive understanding of:

- Key terms and concepts in information security
- The process of risk management and the appropriate use of controls
- Incident management
- The importance of auditing, change control and configuration management
- The needs for security policies, standards, operating procedures and guidelines
- The general principles of law, legal jurisdiction, and how these affect Information security management
- The differences between business continuity and disaster recovery
- The basic concepts and uses of cryptography.

This course is also available as E-Learning; please contact clientservices@pgitl.com
ISO 27001 Lead Auditor Conversion

Our **three day** ISO 27001 Lead Auditor Conversion course enables you to develop the necessary expertise to audit an Information Security Management System (ISMS) and to manage a team of auditors by applying widely recognised audit principles, procedures and techniques. This is a conversion course that allows current auditors of other disciplines (for example ISO 9001 Quality Management or ISO 22301 Business Continuity Management Systems) to concentrate the skillset on being able to audit against the requirements of ISO 27001 Information Security Management.

**Aim**

Provide the knowledge and skills necessary to conduct or lead ISO 27001:2013 audits within an organisation, either internally or externally.

**Who Should Attend?**

- Auditors wishing to convert their skillset to be able to conduct ISO 27001 audits within their organisation or who wish to conduct audits externally
- Auditors wishing to lead their organisation to successful ISO 27001:2013 certification
- Typical job roles include: IT / Information Security Managers and Analysts, Corporate Governance Managers, Risk and Compliance Managers and Analysts, Information Security Consultants
- Trainees should have a knowledge of Information Security Management principles and specifically the requirements of ISO/IEC 27001:2013. Understanding should be gained either through practical experience of ISO 27001 implementation or by attending the ISO 27001:2013 Implementers course.

**Learning Objectives**

- Understand the importance of aligning the ISMS to organisational context
- Understand the role of risk assessment and risk management
- Understand the control requirements of ISO 27001
- Plan and conduct ISO 27001:2013 audits
- Report audit findings and identify areas for improvement
- Understand the role of auditors in effecting continual improvement
- Understand how third parties view the ISMS and its compliance for certification.
CompTIA A+

Our ten day (or six day accelerated/exam focussed) CompTIA A+ course will teach you how to develop your computer hardware configuration and operating system troubleshooting skills and prepare for the vendor-neutral CompTIA A+ (220-901 and 220-902) examinations. This course provides foundational technical skills and the examination is recognised by security professionals and organisations globally. Exam vouchers are included with this course.

Aim

Gain foundational knowledge of PC hardware and software and also to develop practical skills in applying general fault finding and troubleshooting skills, preparing you for a career in the IT industry.

Who Should Attend?

This course will particularly benefit trainees pursuing a career in supporting desktop personal computer users, in job roles such as Support Engineer, Maintenance Engineer, Desktop Engineer, Computer Administrator or PC Support Analyst. Study of the course will also help to prepare for more advanced training, including CompTIA Network+ or CompTIA Security+. This course is suitable for those who have 3-6 months experience in an operational IT role.

Learning Objectives

- Identify the types and characteristics of computer components such as: motherboards, CPUs, memory and storage, input and output devices
- Install and configure peripheral devices
- Install, configure and troubleshoot Microsoft desktop operating systems
- Perform basic PC maintenance
- Secure IT systems using fundamental principles
- Install and configure print devices
- Implement Local Area Networks (LAN) and Internet access
- Communicate effectively with customers.
CompTIA Network+

Our **four day (or three day accelerated/exam focussed)** CompTIA Network+ course will teach you how to develop your network installation, configuration and troubleshooting skills and prepare for the vendor-neutral CompTIA network+ (N10-006) examination. This course provides foundational networking skills and the examination is recognised by security professionals and organisations globally. An exam voucher is included with this course.

**Aim**

Gain foundational knowledge of network hardware, protocols and services and developing practical skills in applying general networking concepts, preparing you to further your career in the IT industry.

**Who Should Attend?**

This course is for IT professionals involved in operating or managing networks, websites and databases, professionals who are responsible for supporting and troubleshooting their organisation’s networks. It is recommended that trainees have attended and passed CompTIA A+ or have equivalent knowledge and experience. This course is suitable for those who have 12-18 months experience in an operational IT role.

**Learning Objectives**

- Describe functionality of routers, firewalls, switches, load balances and proxies
- Design networks with different topologies
- Build network cables
- Identify and use different IP address classes
- Implement subnetting in complex network environments
- Explain the difference between TCP and UDP
- Identify common network protocols, services and ports
- Learn how to effectively set-up wireless networks
- Identify network security risks, threats and vulnerabilities
- Quickly fix network problems by applying troubleshooting methodology
- Apply network standards, best practices and network theory in real live scenarios.
CompTIA Security+

Our **five day (or four day accelerated/exam focussed)** CompTIA Security+ course will teach you how to develop your information security skills and prepare you for the vendor-neutral CompTIA Security+ (ST0-401) exam. This course validates foundation-level security skills, and the examination is recognised by security professionals and organisations globally. An exam voucher is included with this course.

**Aim**

Acquire technical awareness of threats and vulnerabilities which affect modern systems and improves practical knowledge on how to defend those affected technologies, preparing you for a career in cyber security.

**Who Should Attend?**

This course is for IT professionals involved in operating and managing networks, websites and databases, and people who are responsible for protecting their organisation’s networks from threats. It is recommended that you have attended and passed CompTIA Network+ or have equivalent knowledge and networking experience. This course is suitable for those who have 24 months experience in an operational IT role.

**Learning Objectives**

- Effectively use routers, firewalls, switches, load balances and proxies to secure networks
- Design secure networks
- Understand the technologies involved in securing systems and data
- Identify most common network protocols, services and ports
- Mitigate wireless networks insecurities
- Identify and mitigate risks
- Identify and defend against latest security threats and vulnerabilities
- Secure data, applications and hosts by applying various techniques
- Use different access control mechanisms and identity management systems
- Identify and use different cryptographic methods.
Incident Response for IT Staff

Our six day GCHQ Certified Incident Response course for IT staff will provide you with the necessary responsive skills and appropriate decision-making abilities to effectively investigate IT security incidents using cutting edge digital forensics tools, tactics and techniques. You will also become a malware hunter and defender for your organisation and be able to identify suspicious activity on a corporate system and from network traffic to discover and investigate high-end cyber threats.

Aim

Understand the types of tactics a threat actor uses to evade detection by developing advanced skills to locate malicious elements on a network and respond appropriately and learn how to report a compromise, who to alert and how countermeasures may help defend against future threats.

Who Should Attend?

This course is for IT professionals who operate as the IT support function in an organisation. The trainee will learn how to effectively respond to a potential incident and quickly apply the necessary actions. Alternatively the course is available as part of a workforce transformation program ensuring all IT staff are better defenders of their organisation’s network.

Learning Objectives

• Develop skills using fully immersive, hands-on training using a variety of tools
• Effectively discover host or network breaches in order to triage potential attacks
• Understand how malware typically finds its way onto a system
• Understand variations of malware and cyber threats
• Gain knowledge of the fundamentals of Windows operating systems
• Gain knowledge of file systems and processes
• Interrogate the Windows Registry
• Perform volatile memory capture (RAM dumps)
• Perform forensic imaging
• Differentiate between law enforcement and corporate incident response.
• Perform Network traffic forensics
• Perform Disk-based forensics
• Find and identify important artefacts
• Report findings.
Advanced Threat Methodology

Our **six day** GCHQ Certified Advanced Threat Methodology course will teach you precisely how external threats attack the exposed digital surface of your organisation. This knowledge will allow you to develop strategies, system management techniques and user policies to defend your network and critical information more effectively.

**Aim**

Understand cutting-edge cyber-attack techniques employed by real world attackers by demystifying the process of an attack and delving deeper into a ‘hacker’ mind-set.

**Who Should Attend?**

This course is for IT professionals involved in operating and administering networks, websites and databases, and those responsible for protecting their organisation’s networks from threats.

**Learning Objectives**

- Develop skills using fully immersive, hands-on training using a variety of tools for gaining and sustaining access to a remote network
- Gather information using open source tools
- Scan networks and servers using Nmap, analyse network traffic and enumerate remote web browsers
- Send client- and server side exploits using the Metasploit Framework (MSF)
- Understand techniques relating to masking point of origin through pivoting
- Use web based attacks as a primer to conduct further attacks, obtain credentials and gather more information on web servers
- Set up a small botnet using client-side exploits
- Use different attack vectors and attacks to access newer versions of Windows
- Query the Windows Registry and the Active Directory to identify key information
- Understand how the UNIX operating system is used in attacks
- Understand the importance of managed network devices and their role within the network
- Use Offensive Digital Forensics to identify key information post-exploitation
- Discover files of interest and where to look for them using different methods
- Obtain user credentials to demonstrate how they are used within a compromised network
- Understand how an attacker maintains a low profile within a compromised network.
PGI Penetration Testing Associate

Our five day Penetration Testing Associate course covers current techniques and associated skills used for ethical hacking and penetration testing. The course allows you to learn and practice current techniques used by industry qualified cyber-security penetration testers when conducting engagements in real world environments. The course includes the theory, as well as immersive, hands-on demonstrations and exercises of security assessment skills in four days, with the fifth day dedicated to assessments.

Aim

Increase knowledge of current ethical hacking techniques and practice using hands-on penetration testing skills in a safe environment.

Who Should Attend?

This course is for IT professionals who wish to understand ethical hacking techniques and perform tasks in vulnerable environments. By completing the PPTA you will be on your way to becoming a security consultant, knowing how to liaise with technical and non-technical clients. It is recommended that you have an in-depth knowledge of networking and the TCP protocol, as well as some familiarity or experience using the command line and Linux.

Learning Objectives

- Understand information security in the corporate world
- Develop an understanding of ethics and criminal law in relation to ethical hacking
- Network enumeration and network mapping
- Network device management and exploitation
- Service enumeration
- Service topology/dependency mapping
- Service management and exploitation
- Application enumeration and profiling
- Application and operating system management
- Application and operating system exploitation and manipulation
- Conducting penetration testing engagements
- The professionalism, communication skills, ethics and the law associated with penetration testing
- Risk management
- Required critical thinking when conducting security testing.
SOC Analyst

Our **five day** GCHQ Certified Security Operations Centre (SOC) Analyst course puts you at the forefront of your organisation for monitoring for potential network security incidents. The course has been designed by operational SOC professionals to give you imperative insight into the mind of an attacker, and the vendor agnostic skills and operational knowledge required to work in a fully functioning SOC.

**Aim**

Acquire the necessary technical skills and knowledge for an entry level analyst or practitioner to function effectively in a fully operational SOC.

**Who Should Attend?**

This course is specifically relevant for trainees who have:

- A good solid understanding of IT and a minimum of one year in a second-line IT role who wish to progress their career by working within a SOC role
- A keen interest in cyber security and who feel that they have the necessary aptitude to succeed in a technically demanding role
- Recently graduated with relevant qualifications, are either seeking to gain employment in a SOC
- Been newly recruited into a SOC without prior experience in security

**Learning Objectives**

- Understand the principles of Security Operations and how they are applied
- Be able to discuss relevant terminology and the typical roles and responsibilities within a SOC
- Gain an understanding of the cyber threat landscape including intelligence analysis and sources, baselining and analytics
- Comprehend the requirements for compliance and reporting guidelines in areas such as PCI-DSS and ISO 27001
- Address the requirements for case management, compliance and reporting guidelines
- Understand a typical Security Operations Architecture setup
- Understand the techniques employed within a SOC to extract and analyse large quantities of data.
Operational Digital Forensics

Our six day GCHQ Certified Operational Digital Forensics course will provide you with the necessary responsive skills and appropriate decision-making abilities to effectively investigate IT security incidents using cutting edge digital forensics tools, tactics and techniques. You will also become a malware hunter and defender for your organisation and be able to identify suspicious activity on a corporate system and from network traffic to discover and investigate high-end cyber threats.

Aim

Understand the types of tactics a threat actor uses to evade detection by developing advanced skills to locate malicious elements on a network and respond appropriately and learn how to report a compromise, who to alert and how countermeasures may help defend against future threats.

Who Should Attend?

This course is for IT professionals who operate as the IT support function in an organisation. The trainee will learn how to effectively respond to a potential incident and quickly apply the necessary actions. Alternatively the course is available as part of a workforce transformation program ensuring all IT staff are better defenders of their organisation’s network.

Learning Objectives

• Develop skills using fully immersive, hands-on training using a variety of tools
• Effectively discover host or network breaches in order to triage potential attacks
• Understand how malware typically finds its way onto a system
• Understand variations of malware and cyber threats
• Gain knowledge of the fundamentals of Windows operating systems
• Gain knowledge of file systems and processes
• Interrogate the Windows Registry
• Perform volatile memory capture (RAM dumps)
• Perform forensic imaging
• Differentiate between law enforcement and corporate incident response.
• Perform Network traffic forensics
• Perform Disk-based forensics
• Find and identify important artefacts
• Report findings.
Certified Information Systems Security Professional (CISSP®)

Our five day (or four day accelerated) Certified Information Systems Security Professional (CISSP) exam preparation course provides you with a clear understanding of the information security principles and background knowledge required to operate as an effective Information Security Manager within the eight security domains as set out by (ISC)². This course prepares you with a detailed breadth of security knowledge to take the globally renowned CISSP® exam.

The course covers all eight domains of security that comprise the common body of knowledge for information systems security professionals and will help trainees prepare for CISSP® certification. Those considering taking the exam to gain certification must have experience in at least two of the domains in the CBK, for 5 years or more (4 years if they have achieved relevant certifications, e.g. MCSA) to achieve full certification.

The course does not include the cost nor time for taking the six hour CISSP® exam, but does include access to the trainer.

Aim

Understand business critical security issues and determine what measures need to be implemented to mitigate risks and exploit opportunities and to plan investment proportionate to the risk your organisation faces in preparation to undertake the CISSP® exam.

Who Should Attend?

Experienced IT/information security professionals, who are looking to expand their knowledge.

This course and exam certification are specifically relevant for the following roles:

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect
- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Director of Security
- Network Architect.
Learning Objectives

Trainees will learn about the eight domains covered in the CISSP® exam:

- Security and Risk Management (security, risk, compliance, law, regulations, business continuity)
- Asset Security (protecting security of assets)
- Security Engineering (engineering and management of security)
- Communications and Network Security (designing and protecting network security)
- Identity and Access Management (controlling access and managing identity)
- Security Assessment and Testing (designing, performing, and analysing security testing)
- Security Operations (foundational concepts, investigations, incident management, disaster recovery)
- Software Development Security (understanding, applying, and enforcing software security).
Practitioner Certificate in Information Assurance Architecture

Our five day practitioner course prepares you for a career in security architecture. A Security Architect is a senior-level enterprise architect role, either within a dedicated security team or as part of a more general Enterprise Architecture team. The course prepares you to take either the BCS Practitioner Certificate in Information Assurance Architecture (PCiIAA) exam or the CREST Registered Technical Security Architect (CRTSA) exam for Senior or Lead Practitioners. It has been designed to cover all learning objectives required of all domains covered in both certifications. You will also receive access to an online resource that includes content, exercises, model answers, topical quizzes with feedback, module tests and a mock exam to prepare you for taking and successfully completing the BCS PCiIAA exam on the final day of the course or the CREST CRTSA exam at a later date.

Aim

Understand a business environment the IT systems need to provide for, as well as the technical controls that are available to the architect that can be called upon to address the threats against confidentiality, integrity and availability.

Who Should Attend?

- Trainees will require a broad understanding of all aspects of Information Security and Information Assurance equivalent to the BCS Certificate in Information Security Management Principles (CISMP)
- Trainees who wish to gain the BCS PCiIAA or CREST's CRTSA certificate and qualify as a Practitioner, Senior Practitioner or Lead Practitioner in Security Architecture under the CESG Certified Professional (CCP) scheme
- System administrators who wish to become security architects
- Technical architects looking to move into the field of security architecture
- Security professionals wanting to gain an appreciation of the technical and business aspects of their profession, or move into a more senior architecture role
- Trainees who have taken the CISMP and wish to progress into a practitioner role.

This course is also available as E-Learning; please contact clientservices@pgitl.com
Learning Objectives

• Describe the business environment and the information risks that apply to systems
• Describe and apply security design principles
• Identify information risks that arise from potential solution architectures
• Design alternate architectures or countermeasures to mitigate identified information risks
• Ensure that proposed architectures and countermeasures adequately mitigate identified information risks
• Apply “standard” security techniques and architectures to mitigate security risks
• Develop new architectures that mitigate the risks posed by new technologies and business
• Provide consultancy and advice to explain Information Assurance and architectural problems
• Securely configure ICT systems in compliance with their approved security architectures.
Solutions Architecture Security Practitioner

Our **three day** Solutions Architecture Security Practitioner course prepares Solutions or Technical Architects to gain an understanding of information assurance. Many organisations, or projects, cannot afford to have an assigned security architect, yet many solutions or technical architects do not have a good understanding of Information Assurance meaning many systems are designed and built that do not mitigate current or emerging threats from today’s interconnected IT world. You will receive access to an online resource that includes content, exercises, model answers, topical quizzes with feedback, module tests and a mock exam to prepare you for taking and successfully completing the Global Certification Institute (GCI) SASP exam on the final day of the course.

**Aim**

Gain the knowledge of how to architect a wide range of security controls into a system.

**Who Should Attend?**

- Solution or Technical Architects who wish to build security into their projects
- Security professionals wanting to gain an appreciation of the technical and business aspects of their profession, or move into a more senior architecture role.

**Learning Objectives**

- Describe and apply security design principles
- Identify information risks that arise from potential solution architectures
- Design alternate architectures or countermeasures to mitigate identified information risks
- Ensure that proposed architectures and countermeasures adequately mitigate identified information risks
- Apply “standard” security techniques and architectures to mitigate security risks
- Develop new architectures that mitigate the risks posed by new technologies and business practices
- Securely configure ICT systems in compliance with their approved security architectures.

This course is also available as E-Learning; please contact clientservices@pgitl.com
ISO 27001 Lead Implementer

Our five day ISO 27001 Lead Implementer course enables you to develop the necessary expertise to support an organisation in implementing and managing an Information Security Management System (ISMS) in accordance with the requirements of ISO 27001:2013. You will gain an understanding of information risk management and the deployment of control measures proportional to organisational risk. You will develop your project management abilities to lead a team in the implementation of an ISMS. You will also receive access to an online resource that includes content, exercises, model answers, topical quizzes with feedback, module tests and a sample exam paper to prepare you for taking and successfully completing the PECB Certified ISO 27001 Lead Implementer exam on the final day of the course.

Aim

Understand the purpose and benefits of an ISMS and acquire the necessary expertise to lead an organisation in implementing, managing and maintaining an ISMS.

Who Should Attend?

- Project managers or consultants supporting an organisation in the implementation of an Information Security Management System (ISMS)
- ISO 27001 auditors who wish to fully understand the Information Security Management System implementation process
- Senior Managers responsible for the IT governance of an enterprise and the management of its risks
- Members of an information security team
- Technical experts wanting to prepare for an information security function or for an ISMS project management function.

Learning Objectives

Trainees will gain a comprehensive understanding of:

- The implementation of an ISMS in accordance with ISO 27001
- Concepts, approaches, standards, methods and techniques required for the effective management of an ISMS
- The relationship between the components of an ISMS, including stakeholder interests, risk management processes, control measures and continuous improvement
- Knowledge and skills required to advise organisations on best practices in the management of information security
- The vital knowledge to achieve the ISO 27001 Lead Implementer qualification.

This course is also available as E-Learning; please contact clientservices@pgitl.com
ISO 27001 Lead Auditor

Our five day ISO 27001 Lead Auditor course enables you to develop the necessary expertise to audit an Information Security Management System (ISMS) and to manage a team of auditors by applying widely recognised audit principles, procedures and techniques. You will acquire the necessary knowledge and skills to proficiently plan and perform internal and external audits in accordance with the guidelines of ISO 19011. Based on practical exercises, you will develop the skills (mastering audit techniques) and competencies (managing audit teams and audit program, communicating with customers, conflict resolution, etc.) necessary to efficiently conduct an audit. You will also receive access to an online resource that includes content, exercises, model answers, topical quizzes with feedback, module tests and a sample exam paper to prepare you for taking and successfully completing the PECB Certified ISO 27001 Lead Auditor exam on the final day of the course.

Aim

Acquire the necessary knowledge and skills to proficiently plan and conduct internal and external audits and effectively equip trainees with the necessary knowledge to achieve the ISO 27001 Lead Auditor qualification.

Who Should Attend?

- Internal auditors
- Auditors wanting to perform and lead Information Security Management System (ISMS) certification audits
- Project managers or consultants wanting to master the Information Security Management System audit process
- Senior Managers responsible for the IT governance of an enterprise and the management of its risks
- Members of an information security team
- Expert advisers in information technology
- Technical experts wanting to prepare for an information security audit function
- Basic knowledge of ISO 27001 is recommended.

This course is also available as E-Learning; please contact clientservices@pgitl.com
Learning Objectives

Trainees will learn how to:

- Acquire the expertise to perform an ISO 27001 internal audit following ISO 19011 guidelines
- Acquire the expertise to perform an ISO 27001 certification audit following ISO 19011 guidelines and the specifications of ISO 27006
- Acquire the necessary expertise to manage an ISMS audit team
- Understand the operation of an ISO 27001 conformant information security management system
- Understand the relationship between an effective ISMS and the requirements of different stakeholders within an organisation
- Improve the ability to analyse the internal and external environment of an organisation, its risk assessment and audit decision-making.
Qualified Security Team Member (QSTM)

Our five day TigerScheme Qualified Security Team Member course covers current techniques and associated skills used for ethical hacking and penetration testing. The course allows you to learn and practice current techniques used by industry qualified cyber-security penetration testers when conducting engagements in real world environments. The course includes the theory, as well as immersive, hands-on demonstrations and exercises of security assessment skills in four days, with the fifth day dedicated to assessments.

Aim

Increase knowledge of current ethical hacking techniques using hands-on penetration testing skills in a safe environment, whilst gaining a qualification to progress to the CHECK Team Member status.

Who Should Attend?

This course is for IT professionals who wish to understand ethical hacking techniques and perform tasks in vulnerable environments. By taking the QSTM and demonstrating sufficient operation experience you can apply to become a CHECK Team Member. It is recommended that you have an in-depth knowledge of networking and the TCP protocol, as well as some familiarity or experience using the command line and Linux.

Learning Objectives

• Understand information security in the corporate world
• Develop an understanding of ethics and criminal law in relation to ethical hacking
• Understand the soft skills required by a penetration tester
• Network enumeration and network mapping
• Network device management and exploitation
• Service enumeration
• Service topology/dependency mapping
• Service management and exploitation
• Application enumeration and profiling
• Application and operating system management
• Application and operating system exploitation and manipulation
• Conducting penetration testing engagements
• The professionalism, communication skills, ethics and the law associated with penetration testing
• Risk management
• Required critical thinking when conducting security testing.
Open Source Intelligence

Our **three day** GCHQ Certified Open Source Intelligence (OSINT) course will teach you to obtain intelligence from publicly available information. There is a wealth of information available from open sources, but locating and extracting it can prove difficult and time-consuming due to the sheer volume of data available. By employing focused collection and analysis techniques, effectively obtained information can support any number of business objectives. At the end of the course, you will have the necessary skills required to conduct independent online open source investigations while understanding and mitigating your own online digital footprint.

**Aim**

Understand the full range of sources available to the analyst by effectively interrogating and exploiting open source intelligence in a lawful and constructive manner. This will help to build a full information picture and utilise techniques to evaluate source reliability and credibility.

**Who Should Attend?**

Trainees who have an operational need to effectively research and collate publicly available information.

**Learning Objectives**

Trainees will learn:

- How OSINT is used to collect public information and identify potential cyber-attack vectors
- How to gather personal information from social media
- The Deep Web and how to use deep search engines to access unindexed data
- The benefits of fusing of OSINT, SOCMINT, IMINT, HUMINT, TECHINT and covert sources to create a comprehensive intelligence picture
- How to access historic information and deleted versions of websites
- The use of Anonymisation (hidden) services
- Geolocation and geospatial intelligence visualisation.
Malware Awareness

Our one day Malware Awareness course will teach you how an attacker uses malware with common attack tools such as Metasploit and Remote Access Tools (RAT), such as Dark Comet. This will help you develop strategies, system management techniques and user policies to defend your network and critical information.

Aim

Understand current cyber-attack methods employed by attackers by demonstrating the process of an attack and delving deeper into the hacker mind-set.

Who Should Attend?

This course is for IT professionals involved in operating and administering networks, websites and databases, and people who are responsible for protecting their organisation’s networks from threats. The course also benefits investigators who require an understanding of malware and attacker technique for the purpose of working in and around crime prevention.

Learning Objectives

Trainees will gain a comprehensive understanding of:

- Attacker tools and terminology
- How these tools are used to attack victims system
- The capabilities of some of these tools
- How an incident responder may go about searching for signs of these tools
- Steps for dealing with affected computers
- Possible lines of inquiry for investigation
- Notable technical data points which will be useful for analysis
- Undertake fully immersive live training on how an attacker gains access.
DDOS Simulation for Investigators

From a policing angle our two day Distributed Denial of Service (DDOS) Simulation for Investigators course takes you through a simulated DDOS attack scenario for both awareness and practical purposes. Our specialist training guides you through various significant steps; an attacker deciding to launch an attack, attack preparation, attack initiation, the consequences and effects on the victim(s) and then investigation techniques to seek and identify digital evidence.

Aim
Provides technical police officers with an understanding of how an attacker will carry out criminal activity in the case of DDOS attacks and how to investigate criminal activity in the case of DDOS attacks.

Who Should Attend?
• Police officers who want to understand the methodology of an attacker
• Police officers who are investigating DDOS attacks
• Members of an organisation’s security team who would respond to such attacks.

Learning Objectives
• Understand terminology relevant to a DDOS attack
• Understand the technical implementation of a DDOS attack
• Observe a simulated DDOS attack inside of a controlled environment
• Understand how zombie attackers participate in a DDOS attack
• Understand sources of evidence after a DDOS attack, and how these may be investigated
• Understand how a zombie host located during an investigation may be investigated
• Understand situations that present barriers to investigation of a DDOS attack.
Advanced Threat Methodology
For Police

Our six day (or five day accelerated) Advanced Threat Methodology course for Police will teach you, as an investigating police/military officer/staff the essentials of remote network exploitation. You will learn in-depth about the Windows Registry, offensive digital forensics, finding domain controllers, Windows Active Directory queries, finding files of interest, cracking passwords and the use of various techniques in how to manoeuvre around a remote Windows network.

Aim

Understand the methodology used by criminals, demonstrating how vulnerabilities are exploited by engaging in the mindset of a hacker, allowing officers to pro-actively investigate and advise on cybercrime prevention.

Who Should Attend?

This course is for officers or staff who are required to understand the methodology used by criminals and how to investigate this type of crime and/or officers who are able to use intrusive computer methodologies in their role. The course also demonstrates to specialists how vulnerabilities are exploited, allowing them to advise on crime prevention.

Learning Objectives

• Develop skills using fully immersive, hands-on training using a variety of tools for gaining and sustaining access to a remote network
• Effectively use specific open source intelligence gathering to identify areas of interest
• Gain sufficient understanding of how an attacker will carry out their criminal activity
• Conduct information gathering (hostile reconnaissance) using open source tools
• Learn to scan networks and servers using Nmap, analyse network packets (at a low level) and use Beef (the Browser Exploitation Framework) to enumerate remote web browsers
• Learn to send exploits using the Metasploit Framework (MSF), advanced tunneling using custom executables, Meterpreter pivoting, Cross Site Scripting (XSS) and SQL Injection
• Compile and deploy malware to set up a small botnet using client-side exploits
• Learn about the Windows Registry, offensive digital forensics and Windows Active Directory queries
• Learn to find files of interest, how to crack passwords and use the pass-the-hash technique to manoeuvre around a Windows network
• Trace IP addresses through the Internet and how to read and analyse email headers
• Use skills and techniques obtained from the course to put criminal activity into cyber policing context
• Identify relevant case studies associated with hacking and criminal activity.
Operational Digital Forensics for Police

Our six day (or five day accelerated) Operational Digital Forensics course for Police will teach you, as an investigating police/military officer/staff how to analyse data which has been recovered from digital evidence in relation to a cyber-threat. Officers will understand the different types of data that may be held on various devices, become familiar with free open source forensic analysis tools to identify and extract data in preparation for further analysis or reporting. Officers will be able to conduct basic forensic triage of systems and use their new skills to discover and investigate high-end cyber threats. An offensive module including the OWASP Top 10 vulnerabilities provides scenario based learning reflective of various types of cybercrimes being reported that need responding to.

Aim

To provide police officers and staff with sufficient digital device knowledge in order to efficiently and effectively analyse digital evidence, whilst providing enhanced knowledge of the various types of cybercrime and what they may look like.

Who Should Attend?

This course is specifically for officers or staff who respond to reported cybercrimes and those who analyse suspect systems for potential digital evidence or malware infections.

Learning Objectives

- Identify realistic end goals for investigating data extracted from digital media
- Gain insight into better interview techniques for a suspected device user
- Examine RAM and forensic images of infected digital media
- Explain your actions in court
- Outline the current and evolving technology landscape relating to cybercrime
- Understand malware and be aware of the offensive methodology
- Use various types of digital evidence to build or form part of a case including how to translate or report technical information
- Gain knowledge of courtroom presentation involving digital evidence
- Recognise malware on an infected system and gain awareness in malware ability
- Make better and more effective decisions when identifying lines of enquiry.
Introduction to Cyber Technology for Senior Investigating Officers

Our two day Introduction to Cyber Technology course provides senior police officers with an understanding of how technology has enhanced the ability for law enforcement agencies to use digital devices for investigative purposes by demonstrating the availability of a user’s digital footprint and how this can be used within criminal enterprise. Officers are provided with the knowledge of the evasive countermeasures employed by today’s criminals and how they can impede the extraction and analysis of digital evidence.

Aim

Increase knowledge relating to the cyber threat landscape for law enforcement professionals and enhance any understanding of the use of digital technology to help commit crime.

Who Should Attend?

This course is especially relevant for:

• Senior Investigating Officers
• Officers involved in investigating serious organised crime units
• Officers and staff with decision making roles at a crime scene.

Learning Objectives

• Make informed decisions during investigations and identifying availability of digital evidence at a crime scene.
• Discuss the significance of potential digital evidence that can be extracted from modern technology and how it can assist investigations
• Identify what can be digitally analysed and determine where useful data could be located
• Become familiar with constraints of investigating cybercrime
• Acknowledge the use of forensic capability and electronic interference in tackling crime
• Know how technology can be used to assist during an investigation.
Lead Incident Manager

Our five day Lead Incident Manager course will ensure you acquire the necessary knowledge and skills to manage information security incidents in time by being familiar with an incident life cycle. We will present the ISO 27035 information security incident management standard, a process model for designing and developing an organisational incident management process, and how companies may use the standard. The training is also fully compatible with ISO 27035 which supports ISO 27001 by providing guidance for incident management. You will also receive access to an online resource that includes content, exercises, model answers, topical quizzes with feedback, module tests and a sample exam paper to prepare you for taking and successfully completing the PECB Certified ISO 27035 Lead Incident Manager exam on the final day of the course.

Aim
Develops competency to master a model for implementing an incident management process throughout an organisation using the ISO 27035.

Who Should Attend?
This course is for those who have basic knowledge of ISO 27001 or the following roles:
- Incident managers
- Business Process Owners
- Information Security Risk Managers
- Regulatory Compliance Managers
- Members of Incident Response Team
- Those responsible for information security or conformity within an organisation.

Learning Objectives
- Understand the concepts, approaches, methods, tools and techniques allowing an effective information security incident management according to ISO 27035
- Understand, interpret and provide guidance on how to implement and manage incident management processes based on best practices of ISO 27035 and other relevant standards
- Acquire the competence to implement, maintain and manage an ongoing information security incident management program according to ISO 27035
- Acquire the competence to effectively advise organisations on the best practices in information security management.

This course is also available as E-Learning; please contact clientservices@pgitl.com
SOC Incident Responder

Our ten day GCHQ Certified Security Operations Centre (SOC) Incident Responder course puts you at the forefront of monitoring and then effectively reacting to potential security incidents. The course provides experienced cyber security professionals with deep understanding of: attacker tactics, digital forensics (disk, memory and network), malware analysis and interfacing directly with respective parties and stakeholders to perform first line incident response.

Aim

Acquire and expand the necessary technical skills and knowledge to function as an effective and specialist Incident Responder working within a fully operational SOC.

Who Should Attend?

Trainees who have had previous experience in a SOC, who are now considered senior and require incident responder specialist training to appropriately and safely react to client requirements. It is preferable that trainees have experience and fundamental knowledge of Windows and Linux operating systems. If this is not the case – an evening, a half day or a full day can be bolted onto the course for adequate preparation.

Learning Objectives

- Understand the functional requirements needed when responding to an incident
- Understand the roles in an organisation and the language of reporting that may be needed
- Determine the terminology required when liaising with clients when planning to collect data
- Prepare a generic incident response jump kit
- Strategically prepare a plan of action when identifying the scope of work
- Perform effective and efficient digital forensics to quickly acquire data
- Understand the legal requirements to adhere to when acquiring data that may be required for law enforcement or court
- Explain their role, position and actions taken to a client
- Ensure that any potentially malicious software that may be present is contained securely and safely.
Executive Cyber Awareness Training

Our bespoke duration Executive Cyber Awareness training allows you, as a leader or a manager of your organisation, to grasp the business critical issues of cyber security. This will enable you to understand the security measures that need to be implemented to mitigate risks and ensure that appropriate investment plans are proportionate to the risks your company faces. As leaders you will need to develop your cyber threat landscape awareness and will do so by experiencing a variety of demonstrations, discussions and case studies.

Aim

Gain insight of the cyber threat landscape and real-world consequences of ignoring the risk to business by learning the methodologies that an attacker will adopt to breach security and to expand access within a compromised network.

Who Should Attend?

This course is designed for executives and senior managers from both the public and commercial sector organisations, allowing them to appreciate how the many and various issues of cyber security in a digitally enabled environment applies to them, their roles, their reputation and ultimately their organisational survival. Designed specifically for executives from a non-IT or information security background but who have the opportunity to shape and determine their organisation’s working culture, strategy and investment in this area.

Learning Objectives

• Effectively understand and discuss real-world hacking events
• Understand exploitation techniques used by hackers
• Mitigate risk by demystifying cyber security jargon
• Assess the damage malware can cause
• Understand cyber defence operations.

A one day GCHQ Certified Executive Cyber Awareness course is also available.
Cyber Security Fundamentals

Our **two day** GCHQ Certified Cyber Security Fundamentals course is an introduction to cyber awareness for those responsible and accountable for the protection of business data such as senior IT management or a Chief Information Security Officer (CISO). The course provides a broad overview of the cyber threat landscape, risks and associated vulnerabilities with ‘cyber’ and the impact of a breach to businesses and individuals. It provides a fundamental level of knowledge required to inform and positively affect behaviours of end users, reducing the risk of losing or mismanaging sensitive information.

**Aim**

As a leader, develop a well-informed, positive mind-set towards cyber security to be able to design and implement a strategic cyber security plan with significant relevance to business risk.

**Who Should Attend?**

Senior IT or business management professionals such as Chief Information Security Officers (CISO) who are responsible and accountable for the protection of data and the security of their organisation’s systems, or those responsible for cyber awareness and IT security training for the workforce. Key decision makers within an organisation will benefit from becoming more aware of the risks present by both human and technical vulnerabilities.

**Learning Objectives**

- Increase the understanding of the cyber threat landscape
- Identify measures to secure your organisation’s digital footprint
- Analyse cybercrime case studies to demonstrate real-world consequences
- Identify techniques to drive a cyber security culture in an organisation
- Understand why organisational behaviour must adopt safe cyber practices
- Understand techniques used by adversaries and how to protect against them
- Increase knowledge of safe and responsible use of information technology
- Understand the risks associated with information sharing using social media
- Gain insight into how to explain to executives the importance of cyber security in an organisation.
Certified Information Security Manager (CISM)

Our **four day (or three day accelerated)** Certified Information Security Manager exam preparation course provides you with a clear understanding of the risk management requirements from an information security perspective, when applied to business strategy and objectives. This course prepares you with a detailed breadth of knowledge to take the globally renowned CISM exam, of which more than 32,000 individuals have passed, and qualified as CISMrs since 2002. ISACA is the governing body behind the CISM certification. The CISM certification is management-focused and is designed for those individuals who will manage, design, oversee, and assess an organisation’s information security.

The course covers four information security management areas, which have been defined and described in further detail via Tasks and Knowledge statements, approved by the CISM Certification Committee. Those considering taking the exam to gain certification must have five years’ experience in subject areas being covered (although waivers are available for a maximum of two years, for example, for those who already have the CISSP qualification; or holders of other more specialised credentials, such as GIAC or Microsoft Certified Systems Engineer (MCSE) can receive a one-year general information security experience waiver).

The course does not include the cost or time for taking the four hour CISM exam, but does include access to the trainer for mentoring between completing the course and taking the exam.

**Aim**

Promotes international security practices and covers in depth knowledge on how a security manager/leader will carry out responsibilities such as, setting up and running a security department; using governance models to manage security; managing project risks during development and acquisition processes; Business Continuity Planning, Business Impact Analysis, and Disaster Recovery Planning.

**Who Should Attend?**

- Experienced IT/information security professionals who are looking to expand their knowledge into information security management and leadership, or seeking a recognised qualification to underpin their existing management role.
Learning Objectives

Trainees will learn about the four domains covered in the CISM exam, which are:

- Information Security Governance (including security strategy, corporate governance, policies, business cases, obtaining commitment, monitoring and reporting)
- Information Risk Management and Compliance (asset classification, legal & regulatory, risk assessments and threat analysis, evaluating controls, and reporting non-compliance)
- Information Security Program Development and Management (aligning with business functions, security architectures, security awareness, defining resources and establishing security into key processes such as change control, and BCM)
- Information Security Incident Management (response plans, investigation processes, training, testing and review, and integration with DRP / BCP).
Programmes

PGI can design cyber security programmes to cover the broad range of skills and knowledge required to start work as a competent cyber security professional and includes ongoing professional development review throughout. Each course or module is designed to focus on different challenges within cyber space – whether general awareness such as corporate business risk, or more practical training, such as cyber security skills baselining or ethical hacking techniques. The combination gives graduates a wide understanding of cyber issues and responsibilities.

PGI has experience developing syllabuses tailored to our client’s specific requirements and learning objectives. While many of those entering the cyber security profession have some education or professional background in IT, PGI find that few have experience in considering security aspects as part of their work or training. The first phase of a PGI programme can therefore be designed to fill gaps in knowledge by teaching, awareness in collaboration with IT fundamentals from a security perspective.

PGI is able to recognise aptitude and ability of each individual, and identify their suitability for working in three distinct areas within the cyber security industry. These can be broadly defined as trainee defensive security operators (such as SOC or IR specialisms), trainee offensive security operators (such as intelligence analysts or penetration testers) and cyber policy/information assurance specialists. PGI has a portfolio of technical courses to transition staff into working within a specific specialist cyber discipline. Further mentoring and more specific training solutions can be followed for desired specialisms.

Cyber Transformation

When addressing the knowledge gaps, specific and multi-discipline modules can be tailored, combined, become more advanced and specific durations extended or shortened to meet the challenge of upskilling a diverse skillset within teams to achieve an ultimate goal of creating an effective cyber secure team, department or organisation. Individual technical assessments, during and after modules can be taken alongside trainer observations to measure upskilling progression.

Cyber Training Bootcamps

PGI believe the need to upskill trainees before taking on security disciplines is fundamental to ensuring the appropriate conceptual and technical foundational elements are learnt. Once a combined awareness and practical upskilling programme has taken place, trainees operational objectives, personal motivations aligned with stand-out potential in a particular skillset can be identified and assessed so that a relevant and directed training programme can be designed to achieve desired outcomes. This can be supplemented by PGI specialist mentoring.
Cyber Security Reskilling for Technical Delegations

On the following page is an example of an 8 week technical cyber skills conversion programme which covers the broad range of skills and knowledge required to start work as a competent cyber security professional and offers up to 8 certificated cyber security qualifications and up to 40 transferable credits towards Bournemouth University’s Master’s Degree in Cyber Security and Human Factors.

For the final 3 weeks of the programme, PGI divide the group based on aptitude and ability into 20 trainee security operations centre (SOC) and incident response (IR) staff and 20 trainee penetration testing staff. These professions are growth areas in the cyber security skills market; have a large number of vacancies and opportunities; are appropriate for relatively inexperienced staff learning on the job after employment; and provide a good-grounding from which trainees can progress into long-term cyber security careers.
This example 8 week programme involves a total of 8 one week long modules representing 320 hours of technical training, practice and exercises for each trainee.

The diagram below is an example of a two week boot-camp used to effectively upskill staff as ‘Security Champions’ within their departments of a large organisation:
Few organisations are immune to threats that can damage reputations, people, property and critical assets.

With experience in the world’s most hostile environments, few companies can claim the breadth or depth of our cyber security and risk management expertise.

PGI’s professionals work on the front-line of cyber security operations and immerse themselves daily in cyber threat activity and their geopolitical context. Their interpretation of prevailing circumstances, data and influences informs our training and advice to enable government agencies and commercial organisations to make informed, cost-effective decisions and avoid risk.

Risk prevention, cyber security services, operational, behavioural, geopolitical, maritime, strategic intelligence and consulting are just some of the services we provide alongside the PGI Cyber Academy’s training programmes.

Together we’ll avert risks, address crises and build capability.