Version 2.0; 08 January 2016


# GCHQ Certification of Cyber Security Training Courses

Supporting Assessment Criteria for the GCHQ Certified Training (GCT) Scheme



## Document History

| Issue | Date | Comment |
|---|---|---|
| 1.0 | 30 September 2014 | First Issue |
| 2.0 | 08 January 2016 | Second Issue |

## Introduction

Reflecting the aims of the National Cyber Security Programme, UK Government and its delivery partners are working to increase the UK's educational capability in all fields of Cyber Security. Together BIS, EPSRC, GCHQ, CPNI and OCSIA have developed a joint approach and strategy for reaching this goal. As part of that strategy, through the GCHQ Certified Training (GCT) scheme, GCHQ intends to certify cyber security training courses, which are available to anyone and not just the Public Sector. The GCT scheme is designed to provide confidence in cyber security training providers and the courses that they offer.

## Overview

As part of the GCT scheme, each training course will be assessed against the nominated area(s) of the Institute of Information Security Professionals (IISP) Information Security Skills Framework. As part of the application process, applicants will be asked to identify which skill(s) group(s) the training course covers. This self-assessment will then be used as the basis for assessment. In support of this, GCHQ has provided indicative topic coverage for each of the IISP skills groups. The topic coverage provided is the same as that used by the assessment process for the GCHQ certification of masters degrees, which provide a general, broad foundation in cyber security. This is intentional as it provides a common baseline for cyber security capability from awareness and training, to that used at the highest levels of academic pursuit.

## Course Structure

Training providers will be able to submit two types of courses for assessment: courses which provide a fundamental coverage of nominated area(s) of the IISP Skills Framework, or courses which provide in depth coverage. Training providers will be asked to indicate this as part their submission for assessment under the GCT scheme. Courses can provide either a fundamental or in depth coverage in one or more of the IISP skill(s) group(s).

*Eighty per cent* of the learning time of the training course must cover the IISP skill(s) group(s) as nominated by the training provider in their self-assessment.

It is *expected* that a training course at the **Awareness Level** will:

- Provide an introduction, awareness and overview of one or more of the nominated IISP skill(s) group(s)
- Be applicable for those who are taking up a new cyber security role or wishing to enter the

profession
- Not require any training, professional or academic prerequisites
- Not have to include any self-study
- Not have to provide any practical/'hands-on' learning
- Not have to include formal examination or assessment although this can be offered if required

It is *expected* that a training course at the **Application Level** will:

- Provide a detailed insight and understanding of one or more of the nominated IISP skill(s) group(s)
- Be applicable for those who are already performing a cyber-security role and wish to further their professional capability
- Require training, professional or academic prerequisites
- Typically run for two or more days
- Include self-study
- Provide practical/'hands-on' learning
- Include formal examination or assessment, which could form part of a professional certification

## The Assessment Process

APM Group (APMG) will assess three distinct areas of course delivery.

The quality management systems of the training provider will be checked to ensure the management of applicants, their personal details and the delivery of training is consistent, efficient and effective.

The trainers will be assessed for their teaching ability and their technical knowledge in the IISP skill(s) group(s) covered by the course being assessed.

The course materials will be assessed to ensure they deliver the expected level of learning to delegates, in a way that is effective such that it provides the best opportunity for the delegates to feel they have received a high quality training course. The course certificate will detail the IISP skill(s) group(s) covered and the type of training offered (awareness or practical), such that prospective applicants will have a full understanding of what to expect from the course. The marketing for the course will also be assessed to ensure it does not mislead potential applicants.

Certifications of training courses by APMG will be subject to a set of terms and conditions (T&Cs) that all applicants will have to agree to as part of the application process.

## Topics that can be covered by Cyber Security Training Courses in Support of the GCT Scheme

*The Security Discipline Principles and Skills Groups that form part of the tables in this document are derived from the IISP Information Security Skills Framework and are copyright © The Institute of*

Version 2.0; 08 January 2016



The information within the tables is intended to provide an indicative mapping of potential topic coverage to the IISP Skills Framework[1]. The tables are structured on the basis of Security Disciplines that lead to a series of Indicative Topics:

a. The set of Security Disciplines and Principles has been taken from the IISP Skills Framework, along with summary versions of the associated Knowledge Requirements expressed in CESG's[2] March 2014 document on Certification for IA Professionals.[3]

b. The Skills Groups are based upon those expressed in the IISP framework, but with some of the groups having been merged together where appropriate (e.g. where Training Courses would be unlikely to be focusing their coverage or where the treatment of the Skills Groups would essentially encompass the same topics). A new Skills Group on Control Systems has been added to reflect the growing importance of this subject area.

c. To help with later referral, the Skills Groups have been numbered *i* to *xiv*. The IISP Skills Groups to which they refer are also shown (e.g. *A2, A5*, etc.).

d. The Indicative Topic Coverage highlights examples of the specific topics that one would expect to see represented within the syllabi of Training Courses in order for broad coverage of the related Skills Group to be achieved. Given that they are indicative topics, courses would not be required to cover all of them explicitly (and indeed other topics may additionally be relevant), but there would be expected to be sufficient weight of coverage within each area if the Skills Group was to be satisfactorily addressed.

[1] IISP Skills Framework:
https://www.iisp.org/imis15/iisp/Accreditation/Our_Skills_Framework/iisp/About_Us/Our_Skills_Framework.aspx?hkey=e77a6f03f9498f423efaa7bf585381290ec4

[2] CESG is the information security arm of GCHQ: http://www.cesg.gov.uk

[3] CESG Certification for IA Professionals: http://www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **A. Information Security Management**<br><br>*Principle: Capable of determining, establishing and maintaining appropriate governance of (including processes, roles, awareness strategies, legal environment and responsibilities), delivery of (including polices, standards and guidelines), and cost-effective solutions (including impact of third parties) for information security within a given organisation).*<br><br>*GCHQ Knowledge Requirements include:*<br><br>*Management frameworks such as ISO 27000 series*<br>*Legislation such as Data Protection Act*<br>*Common management Frameworks such as ISO 9000* | **i. Governance, Policy, Strategy, Innovation, Awareness and Audit (A1, A2, A3, A4, A5, G1)** | • The role and function of security policy<br>• Types of security policy<br>• Security standards (e.g. ISO/IEC 27000)<br>• Security concepts and fundamentals<br>• Security roles and responsibilities<br>• Security professionalism<br>• Governance and compliance requirements in law<br>• Security culture<br>• Awareness raising methods<br>• Acceptable use policies<br>• Security standards and certifications<br>• Understanding auditability<br>• The internal audit process<br>• Methods for realising business benefit<br>• Risk managed business and operational processes |
| | **ii. Legal & Regulatory Environment, Third Party Management (A6, A7)** | • Computer Misuse legislation<br>• Data Protection law<br>• Intellectual property and copyright<br>• Employment issues<br>• Regulation of security technologies<br>• Third party management<br>• Methods for establishing confidence in third parties |

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **B. Information Risk Management**<br><br>*Principle: Capable of articulating the different forms of threat to, and vulnerabilities of, information systems and assets. Comprehending and managing the risks relating to information systems and assets.*<br><br>*GCHQ Knowledge Requirements include:*<br><br>*Information risk management methodologies such as ISO 27005 - Information Security Risk Management*<br>*Generic risk management methodologies such as ISO 31000 – Risk Management; Principles & Guidelines*<br>*Key concepts such as threats, vulnerabilities, business impacts, and risk tolerance* | **iii. Risk Assessment and Management (B1, B2)** | • Threat, vulnerability and risk concepts<br>• Threat landscape, adversarial thinking<br>• Asset valuation and management<br>• Business impact of risk<br>• Risk analysis methodologies<br>• Handling risk and selecting countermeasures/controls to mitigate risk<br>• Understanding impacts and consequences<br>• Security economics |

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **C. Implementing Secure Systems**<br><br>*Principle: Comprehends the common technical security controls available to prevent, detect and recover from security incidents and to mitigate risk. Capable of articulating security architectures relating to business needs and commercial product development that can be realised using available tools, products, standards and protocols, delivering systems assured to have met their security profile using accepted methods*<br><br>*GCHQ Knowledge Requirements include:*<br><br>• *Security Architectures and Patterns*<br>• *Secure Development processes*<br>• *Business requirements*<br>• *Skills frameworks (e.g. SFIA)*<br>• *Architectural frameworks (e.g. The Open Group Architecture Framework – TOGAF)*<br>• *Range of core security technologies (e.g. Access control models, encryption, Authentication techniques) and how to apply them* | **iv. Security Architecture (C1)**<br>**v. Secure Development (C2)** | • **Design and development considerations**: trusted computing base, security architecture and patterns, security models and design principles (e.g., principle of least privilege, fail-safe defaults), software (program) security, emission security<br>• **Selecting and applying core technologies**: authentication, access control, privacy controls, security protocols<br>• **Recognising security needs across platforms:** operating system security, Web security, embedded security, cloud and virtualisation security, security as a service<br>• **Cryptography**: cipher and algorithm types, applications to confidentiality, integrity and authentication, PKI<br>• **Network security**: Internet security protocols, tunnelling, VPNs, network attack and defence, TLS<br>• **Human factors:** usable security, psychology of security, insider threat<br>• **Security systems development**: managing secure systems development, principles of secure programming, formal approaches, understanding implementation errors and exploits. |
| | **vi. Control Systems** | • SCADA and SMART Systems, cyber system of systems (from abstract to physical effect), non-IP protocols and standards (e.g., WiFi, Bluetooth, GSM, CAN, MODBUS), cyber-physical systems analysis, embedded systems, assurance of control systems hardware and software, design/implementation methodologies to minimise the risk of vulnerabilities, risk modelling and risk-based decision making |

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **D. Information Assurance Methodologies and Testing**<br><br>*Principle: Develops and applies standards and strategies for verifying that measures taken mitigate identified risks.*<br><br>*GCHQ Knowledge Requirements include:*<br>• *Assessment Methodologies (e.g. Common Criteria)*<br>• *Information Risk Management Frameworks, Assessment services or standards (e.g. CHECK)*<br>• *Governance aspects and Management responsibilities*<br>• *Testing strategies and methodologies (e.g., TEMPEST testing)* | **vii. Information Assurance Methodologies (D1)**<br><br>**viii. Security Testing (D2)** | • Assessment methodologies (e.g. 27000 series and Common Criteria)<br>• Understanding security vulnerabilities and related mitigation measures<br>• System and software testing<br>• Penetration testing<br>• Security metrics<br>• Static and dynamic analysis of products and systems |

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **E. Operational Security Management**<br><br>*Principle: Capable of managing all aspects of a security programme, including reacting to new threats and vulnerabilities, secure operational and service delivery consistent with security polices, standards and procedures, and handling security incidents of all types according to common principles and practices, consistent with legal constraints and obligations.*<br><br>*GCHQ Knowledge Requirements include:*<br><br>• *Governance and Management responsibilities*<br>• *IT Service Management processes (e.g. ITIL)*<br>• *Existing and Emerging Vulnerabilities*<br>• *Use of penetration testing and vulnerability testing*<br>• *Risk Assessment and Monitoring*<br>• *Operating Procedures and accountability*<br>• *Continuous improvement* | **ix. Secure Operations Management and Service Delivery (E1, E2)** | • **Internet threats: c**ommon attacks (human and technical), malicious code, situational awareness, threat trends, threat landscape, CERTs, adversarial thinking<br>• **Cryptography**: AES and RSA, key management, digital signatures<br>• **Network security**: networking fundamentals, firewalls and traffic filtering, intrusion detection and prevention systems, intrusion analysis, network monitoring, mobile and wireless network security<br>• **System security**: authentication (secrets, tokens, biometrics), access control (MAC, DAC, RBAC) and privilege management, mobile device security and BYOD, anti-virus technologies<br>• **Application security**: email, Web, social networks, DRM, database security, big data security, identity management<br>• **Physical security**: physical and environmental controls, physical protection of IT assets |
| | **x. Vulnerability Assessment (E3)** | • Malware analysis: static and dynamic analysis, detection techniques, host-based intrusion detection, kernel rootkits<br>• System and network-level vulnerabilities and their exploitation<br>• Vulnerability analysis and management<br>• Penetration testing<br>• Social Engineering<br>• Dependable/resilient/survivable systems |

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **F. Incident Management**<br><br>*Principle: Capable of managing or investigating an information security incident at all levels.*<br><br>*GCHQ Knowledge Requirements include:*<br><br>• *Secure Information Management (stakeholder management within organisational context)*<br>• *Incident detection techniques*<br>• *Incident response management (internal and external)*<br>• *Audit log management*<br>• *Forensics (e.g. Evidential standards, Tools, Impact assessment)* | **xi. Incident Management (F1)** | • Intrusion detection methods<br>• Intrusion response<br>• Intrusion management<br>• Incident handling<br>• Intrusion analysis, monitoring and logging |
| | **xii. Investigation (F2)** | • Understanding of legislation and legal constraints<br>• Evidence gathering rules and techniques |
| | **xiii. Forensics (F3)** | • Collecting, processing and preserving digital evidence<br>• Device forensics<br>• Memory forensics<br>• Network forensics<br>• Anti-forensic techniques<br>• Forensic report writing and expert testimony |

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **G. Audit, Assurance & Review**<br><br>*Principle: Capable of defining and implementing the processes and techniques used in verifying compliance against security policies, standards, legal and regulatory requirements.*<br><br>*GCHQ Knowledge Requirements include:*<br>• Audit methodologies (e.g., Certified Information Systems Auditor - CISA)<br>• Vertical/horizontal auditing techniques<br>• Audit processes and techniques (e.g. HMG IA Maturity Model) | The Audit and Review Skills Group (G1) has been incorporated into Skills Group i above | The indicative topic coverage has been included in Skills Group i above |

| Security Discipline | Skills Group | Indicative Topic Coverage |
|---|---|---|
| **H. Business Continuity Management**<br><br>*Principle: Capable of defining the need for, and of implementing processes for, establishing business continuity.*<br><br>*GCHQ Knowledge Requirements include:*<br><br>• *Business continuity management lifecycle*<br>• *Business Impact Analysis process*<br>• *Related standards (e.g. ISO 22301, ISO 27001, BS 25999, BS 27031)* | **xiv. Business Continuity Planning and Management (H1, H2)** | • Continuity Planning<br>• Backup<br>• Disaster recovery |
| **I. Information Systems Research – N/A**<br>*Principle: Original investigation in order to gain knowledge and understanding relating to information security, including the invention and generation of ideas, performances and artefacts where these lead to new or substantially improved insights; and the use of existing knowledge in experimental development to produce new or substantially improved devices, products and processes.* | **xv. Research (I2) – N/A** | N/A |
| **J. Professional Skills – N/A** | No IISP reference – N/A | N/A |