Assessors Panel

CREST Intrusion Analysis & Incident Management Syllabus

Issued by	CREST Assessors Panel
Document Reference	C-IA-EX01
Version Number	6.0
Status	Public Release
Issue Date	4th April 2014

Table of Contents

1 Introduction 4

1.1 CREST Certified Network Intrusion Analyst (CCNIA) 4

1.2 CREST Certified Host Intrusion Analyst (CCHIA) 4

1.3 CREST Certified Malware Reverse Engineer (CCMRE) 4

1.4 CREST Registered Intrusion Analyst (CRIA) 4

1.5 CREST Certified Incident Manager (CCIM)

Error! Bookmark not defined.

2 Certification Examination Structure 5

3 Syllabus Structure 6

Appendix A - Soft Skills and Incident Handling 7

Appendix B - Core Technical Skills 10

Appendix C - Background Information Gathering & Open Source 14

Appendix D - Network Intrusion Analysis 16

Appendix E - Analysing Host Intrusions 21

Appendix F - Reverse Engineering Malware 26

Appendix G - Incident Management 29

Appendix H – Computer Networking Fundamentals (Core Skill) 33

Appendix I - Virtualisation Technologies 38

Appendix J - Platform Security 40

Appendix K - Identification and Access Management 44

Appendix L - Applications 45

Appendix M - Security Methodologies 47

Appendix N - Security Vulnerabilities & Prevention Techniques 49

Version History

Version	Date	Comments	Status
0.1	22nd December 2010	Assessors Panel	Draft
0.2	29th December 2010	Minor revisions	Draft
0.3	10th January 2011	Minor revision and issued for comment	Draft
0.4	25th January 2011	Amendments following syllabus review	Draft
1.0	12th September 2011	Technical Committee and Assessors Panel	Public Release
1.1	11th November 2011	Minor Revisions	Draft
2.0	14th November 2011	Amended to include CRIA syllabus	Public Release
3.0	1st August 2013	Logo Update	Public Release
4.0	8th August 2013	Section G added – Incident Management	Internal Release
5.0	4th April 2014	Additional Appendices added for CCIM exam	Internal Release
6.0	4th April 2014	Header amended. Appendices G-K amended to CCIM only	Public Release

Document Review

Reviewer	Position
Chair	Assessors Panel
Chair	CREST Board

1 Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the Certification examinations in the area of Intrusion Analysis. There are specialist exams for each subject area and a core skills exam which covers all 3 areas:

1.1 CREST Certified Network Intrusion Analyst (CCNIA)

The (CCNIA) examination tests candidates' knowledge and expertise in analysing data sources for evidence relating to potential network compromise.

1.2 CREST Certified Host Intrusion Analyst (CCHIA)

The (CCHIA) examination tests candidates' knowledge of analysing Windows hosts for evidence of potential compromise.

1.3 CREST Certified Malware Reverse Engineer (CCMRE)

The (CCMRE) examination tests candidate's ability to reverse engineer malware, particularly remote access Trojans.

1.4 CREST Registered Intrusion Analyst (CRIA)

The (CRIA) examination tests a candidates' knowledge across all 3 subject areas.

1.5 CREST Certified Incident Manager (CCIM)

The (CCIM) examination tests a candidates' knowledge across a wider range of areas including traditional incident response technical tasks and also a wide range of general technology areas to ensure they are competent to assess and handle a wide range of potential incident scenarios. The level of detail in these areas is high level but broad with "an awareness of" being a good description of the level of detail required. The specific Appendix G section for this exam focusses in detail on core response manager skills and the level of detail required here is greater as this is assumed to be the core domain of knowledge for an incident manager.

All Intrusion Analyst Certification examinations also cover a common set of core skills and knowledge; success at any of these Examinations will confer the relevant CREST Registered/Certified status to the individual.

2 Certification Examination Structure

The technical Certification Examinations have two components: a written paper and a practical assessment.

In the certified tester exams, the written paper consists of two sections: a set of multiple choice questions and a selection of long form questions that will require longer written answers. The registered tester written section contains only multiple choice questions.

The practical assessment tests candidates' abilities to analyse data provided to the candidate.

The incident manager exam does not have a practical test element but has a mix of multiple choice, long form and detailed scenario type questions.

The relevant Notes for Candidates document for the Certification Examinations provides further information regarding the Certification Examinations in general and the skill areas that will be assessed within the practical components.

3 Syllabus Structure

The syllabus is divided into ten knowledge groups (Appendices A to J below), each of which is subdivided into specific skill areas.

For each skill area, CREST has indicated where and how the area will be assessed: in which Certification Examination (Network Intrusion Analysis, Host Intrusion Analysis or Malware Reverse Engineering) and in which component (Written Multiple Choice, Written Long Form, or Practical).

Within the tables, the following acronyms apply:

CCNIA	CREST Certified Network Intrusion Analysis
CCHIA	CREST Certified Host Intrusion Analysis
CCMRE	CREST Certified Malware Reverse Engineer
CRIA	CREST Registered Intrusion Analyst
CCIM	CREST Certified Incident Manager
MC	Written Multiple Choice
SF	Written Short Form
LF	Written Long Form
P	Practical

Appendix A - Soft Skills and Incident Handling

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
A1	Engagement Lifecycle Management	Benefits and utility of incident response to the client. Awareness of steps that can be taken to prepare for potential incidents. Structure of incident response engagements, including the relevant processes and procedures. Knowledge of appropriate actions that should be taken when investigating an incident. Understanding that some actions should be avoided due to risk of evidence corruption. Know how to safely handle malware and potentially malicious files encountered during an engagement. Understanding limitations of system logs.	MC LF	MC LF	MC	MC	MC SF LF
A2	Incident Chronology	Use of timelines to analyse event data Time zone issues System interpretation of timestamps with images	MC LF P	MC LF P	MC	MC P	MC SF LF
A3	Law &	Knowledge of pertinent UK legal	MC	MC	MC	MC	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
	Compliance	issues: Computer Misuse Act 1990 Human Rights Act 1998 Data Protection Act 1998 Police and Justice Act 2006 Regulation of Investigatory Powers Act 2000 Criminal Justice Act 2008 Protection of Children Act 1978 Sexual Offences Act 2008 Digital Millennium Copyright Act and consequences for reverse engineering. Knowledge of evidential integrity and chain of custody. Awareness of sector-specific regulatory issues (e.g. FSA, PCI). Understanding of situations that require notification of third-parties. Understanding of when and how to engage law enforcement Knowledge of CERTS and their role and jurisdiction Add some new laws Money laundering? Anti-terrorism					SF
A4	Record Keeping,	Understanding reporting	P	P	P	P	SF LF

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
	Interim Reporting & Final Results	requirements. Understanding the importance of accurate and structured record keeping during the engagement.					V
A5	Threat Assessment	Understanding how a threat translates to the client and the business context of a given incident. High level methodologies surrounding threat assessment. Attribution of attacks. Knowledge of attacker motivation. Identifying key individuals likely to be selected for targeted attack.	LF MC	LF MC	LF MC	MC	MC SF LF

Appendix B - Core Technical Skills

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
B1	IP Protocols	IP protocols: IPv4 and IPv6, TCP, UDP and ICMP. Detailed knowledge of application layer protocols commonly used by Trojan malware, namely TCP, UDP, HTTP[S], SMTP, and DNS. In-depth understanding of how the Internet (web browser/server architecture) and email systems function. Fundamental knowledge of at least the following protocols; IRC, DHCP, FTP, SMB, SNMP, ICMP.	MC LF	MC	MC	MC P	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
B2	Network Architectures	Varying networks types that could be encountered during a analysis engagements: CAT 5/6 Basic understanding of common fibre technologies Windows Domain architectures Network Address Translation 10/100/1000baseT Wireless (802.11) Security implications of shared media, switched media and VLANs. IP Subnets IP Routing	MC LF	MC	MC	MC	MC SF LF
B3	Common Classes of Tools	Knowledge of common classes of tools used to perform intrusion analysis and reverse engineering. Basic understanding of the capabilities of common tools.	MC	MC	MC	MC P	MC
B4	OS Fingerprinting	Passive operating system fingerprinting techniques.	MC P	MC		MC P	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
B5	Application Fingerprinting	Determining server types and network application versions from evidential data. Identification of client software versions from meta-data contained within common document types. Identification of client/server software versions from service banners, user-agent strings, email headers etc.	MC P	MC P		MC P	MC
B6	Network Access Control Analysis	Reviewing firewall rule bases and network access control lists.	MC LF P	MC P		MC P	MC SF LF
B7	Cryptography	Differences between encryption and encoding. Symmetric / asymmetric encryption Encryption algorithms: DES, 3DES, AES, RSA, RC4. Hashes: SHA family and MD5 Message Integrity codes: HMAC	MC LF	MC LF	MC LF	MC	MC SF LF
B8	Applications of Cryptography	SSL, IPsec, SSH, PGP Common wireless (802.11) encryption protocols: WEP, WPA, TKIP	MC	MC	MC	MC	MC SF LF

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
B9	File System Permissions	File permission attributes within Windows file systems and their security implications. Analysing registry ACLs.	MC	P MC LF	MC	MC P	MC
B10	Host Analysis Techniques	Listing processes and their associated network sockets (if any). Assessing patch levels on a Windows host using the command prompt. Finding interesting files on a Windows host.	MC	MC P	MC	MC P	MC
B11	Understanding Common Data Formats	Candidates are expected to be able to interpret email headers, commenting on the reliability of the information contained within. Understanding of the information contained within a PKI certificate Understanding of various encoding employed for transmission of data (e.g. web and email)	MC LF	MC LF	MC	MC	MC

Appendix C - Background Information Gathering & Open Source

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
C1	Registration Records	Information contained within IP and domain registries (WHOIS).	MC	MC	MC	MC	MC
C2	Domain Name Server (DNS)	DNS queries and responses DNS zone transfers Structure, interpretation and analysis of DNS records: • SOA • MX • TXT • A • NS • PTR • HINFO • CNAME Awareness of dynamic DNS providers, how they function and security implications. Understand the concept of fast-flux DNS.	MC LF P	MC	MC	MC P	MC
C3	Open Source Investigation and Web Enumeration	Effective use of search engines and other open source intelligence sources to gain information about a target. Knowledge of information that can be retrieved from common social networking sites	MC	MC	MC	MC	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
C4	Extraction of Document Meta Data	Be able to extract meta-data such as author, application versions, machine names, print and operating system information from common document formats.	MC P	MC		MC	MC
C5	Community Knowledge	Ability to interpret common anti-virus threat reports Ability to interpret open-source research when investigating incidents, eliminating false positives. Knowledge of popular open-source security resources (web sites, forums, etc.).	MC LF	MC LF	MC	MC	MC SF LF

Appendix D - Network Intrusion Analysis

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
D1	Network Traffic Capture	Methods of data collection and types of data to be collected. Designing a collection system to ensure sufficient data is collected without overwhelming capture devices. Impact assessment of any changes to network. Knowledge of SPAN ports, traditional network TAPs and aggregating TAPs. Ability to estimate capture requirements during scoping. Consideration of appropriate capture device deployment location. Constraints and limitations of capture and analysis toolsets. Knowledge of different capture options (e.g. NetFlow, limited capture, full packet capture etc.) The ability to assure integrity and security of network after introduction of a capture device Provide arguments and evidence that supports the integrity of any data captured.	MC LF P			MC P	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
D2	Data Sources and Network Log Sources	Types of data to be collected and existing data sources which should be considered to provide a complete picture of activity. Candidates should be familiar with the type of information provided in at least the following: • Proxy logs • syslogs • Email logs • Firewall logs • DHCP logs • VPN logs • Web server logs • Antivirus logs • DNS logs • Domain logs • Windows event logs • Internet history • Database logs Correlation of information contained within any number of different log formats.	MC LF P	MC LF		MC P	MC SF LF
D3	Network configuration security issues	Observation/detection of common network misconfiguration issues such as: • IP Routing issues • DNS information leakage • Unexpected traffic routes • Email routing issues • Firewalls/rules not working	MC P			MC P	MC SF LF

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
		Detection of deliberate attempts to bypass firewall/proxy rules.					
D4	Unusual Protocol Behaviour	Observation/detection of common protocols exhibiting non-standard behaviour. Verification of various protocols regardless of TCP/UDP port in use. Identification of illegal protocol usage for purposes of vulnerability exploitation or cache poisoning etc.	MC LF P			MC	MC
D5	Beaconing	Ability to recognise and detect both covert and open malware beacons from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC LF P	MC		MC P	MC SF LF
D6	Encryption	Understanding of channel fingerprinting. Analysis of traffic flows (volume, directions, QoS, timing, custom or standard encryption). Identification of weak obfuscation using XOR, ROL or codebooks and approaches to deobfuscation.	MC LF P			MC	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
D7	Command and Control Channels	Ability to recognise and detect both covert and open C&C from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC LF P			MC P	MC SF LF
D8	Exfiltration of Data	Ability to recognise and detect both covert and open exfiltration of data from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC LF P	MC		MC P	MC SF LF
D9	Incoming attacks	Detect successful incoming attacks against public facing services, including email, from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC LF P			MC P	MC
D10	Reconnaissance	Detect internal and external reconnaissance activities from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC LF P			MC P	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
D11	Internal spread and privilege escalation	Detect the spread of malware within a network and indicators of privilege escalation from statistical analysis and manual review of traffic that may include a variety of different IP protocols and logs.	MC LF P			MC P	MC SF LF
D12	Web based attacks	Ability to identify potentially malicious elements within html and other common web file types Ability to decode obfuscated JavaScript code and determine whether or not the code is malicious in nature.	MC LF P	MC LF P		MC	MC SF LF
D13	False Positive Acknowledgement	Determine whether or not a given IDS alert is a true hit or false positive. Suggest improvements to common IDS signatures to reduce false positive rates.	MC LF P			MC P	MC

Appendix E - Analysing Host Intrusions

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
E1	Host-based Data Acquisition	Fundamental acquisition concepts, techniques and methodologies, including static and dynamic evidence gathering and image formats. Local and remote acquisition scenarios.		MC LF		MC	MC
E2	Live Analysis Laboratory Set-up	Basic infrastructure configurations Host hardening and sandbox environments Booting an image Issues relating to dynamic analysis of executables		MC LF	MC	MC	MC
E3	Windows File System Essentials	Disk partitioning FAT – File Allocation Table, directory entries NTFS – $MFT, $Bitmap ACLs & SIDs Unallocated space File carving EFS & BitLocker		MC LF P	MC	MC	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
E4	Windows File Structures	Browser artefacts Prefetch Volume Shadow Copy System Restore Points User profiles Temporary files Network configuration (hosts file) Pagefile & hibernation file		MC LF P	MC	MC P	MC
E5	Application File Structures	Archive formats (Zip, RAR, etc) PE files Office documents (macros, etc) PDF Email file structures (Exchange, PST) AV artefacts (quarantines and logs) Thick-client files (Java, Flash, .NET)	MC	MC LF P	MC	MC P	MC
E6	Windows Registry Essentials	Registry structures (hive format) USB/removable storage artefacts Autorun/startup locations ACLs Protected storage		MC P	MC	MC P	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
E7	Identifying Suspect Files	Use of hash tables to find common malware Strings File permissions Packed executables Fuzzy hashing Signature analysis	MC P	MC LF P		MC P	MC
E8	Storage Media	Hard Disks – Interface types (PATA/SATA, SCSI, SAS), HPA, DCO, Password protection Solid State Devices – Hard Disks, Pen Drives, Media Cards, wear levelling issues, how this media type varies from magnetic Full Disk Encryption RAID – levels of RAID type and error correction NAS	MC	MC		MC	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
E9	Memory Analysis	Analysis – running processes, parent/child process identification, DLLs, sockets Process Acquisition Clipboard contents Start up – encryption password identification Correlating memory artefacts with on-disk applications		MC LF P	MC LF	MC	MC
E10	Infection vectors	Infected Executables/DLL, Documents (Macros), JavaScript Drive-by downloads USB/external media/shared drive vectors Passive exploitation Email-based attacks	MC LF P	MC LF P	MC LF	MC P	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
E12	Malware Behaviours and Anti-Forensics	Encryption Steganography Password Protection Obfuscation Covert storage techniques Covert communication techniques (command and control, recon, and exfiltration) Data Erasure Applications Filing System – NTFS ADS		MC LF P	MC LF	MC	MC
E13	Rootkit Identification	How to identify rootkits Hooking techniques		MC LF P	MC LF	MC	MC
E14	Live malware analysis	Identification of open files/registry keys/network sockets Process monitoring tools		MC LF P	MC LF	MC P	MC

Appendix F - Reverse Engineering Malware

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
F1	Windows Anti-Reverse Engineering	Common techniques to prevent debugging or virtualisation of the malware code and ways of circumventing them. Known anti-reverse engineering techniques including high profile bugs in common debuggers and disassemblers.			P MC	MC	MC
F2	Functionality Identification	Identifying common cryptographic algorithms in binaries through, for example, use of standard constants and common instructions. Identifying network send/receive loops Infection vectors and persistence mechanisms			P LF	MC P	MC
F3	Windows NT Architecture	Core architecture of NT kernel and user mode, including process model and security mechanisms (Windows XP and newer) NT Native APIs, Driver interfaces Differences between 64 bit and 32 bit platforms		MC	MC	MC	MC
F4	Windows API Development	Common API calls, e.g. file, network.			MC	MC	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
F5	Binary code structure	Function calling conventions Compiler generated constructs, e.g. binary implementation of C++ objects (Virtual Function Table etc.)			MC	MC	MC
F6	Cryptographic Techniques	Encryption Key material identification and extraction Identifying implementation weaknesses			LF P	MC	MC
F7	Processor Architectures	Intel x86/x64 instruction set Virtual Memory Implementation Virtualisation Technology			MC	MC P	MC
F8	Windows Executable File Formats	Standard windows executable formats (e.g. PE, EXE, COM) Extracting important information in executable files		MC	MC P	MC P	MC
F9	Hiding Techniques	Common techniques for process injection Rootkit techniques for hiding files and other system resources including: • SSDT patching • Filter drivers • Process list manipulation			MC LF P	MC	MC

ID	Skill	Details	How Examined				
			CC NIA	CC HIA	CC MRE	CR IA	CC IM
F10	Malware Reporting	Signature identification Cleanup of malware Infection vectors Footprint	MC	MC	MC LF	MC	MC
F11	Binary Obfuscation	Packers and Executable Encryption Techniques to restore packed executables Rebuilding executable content from memory Virtual machine instruction sets (e.g. PCode)	MC	MC	MC P LF	MC	MC
F12	Behavioural Analysis	Use of common tools to identify patterns of behaviour Aspects of command and control Infection vectors and persistence mechanisms	MC	MC	MC P LF	MC P	MC

Appendix G - Incident Management

ID	Skill	Details	How Examined CCIM only
G1	Client management	Client and project including effective management of the people involved during volatile and highly charged situations.	MC SF LF
G2	Containment techniques	Containment techniques with short and medium term actions that are properly considered and risk assessed for each environment. This requires an awareness of business continuity arrangements and requirements for the wider business.	MC SF LF
G3	Project management and time management	Project management and time management are essential investigative and management skills for managing staff, costs and deliverables to meet client requirements. Contracts, NDAs, scope and authorisation all need careful proactive management during an engagement	MC SF LF
G4	Evidence handling	Evidence handling and control and management of the evidential chain require a qualified person to take control of the situation, keep the appropriate logs and take the necessary actions to preserve evidential integrity.	MC SF LF
G5	Communications	Communications both to the client and also to third parties needs to be carefully managed and scripted to avoid misinformation spreading and messages being poorly understood. This involves working with PR and branding teams to ensure all media contact is appropriately managed. This may require use of an existing crisis management plan.	MC SF LF

ID	Skill	Details	How Examined CCIM only
G6	Recovery and remediation	Recovery and remediation options are necessarily very client and project specific. Appropriate guidance is needed based on multiple requirements such as time, cost and on-going threat.	MC SF LF
G7	On-going technical prevention	Once an environment has been cleared of malware it essential to ensure that measures are in place for on-going technical prevention. These may be changes to business practices, user environments or architectural changes to security at a wider organisational level.	MC SF LF
G8	Judgement making and critical reasoning	When working in volatile situations it is essential that the on-going drip feed of information is used to update the understanding of the situation in near real time. This requires critical reasoning and judgement making skills and the willingness to completely change a position as new information comes to light.	MC SF LF
G9	Written skills	Written comprehension is a key part of taking information from the numerous reports and data sources available.	MC SF LF
G10	Third Parties	Dealing with external third parties in a knowledgeable way is becoming an ever more important part of incident response as more services are being offloaded to SaaS, IaaS and other cloud offerings.	MC SF LF

ID	Skill	Details	How Examined CCIM only
G11	Reporting Agencies	Dealing with external reporting bodies often falls within the remit of an incident manager, even if this is only a case of explaining to a client who needs to be contacted. Awareness of relevant CERTs, government agencies and public bodies (eg FSA) is essential.	MC SF LF
G12	Threat intelligence, Contextualisation Attribution and Motivation.	Keeping up to date with threat intelligence and situational awareness is essential. This can include open source information, company specific research and also classified sources. Identifying likely actors and their motivation.	MC SF LF
G13	Industry Best Practice	Awareness of industry best practice and open/industry standards (SANS, ENISA, NIST and ISO standards) GPG13 and Forensic readiness planning (SPF)	MC SF LF
G14	Risk Analysis	Business Impact Assessments Awareness of the relevance and importance of Risk Assessments and Business Impact Assessments to the role of an incident manager in providing appropriate guidance to a client organisation.	MC SF LF
G15	Attack & compromise lifecycle.	Attack / compromise lifecycles (kill chain). Anatomy of an attack and the key components and stages of an incident. Compromise, Disruption, Extraction of data, etc.	MC SF LF
G16	Legal and Jurisdictional Issues	Complexities of remote and international working, including legal and jurisdictional issues and also the added complexity of remote capture over variable quality WAN links.	MC SF LF

ID	Skill	Details	How Examined CCIM only
G17	Ethics	An awareness of the strong ethical requirements needed when working in incident response. This includes a detailed understanding of the CREST Code of Conduct and an the responsibilities it places on individuals and companies.	MC SF LF
G18	Technical vulnerability root cause identification	Technical vulnerability root cause identification requires seeing further than the technical issues and identifying business level strategic failures that allowed a problem to occur in the first place. Missing patches may be accidental or endemic and may reoccur if the root cause is not identified and treated.	MC SF LF
G19	Physical threats	An awareness of potential physical threats that provide may provide network access is required. Many attacks may be a blend of logical and physical attacks, such as those originating from public access locations or wireless networks.	MC SF LF
G20	Insider attacks	An awareness of potential insider attacks and attacks that start with exploiting human targets. This includes lost hardware such as media sticks, laptops, phones and other portable devices.	MC SF LF

Appendix H – Computer Networking Fundamentals (Core Skills)

ID	Area	Details	How is it Examined CCIM only
H1	Wireless Networking	Understanding the existence and use of varying networks types that could be encountered during an architecture project: • Wireless (802.11a) • Wireless (802.11b/g/n) • WiMax • Microwave Point to Point • Optical Point to Point • 2G/3G/4G (GSM, GPRS, HSDPA) • TETRA	MC
H2	Virtual Private Networks	Understanding the existence and use of varying VPN types that could be encountered during an architecture project: • Point to Point • Roaming remote user • Virtual Circuits / Tagging • IPSEC • PPTP • L2TP • SSL/TLS • SSTP • DMVPN • MPLS	MC
H3	ICMP	Understanding the existence and uses of ICMP messages and how the various message types can be useful in designing and debugging a network architecture.	MC

ID	Area	Details	How is it Examined CCIM only
H4	Ipv6	Understanding the existence and benefits of Ipv6 together with potential pitfalls to early adopters and issues around interoperability with existing legacy systems.	MC
H5	DNS	Understanding the existence and use of DNS protocol and services both within the public Internet and also within corporate networks. This will specifically include the role of DNS within Microsoft Active Directory. • DNS queries and responses • DNS zone transfers • Public DNS Hierarchy & Authorities • DNS Security Options & Risks • Reverse DNS Structure and interpretation of key types of DNS record entries: • MX • A • NS • PTR • CNAME	MC
H6	NTP	Understanding the existence and use of NTP protocol and services both within the public Internet and also within corporate networks. This will specifically include the importance of NTP within logging and monitoring solutions. • Time sources • Authoritative sources • Time synchronisation	MC

ID	Area	Details	How is it Examined CCIM only
H7	Bluetooth	Understanding the existence and use of Bluetooth protocol and services and their implications for the security of the wider corporate network architecture. • Potential Attack Vectors • Range Limits • File Transfer • Personal Area Data Networking	MC
A8	Ipv4	Ipv4 network fundamentals including understanding of • IP addresses • Subnet Masks • Public / Private IP Space • ARP protocols • Network Address Translation • Fragmentation • Quality of Service • CIDR	MC
H9	TCP/UDP	TCP/UDP network fundamentals including the implications of • Connection orientated links • Connectionless links • Resilience / Packet Loss • Applications of TCP versus UDP	MC
H10	Routing Protocols	Routing fundamentals including an understanding of • CIDR • RIP • OSPF • EIGRP • Static Routing • Failover • HSRP • BGP	MC

ID	Area	Details	How is it Examined CCIM only
H11	Data Link Layer	Layer 2 network fundamentals including an understanding of • Ethernet • VLANS • DSL • ISDN • PPP • ARP To include effects of packet size limits, latency, broadcast domains and the types of segregation available within these protocols.	MC
H12	Physical Layer Networks	Layer 1 physical network fundamentals including an understanding of • Copper Ethernet • Fibre Optic Ethernet • Satellite Links • Radio Links • ATM • SDH • MTU To include effects of packet size limits, latency, broadcast domains and the types of segregation available within these protocols.	MC
H13	SNMP	Understanding the existence and use of SNMP protocols for systems monitoring, particularly within corporate networks. This will specifically include the importance of SNMP within logging and monitoring solutions. • Community Strings / Authentication • Encryption • SNMP Versions	MC

ID	Area	Details	How is it Examined CCIM only
H14	Syslog	Understanding the existence and use of Syslog protocol for systems monitoring, particularly within corporate networks. This will specifically include the importance of Syslog within logging and monitoring solutions and inherent weaknesses within the protocol.	MC

Appendix I - Virtualisation Technologies

ID	Area	Details	How is it Examined CCIM only
I1	Hardware Virtualisation	Understanding the existence and use of hypervisor solutions to provide platform virtual machine solutions and the security implications (notably management issues and lack of physical segregation) of these technologies. Example – VMWare ESXi (VSphere)	MC
I2	Ethernet based Virtual LANs (VLANs)	Understanding the appropriate configuration and uses of VLAN technologies in system architecture design and the security implications (notably management issues and lack of physical segregation) of these technologies.	MC
I3	Virtualised Firewalls	Understanding the appropriate configuration and uses of virtualised firewall solutions and the security implications (notably management issues and lack of physical segregation) of these technologies. Example – Juniper Netscreen VSYS	MC
I4	Virtualised Operating Systems	Understanding the appropriate configuration and uses of virtualised operating systems and the security implications (notably management issues and lack of physical segregation) of these technologies. Example – Solaris Containers	MC
I5	Virtualised Databases	Understanding the appropriate configuration and uses of virtualised database systems and the security implications (notably management issues and lack of physical segregation) of these technologies. This will include the difference between database instances and virtual databases. Example - Oracle (11g) Virtual Private Database	MC

ID	Area	Details	How is it Examined CCIM only
I6	Cloud Technologies	Understanding the implications of Cloud solutions including Software as a Service (SaaS), Cloud hosting and Cloud Storage. Note this section refers to the specific concerns around the use of shared clouds as the virtualisation technologies employed are dealt with earlier in this section.	MC

Appendix J - Platform Security

ID	Area	Details	How is it Examined CCIM only
J1	Operating Systems	Awareness of common server and desktop operating systems and their fundamental security characteristics. To include • Microsoft Windows (all) • Sun Solaris • HP UX • AIX • Linux (all) & BSD (all) • Mac OS X	MC
J2	Hardware Thin Client systems	Awareness of common thin client hardware platforms, their base operating systems and their fundamental security characteristics. To include • Wyse ThinOS • Windows XP Embedded	MC
J3	Mobile Devices	Awareness of common mobile hardware platforms, their base operating systems and their fundamental security characteristics. To include • Apple IOS (IPhone, IPad) • Android (tablets and phones) • Windows Mobile • Blackberry	MC

ID	Area	Details	How is it Examined CCIM only
J4	Desktops	Awareness of common desktop platforms, their base operating systems and their fundamental security characteristics. To include • Laptops • Netbooks • Desktops • Windows (all) • Linux & BSD • Apple (all) • Lockdown policies (including GAP)	MC
J5	Embedded Systems	Awareness of common embedded systems and their fundamental security strengths and weaknesses • NAS Devices • IP Cameras / CCTV • NTP time sources • Logging & Monitoring solutions • Network Diagnostic equipment • Building Management Systems • HVAC Systems • Physical Security/Alarm Systems	MC
J6	SAN and NAS systems	Awareness of common SAN and NAS technologies and their fundamental security strengths and weaknesses (including management issues) • Fibre Channel • ISCSI • LUNs • Partitioning / Separation • NFS • SMBFS/CIFS	MC

ID	Area	Details	How is it Examined CCIM only
J7	Multi-Function Devices	Awareness of common network enabled Multi-Function Devices and their fundamental security strengths and weaknesses. Example - Combination printer/scanner/copier/fax devices offer rich variety of functionality to users but are often not configured appropriately for use in secure environments.	MC
J8	Trusted Computing	Awareness of Trusted Platform Module concepts and common hardware and software components and their implementations. Specifically how the TPM can be used to increase platform integrity and to provide more secure disk encryption and password protection solutions.	MC
J9	Resilience	Awareness of the need for and requirements of typical resilience solutions. Including resilience concepts such as hot standby, dual routing and implementations such as RAID, clustering (including databases), fault tolerant clouds, HSRP and VRRP.	MC
J10	Databases	Awareness of common databases and their fundamental security strengths, weaknesses and architectural features. • Microsoft SQL • Oracle • MySQL	MC
J11	Desktop Virtualisation	Awareness of common thin client technologies and the implications they have for security when connected to a corporate network. • Microsoft Terminal Services • Citrix (CAG etc) • VMWare View (VDI) • VNC	MC

ID	Area	Details	How is it Examined CCIM only
J12	Personal devices	Awareness of the security implications of devices not owned and managed by a corporate (Consumerisation) entity being connected to a corporate network or used to process its data. • Laptops • Mobile Phones • PDAs • Tablets • Home Computers	MC
J13	Platform and Application Logging	Understanding the existence and use of Operating System and Application level logging and auditing functions. This includes the Windows Event sub-system for monitoring, particularly within corporate networks. This will specifically include the importance of data level logging of event such as • File Access audit logs • Database Access audit logs • Web Server Logs • Middleware Application Logs	MC

Appendix K - Identification and Access Management

ID	Skill	Details	How Examined CCIM only
K1	Directories and Identity Management	Awareness of the common directory technologies used in large scale network architectures. • Microsoft Active Directory • LDAP • Microsoft Federated Identity Manager • Novell Netware (Open Enterprise Server) • Lotus Notes Understanding of the principles of identity and how these differ from access and authentication controls.	MC
K2	Role Based Access Controls (RBAC)	An understanding of the design concepts required to implement an effective RBAC solution, notably Subject, Roles and Permissions.	MC
K3	Authentication	Awareness of the common single and multifactor authentication schemes available including passwords, tokens, certificates, single sign on and biometric solutions.	MC
K4	Smart Cards	Awareness of the uses and commercially available implementations of Smart Card authentication systems for use in enterprise class IT systems.	MC
K5	RFID & NFC	Awareness of the uses and commercially available implementations of RFID & NFC authentication systems for use in enterprise class IT systems. An awareness of the wider use of RFID technologies is also required.	MC
K6	Biometrics	Awareness of the uses and commercially available implementations of biometric authentication systems and their limitations in large scale practical solutions.	MC

Appendix L - Applications

ID	Skill	Details	How Examined CCIM only
L1	Thin client	An understanding of the concepts behind thin client applications and the implications they have for system design and the placement of security barriers such as firewalls.	MC
L2	Thick client	An understanding of the concepts behind thick client applications and the implications they have for system design and the placement of security barriers such as firewalls.	MC
L3	Web client	An understanding of the concepts behind web client applications and the implications they have for system design and the placement of security barriers such as firewalls.	MC
L4	Email/Messaging	An understanding of the concepts behind messaging systems such as email and the implications they have for system design and the placement of security barriers such as firewalls and content filters.	MC
L5	VOIP	An understanding of the concepts behind VOIP applications and the implications they have for system design and the placement of security barriers such as firewalls.	MC
L6	Mobile applications	An understanding of the concepts behind mobile applications and the implications they have for system design and the placement of security barriers such as firewalls due to their tendency to significantly increase the size of the security perimeter.	MC

ID	Skill	Details	How Examined CCIM only
L7	SCADA	An understanding of the concepts behind SCADA systems and the types of networks and technology often used to support them. An awareness of the key differences in approach to security compared to “standard” computer systems is also required.	MC

Appendix M - Security Methodologies

ID	Skill	Details	How Examined CCIM on ly
M1	Malware Protection	Awareness of the tools and products available to provide protection against attacks from malware and viruses.	MC
M2	Content Filtering	Awareness of the tools and products available to identify inappropriate and potentially malicious content in data transmissions such as email and web access.	MC
M3	DLP	Awareness of the tools and products available to enable Data Loss Prevention.	MC
M4	File Integrity Monitoring	Awareness of the tools and products available to identify unauthorised changes to files and file systems that may be the result of malware or hacker attacks.	MC
M5	SIEM	Awareness of the tools and products available that provide Security Information and Event Management capabilities for large corporate networks and systems.	MC
M6	Network Firewalls	Awareness of the common network firewall products that are available on the open market and an understanding of the capabilities they offer. Specifically, an understanding of the role of network firewalls and the threats they can and cannot protect against.	MC
M7	XML Firewalls	Awareness of the common XML firewall products that are available on the open market and an understanding of the capabilities they offer. Specifically, an understanding of the role of XML firewalls and the threats they can and cannot protect against.	MC

ID	Skill	Details	How Examined CCIM on ly
M8	Application Firewalls	Awareness of the common application firewall products that are available on the open market and an understanding of the capabilities they offer. Specifically, an understanding of the role of application firewalls and the threats they can and cannot protect against.	MC
M9	IDS/IPS	Awareness of the common IDS/IPS products that are available on the open market and an understanding of the capabilities they offer.	MC
M10	VPN Products	Awareness of the common VPN products that are available on the open market and an understanding of the capabilities they offer. Specifically the appropriateness of various products for use on government networks and their ability to be operate in line with relevant government standards.	MC
M11	Data Encryption	Awareness of the commonly available products used for encrypting data in transit and data at rest. Specifically the capabilities of the products in terms of the algorithms they offer and the types of authentication schemes they support.	MC
M12	Diodes	Awareness of the commonly available products used for ensuring information can flow only in one direction between computer systems.	MC
M13	DRM	Awareness of the commonly available products used for securing and controlling the distribution of proprietary information.	MC
M14	HSM	Awareness of the commonly available Hardware Security Module (HSM) products.	MC

Appendix N - Security Vulnerabilities & Prevention Techniques

ID	Skill	Details	How Examined CCIM only
N1	Content Injection	Awareness of the common types of cross site scripting attacks and how they can affect web applications. The differences in risk profile between internal and Internet facing applications should be understood.	MC
N2	SQL Injection	Awareness of the common types of SQL injection attacks and how they can affect both web applications and traditional applications. The differences in risk profile between internal and Internet facing applications should be understood.	MC
N3	Command Injection	Awareness of the common types of command injection attacks and how they can affect both web applications and traditional applications. The differences in risk profile between internal and Internet facing applications should be understood.	MC
N4	Buffer Overflows	Awareness of the common types of buffer overflow attacks and how they can affect applications.	MC
N5	Script Attacks	Awareness of the common types of script language attacks and how they can affect applications. The default Windows client side scripting languages should be understood.	MC
N6	File System attacks	Awareness of the common types of file system mistakes and consequent attacks and how they can affect the security of systems.	MC
N7	User Escalation	Awareness of the common types of desktop weakness and consequent attacks and how they can affect the security of systems.	MC

ID	Skill	Details	How Examined CCIM only
N8	User Account Control	Awareness of key Microsoft technologies for securing modern operating systems and applications, including • User Account Control • Address Space Layout Randomisation • Data Execution Prevention	MC