Technical Committee and Assessors Panel

CREST CCIAS Syllabus

Issued by	CREST Technical Committee and Assessors Panel
Document Reference	CCIAS-Syl
Version Number	1.0
Status	Release
Issue Date	1/4/2012
Review Date	1/4/2013

Table of Contents

Version History

Version	Date	Authors	Status
0.1	30/11/2011	Technical Committee and Assessors Panel	Internal Draft
0.2	1/12/2011	Technical Committee and Assessors Panel	Internal Draft
0.3	2/12/2011	Technical Committee and Assessors Panel	Updated
0.4	5/12/2011	Technical Committee and Assessors Panel	Includes distribution of questions
0.5	15/12/2011	Technical Committee and Assessors Panel	Updated with new sections
0.6	2/1/2012	Technical Committee and Assessors Panel	Updated with new sections
1.0	11/4/2012	Technical Committee and Assessors Panel	Release

Document Review

Reviewer	Position
Chair	Technical Committee / 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.

CESG Certified IA Specialist (CCIAS)

The (CCIAS) Examination tests candidates' knowledge and expertise in a common set of core skills and knowledge for systems architects; success will confer CREST Registered status to the individual.

2 Certification Examination Structure

CESG Certified IA Specialist (CCIAS)

.

3 Syllabus Structure

The syllabus is divided into ten knowledge groups (Appendices A to I 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: including in which component (Written Multiple Choice or Written Long Form).

Within the tables, the following acronyms apply:

CCIAS	CESG Certified IA Specialist
MC	Written Multiple Choice
LF	Written Long Form

Appendix A: Computer Networking Fundamentals (Core Skill)

ID	Area	Details	How is it Examined CCIAS
A1	Wireless Networking	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
A2	Virtual Private Networks	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
A3	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
A4	IPv6	Understanding the existence and benefits of IPv6 together with potential pitfalls to early adopters and issues around interoperability with existing legacy systems.	MC

ID	Area	Details	How is it Examined CCIAS
A5	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
A6	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
A7	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

ID	Area	Details	How is it Examined CCIAS
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
A9	TCP/UDP	TCP/UDP network fundamentals including the implications of • Connection orientated links • Connectionless links • Resilience / Packet Loss • Applications of TCP versus UDP	MC
A10	Routing Protocols	Routing fundamentals including an understanding of • CIDR • RIP • OSPF • EIGRP • Static Routing • Failover • HSRP • BGP	MC
A11	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

ID	Area	Details	How is it Examined
			CCIAS
A12	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
A13	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
A14	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 B: Virtualisation Technologies

ID	Area	Details	How is it Examined CCIAS
B1	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
B2	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
B3	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
B4	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
B5	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
B6	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 C: Platform Security

ID	Area	Details	How is it Examined CCIAS
C1	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
C2	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
C3	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
C4	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

ID	Area	Details	How is it Examined CCIAS
C5	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
C6	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
C7	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
C8	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
C9	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

ID	Area	Details	How is it Examined CCIAS
C10	Databases	Awareness of common databases and their fundamental security strengths, weaknesses and architectural features. • Microsoft SQL • Oracle • MySQL	MC
C11	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
C12	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
C13	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 D: Identification and Access Management

ID	Skill	Details	How Examined
			CCIAS
D1	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
D2	Role Based Access Controls (RBAC)	An understanding of the design concepts required to implement an effective RBAC solution, notably Subject, Roles and Permissions.	MC
D3	Authentication	Awareness of the common single and multifactor authentication schemes available including passwords, tokens, certificates, single sign on and biometric solutions.	MC
D4	Smart Cards	Awareness of the uses and commercially available implementations of Smart Card authentication systems for use in enterprise class IT systems.	MC
D5	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
D6	Biometrics	Awareness of the uses and commercially available implementations of biometric authentication systems and their limitations in large scale practical solutions.	MC

Appendix E: Cryptography

ID	Skill	Details	How Examined
			CCIAS
E1	Public Key Infrastructure (PKI)	An understanding of the concepts behind PKI solutions including certification generation, handling, recovery, non-repudiation, revocation and hierarchical chains of trust.	MC
E2	Storage Encryption	An understanding of the concepts behind storage encryption including the advantages and weakness of common solutions. Knowledge of common products that can be used to meet this requirement is also required.	MC
E3	Network Encryption	An understanding of the concepts behind network encryption including the advantages and weakness of common solutions. Knowledge of common products that can be used to meet this requirement is also required.	MC
E4	Encryption Algorithms	Awareness of common, publically available encryption algorithms as used by mainstream COTS and GOTS solutions.	MC
E5	Hashing Algorithms	Awareness of common, publically available hashing algorithms as used by mainstream COTS and GOTS solutions.	MC

Appendix F: Applications

ID	Skill	Details	How Examined
			CCIAS
F1	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
F2	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
F3	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
F4	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
F5	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
F6	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
F7	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 G: Governance

ID	Skill	Details	How Examined
			CCIAS
G1	Systems Management	An understanding of the concepts behind systems management solutions and the practical tasks that need to be performed in order to keep a system running.	MC
G2	Architectural Patterns	Awareness of the architectural patterns available from known and trusted sources that can reduce the size of a design project significantly.	MC
G3	Software Development Life Cycle (SDLC)	An understanding of the concepts behind the Software Development Life Cycle and how they can be used to drive up both the quality and security of software products. Implications of Waterfall, Rapid, and Agile methodologies to the way in which security should be included in the SDLC.	MC
G4	Accreditation	Awareness of key role that accreditation plays in ensuring the security of government and military networks.	MC
G5	Penetration Testing	Awareness of the concepts employed by penetration test teams so that wherever possible the majority of likely attacks can be designed out of a architecture solution.	MC
G6	TOGAF	Awareness of The Open Group Architecture Framework (TOGAF) methodologies and how they can be used to assist in correctly defining and designing enterprise architectures. Awareness of other methodologies such as MODAF and SABSA™.	MC
G7	Data types and classification	Awareness of the data classification schemes relevant to the environment being designed. This will include Government Protective Marking scheme, PCI data definitions, Data Protection Act definitions as well as other systems used locally within areas such as health and education.	MC
G8	Information flows	An understanding of the concepts behind mapping information flows through an organisations internal business process to identify high risk areas.	MC
G9	Data sanitisation	An understanding of the concepts behind data sanitisation and the various standards and techniques that are available for use.	MC

ID	Skill	Details	How Examined
			CCIAS
G10	Backups	An understanding of the concepts behind backup strategies and the various standards, techniques, products and toolsets that are available for use.	MC
G11	Attack Techniques	Awareness of the likely attack techniques that could be employed by those posing a credible threat to the system. This would be based on an understanding of risk assessment techniques and the use of available intelligence.	MC
G12	Assured Products	Awareness of the relevant schemes available for selecting assured products. This would include Common Criteria evaluations, CAPS evaluations and where required specific local evaluations under relevant schemes.	MC
G13	Third parties & Outsourcing	Understanding of the security requirements and issues around using third parties and outsourcers or cloud service providers to deliver IT services.	MC
G14	Codes of Connection	Knowledge of and understanding of the role and contents of government codes of connection such as GCSx.	MC
G15	Capacity Planning	Understanding of the issues and common approaches to managing capacity in systems and networks.	MC
G16	Security Functional Testing	Awareness of the benefits and pitfalls of security functional testing in ensuring that all security related components are providing the benefits intended by the system designer.	MC

Appendix H: Security Methodologies

ID	Skill	Details	How Examined
			CCIAS
H1	Malware Protection	Awareness of the tools and products available to provide protection against attacks from malware and viruses.	MC
H2	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
H3	DLP	Awareness of the tools and products available to enable Data Loss Prevention.	MC
H4	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
H5	SIEM	Awareness of the tools and products available that provide Security Information and Event Management capabilities for large corporate networks and systems.	MC
H6	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
H7	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
H8	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
H9	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

ID	Skill	Details	How Examined
			CCIAS
H10	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
H11	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
H12	Diodes	Awareness of the commonly available products used for ensuring information can flow only in one direction between computer systems.	MC
H13	DRM	Awareness of the commonly available products used for securing and controlling the distribution of proprietary information.	MC
H14	HSM	Awareness of the commonly available Hardware Security Module (HSM) products.	MC

Appendix I: Security Vulnerabilities & Prevention Techniques

ID	Skill	Details	How Examined
			CCIAS
I1	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
I2	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
I3	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
I4	Buffer Overflows	Awareness of the common types of buffer overflow attacks and how they can affect applications.	MC
I5	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
I6	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
I7	User Escalation	Awareness of the common types of desktop weakness and consequent attacks and how they can affect the security of systems.	MC
I8	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