

**Unit 521 ICT Systems Security+  
(Optional)**

There are 5 domains measured by the Security+.

1. General security concepts
2. Communication security
3. Infrastructure security
4. Basics of cryptography
5. Operational/Organizational security.

**Guided learning hours**

The recommended guided learning hours for this unit are 90 hours

**Connections with other awards**

**VRQ links**

e-Equals Advanced Diploma for IT Practitioners (ICT Systems Support)  
Unit 511 – ICT Security

**Assessment**

Assessment will be by means of CompTIA's Security+ examination. The table below lists the domains measured by this examination and the extent to which they are represented in the examination.

<b>CompTIA Security+ Certification Domains</b>	<b>Exam Weighting</b>
1.0 General security concepts	30
2.0 Communication security	20
3.0 Infrastructure security	20
4.0 Basics of cryptography	15
5.0 Operational/Organizational security	15

<b>Domain 1.0: General security concepts</b>	<b>Candidate's signature</b>	<b>Date</b>
<p><b>Content limits</b></p> <p>1.1 Recognise and be able to differentiate and explain the following access control models.</p> <ul style="list-style-type: none"> <li>▪ MAC (Mandatory Access Control)</li> <li>▪ DAC (Discretionary Access Control)</li> <li>▪ RBAC (Role Based Access Control)</li> </ul> <p>1.2 Recognise and be able to differentiate and explain the following access control models.</p> <ul style="list-style-type: none"> <li>▪ Kerberos</li> <li>▪ CHAP (Challenge Handshake Authentication Protocol)</li> <li>▪ Certificates</li> <li>▪ Username/password</li> <li>▪ Tokens</li> <li>▪ Multi-factor</li> <li>▪ Mutual</li> <li>▪ Biometrics</li> </ul> <p>1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols.</p> <p>1.4 Recognise the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk</p> <ul style="list-style-type: none"> <li>▪ DOS/DDOS (Denial of Service/Distributed Denial of Service)</li> <li>▪ Back door</li> <li>▪ Spoofing</li> <li>▪ Man in the middle</li> <li>▪ Replay</li> <li>▪ TCP/IP hijacking</li> <li>▪ Weak keys</li> <li>▪ Mathematical</li> <li>▪ Social engineering</li> <li>▪ Birthday</li> <li>▪ Password guessing <ul style="list-style-type: none"> <li>▪ Brute force</li> <li>▪ Dictionary</li> </ul> </li> <li>▪ Software exploitation</li> </ul>		
	<b>Candidate's signature</b>	<b>Date</b>

<b>Domain 1.0: General security concepts</b>	<b>Candidate's signature</b>	<b>Date</b>
<p><b>Content limits (continued)</b></p> <p>1.5 Recognise the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk</p> <ul style="list-style-type: none"><li>▪ Viruses</li><li>▪ Trojan horses</li><li>▪ Logic bombs</li><li>▪ Worms</li></ul> <p>1.6 Understand the concept of and know how to reduce the risks of social engineering</p> <p>1.7 Understand the concept and significance of auditing, logging and system scanning.</p>		

Domain 2.0: Common security	Candidate's signature	Date
<p><b>Content limits</b></p> <p>2.1 Recognise and understand the administration of the following types of remote access technologies</p> <ul style="list-style-type: none"> <li>▪ 802.1x</li> <li>▪ VPN (Virtual Private Network)</li> <li>▪ RADIUS (Remote Authentication Dial-In User Service)</li> <li>▪ TACACS (Terminal Access Controller Access Control System)</li> <li>▪ L2TP/PPTP (Later Two Tunneling Protocol/Point to Point Tunneling Protocol)</li> <li>▪ SSH (Secure Shell)</li> <li>▪ IPSEC (Internet Protocol Security)</li> <li>▪ Vulnerabilities</li> </ul> <p>2.2 Recognise and understand the administration of the following email security concepts</p> <ul style="list-style-type: none"> <li>▪ S/MIME (Secure Multipurpose Internet Mail Extensions)</li> <li>▪ PGP (Pretty Good Privacy) like technologies</li> <li>▪ Vulnerabilities               <ul style="list-style-type: none"> <li>▪ SPAM</li> <li>▪ Hoaxes</li> </ul> </li> </ul> <p>2.3 Recognise and understand the administration of the following internet security concepts</p> <ul style="list-style-type: none"> <li>▪ SSL/TLS (Secure Sockets Layer/Transport Layer Security)</li> <li>▪ HTTP/S (Hypertext Transfer Protocol/Hypertext Transfer Protocol over Secure Sockets Layer)</li> <li>▪ Instant messaging               <ul style="list-style-type: none"> <li>▪ Vulnerabilities</li> <li>▪ Packet sniffing</li> <li>▪ Privacy</li> </ul> </li> <li>▪ Vulnerabilities               <ul style="list-style-type: none"> <li>▪ Java script</li> <li>▪ ActiveX</li> <li>▪ Buffer overflows</li> <li>▪ Cookies</li> <li>▪ Signed applets</li> <li>▪ CGI (Common Gateway Interface)</li> <li>▪ SMTP (Simple Mail Transfer Protocol) relay</li> </ul> </li> </ul> <p>2.4 Recognise and understand the administration of the following directory security concepts</p> <ul style="list-style-type: none"> <li>▪ SSL/TLS (Secure Sockets Layer/Transport Layer Security)</li> <li>▪ LDAP (Lightweight Directory Access Protocol)</li> </ul>		

<b>Domain 2.0: Common security</b>	<b>Candidate's signature</b>	<b>Date</b>
<p><b>Content limits (continued)</b></p> <p>2.5 Recognise and understand the administration of the following file transfer protocols and concepts</p> <ul style="list-style-type: none"><li>▪ S/FTP (File Transfer Protocol)</li><li>▪ Blind FTP (File Transfer Protocol)/Anonymous</li><li>▪ File sharing</li><li>▪ Vulnerabilities<ul style="list-style-type: none"><li>▪ Packet sniffing</li><li>▪ 8.3 naming conventions</li></ul></li></ul> <p>2.6 Recognise and understand the administration of the following wireless technologies and concepts</p> <ul style="list-style-type: none"><li>▪ WTLS (Wireless Transport Layer Security)</li><li>▪ 802.11 and 802.11x</li><li>▪ WEP/WAP (Wired Equivalent Privacy/Wireless Application Protocol)</li><li>▪ Vulnerabilities</li><li>▪ Site surveys</li></ul>		

<b>Domain 3.0: Infrastructure security</b>	<b>Candidate's signature</b>	<b>Date</b>
<p><b>Content limits</b></p> <p>3.1 Understand security concerns and concepts of the following types of devices</p> <ul style="list-style-type: none"><li>▪ Firewalls</li><li>▪ Routers</li><li>▪ Switches</li><li>▪ Wireless</li><li>▪ Modems</li><li>▪ RAS (Remote Access Server)</li><li>▪ Telecom/PBX (Private Branch Exchange)</li><li>▪ VPN (Virtual Private Network)</li><li>▪ IDS (Intrusion Detection System)</li><li>▪ Network monitoring/diagnostics</li><li>▪ Workstations</li><li>▪ Servers</li><li>▪ Mobile devices</li></ul> <p>3.2 Understand the security concerns for the following types of media</p> <ul style="list-style-type: none"><li>▪ Coaxial cable</li><li>▪ UTP/STP (Unshielded Twisted Pair/Shielded Twisted Pair)</li><li>▪ Fiber optic cable</li><li>▪ Removable media<ul style="list-style-type: none"><li>▪ Tape</li><li>▪ CD-R (Recordable Compact Disks)</li><li>▪ Hard drives</li><li>▪ Diskettes</li><li>▪ Flashcards</li><li>▪ Smartcards</li></ul></li></ul> <p>3.3 Understand the concepts behind the following kinds of Security Topologies</p> <ul style="list-style-type: none"><li>▪ Security zones<ul style="list-style-type: none"><li>▪ DMZ (Demilitarised Zone)</li><li>▪ Intranet</li><li>▪ Extranet</li></ul></li><li>▪ VLANs (Virtual Local Area Network)</li><li>▪ NAT (Network Address Translation)</li><li>▪ Tunneling</li></ul>		

Domain 3.0: Infrastructure security	Candidate's signature	Date
<p><b>Content limits (continued)</b></p> <p>3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system</p> <ul style="list-style-type: none"> <li>▪ Network based           <ul style="list-style-type: none"> <li>▪ Active detection</li> <li>▪ Passive detection</li> </ul> </li> <li>▪ Host based           <ul style="list-style-type: none"> <li>▪ Active detection</li> <li>▪ Passive detection</li> </ul> </li> <li>▪ Honey pots</li> <li>▪ Incident response</li> </ul> <p>3.5 Understand the following concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system</p> <ul style="list-style-type: none"> <li>▪ OS/NOS (Operating System/Network Operating Systems) hardening           <ul style="list-style-type: none"> <li>▪ File system</li> <li>▪ Updates (hotfixes, services packs, patches)</li> </ul> </li> <li>▪ Network hardening           <ul style="list-style-type: none"> <li>▪ Updates (firmware)</li> <li>▪ Configuration               <ul style="list-style-type: none"> <li>▪ Enabling and disabling services and protocols</li> <li>▪ Access control lists</li> </ul> </li> </ul> </li> <li>▪ Application hardening           <ul style="list-style-type: none"> <li>▪ Updates (hotfixes, service packs, patches)</li> <li>▪ Web servers</li> <li>▪ E-mail servers</li> <li>▪ FTP (File Transfer Transfer Protocol) servers</li> <li>▪ DNS (Domain Name Service) servers</li> <li>▪ NNTP (Network News Transfer Protocol) servers</li> <li>▪ File/print servers</li> <li>▪ DHCP (Dynamic Host Configuration Protocol) servers</li> <li>▪ Data repositories               <ul style="list-style-type: none"> <li>▪ Directory services</li> <li>▪ Databases</li> </ul> </li> </ul> </li> </ul>		

Domain 4.0: Basics of cryptography	Candidate's signature	Date
<p><b>Content limits</b></p> <p>4.1 Be able to identify and explain the following different kinds of cryptographic algorithms</p> <ul style="list-style-type: none"> <li>▪ Hashing</li> <li>▪ Symmetric</li> <li>▪ Asymmetric</li> </ul> <p>4.2 Understand how cryptography addresses the following security concepts</p> <ul style="list-style-type: none"> <li>▪ Confidentiality</li> <li>▪ Integrity <ul style="list-style-type: none"> <li>▪ Digital signatures</li> </ul> </li> <li>▪ Authentication</li> <li>▪ Non-repudiation <ul style="list-style-type: none"> <li>▪ Digital signatures</li> </ul> </li> <li>▪ Access control</li> </ul> <p>4.3 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure)</p> <ul style="list-style-type: none"> <li>▪ Certificates <ul style="list-style-type: none"> <li>▪ Certificate policies</li> <li>▪ Certificate practice statements</li> </ul> </li> <li>▪ Revocation</li> <li>▪ Trust models</li> </ul> <p>4.4 Identify and be able to differentiate different cryptographic standards and protocols</p> <p>4.5 Understand and be able to explain the following concepts of Key Management and Certificate Lifecycles</p> <ul style="list-style-type: none"> <li>▪ Centralised vs Decentralised</li> <li>▪ Storage <ul style="list-style-type: none"> <li>▪ Hardware vs Software</li> <li>▪ Private Key Protection</li> </ul> </li> <li>▪ Escrow</li> <li>▪ Expiration</li> <li>▪ Revocation <ul style="list-style-type: none"> <li>▪ Status checking</li> </ul> </li> <li>▪ Suspension <ul style="list-style-type: none"> <li>▪ Status checking</li> </ul> </li> <li>▪ Recovery <ul style="list-style-type: none"> <li>▪ M-of-N Control (Of M appropriate individuals, N must be present to authorise recovery)</li> </ul> </li> <li>▪ Renewal</li> <li>▪ Destruction</li> <li>▪ Key usage <ul style="list-style-type: none"> <li>▪ Multiple key pairs (single, dual)</li> </ul> </li> </ul>		

Domain 5.0: Operational/organizational security	Candidate's signature	Date
<p><b>Content limits</b></p> <p>5.1 Understand the application of the following concepts of physical security</p> <ul style="list-style-type: none"><li>▪ Access control<ul style="list-style-type: none"><li>▪ Physical barriers</li><li>▪ Biometrics</li></ul></li><li>▪ Social engineering</li><li>▪ Environment<ul style="list-style-type: none"><li>▪ Wireless cells</li><li>▪ Location</li><li>▪ Shielding</li><li>▪ Fire suppression</li></ul></li></ul> <p>5.2 Understand the security implications of the following topics of disaster recovery</p> <ul style="list-style-type: none"><li>▪ Backups<ul style="list-style-type: none"><li>▪ Off site storage</li></ul></li><li>▪ Secure recovery<ul style="list-style-type: none"><li>▪ Alternate sites</li></ul></li><li>▪ Disaster recovery plan</li></ul> <p>5.3 Understand the security implications of the following topics of business continuity</p> <ul style="list-style-type: none"><li>▪ Utilities</li><li>▪ High availability/fault tolerance</li><li>▪ backups</li></ul> <p>5.4 Understand the concepts and uses of the following types of policies and procedures</p> <ul style="list-style-type: none"><li>▪ Security policy<ul style="list-style-type: none"><li>▪ Acceptable use</li><li>▪ Due care</li><li>▪ Privacy</li><li>▪ Separation of duties</li><li>▪ Need to know</li><li>▪ Password management</li><li>▪ SLAs (Service Level Agreements)</li><li>▪ Disposal/destruction</li><li>▪ HR (Human Resources) policy<ul style="list-style-type: none"><li>▪ Termination (adding and revoking passwords and privileges, etc)</li><li>▪ Hiring (adding and revoking passwords and privileges, etc)</li><li>▪ Code of ethics</li></ul></li></ul></li><li>▪ Incident response policy</li></ul>		

<b>Domain 5.0: Operational/organizational security</b>	<b>Candidate's signature</b>	<b>Date</b>
<p><b>Content limits (continued)</b></p> <p>5.5 Explain the following concepts of privilege management</p> <ul style="list-style-type: none"><li>▪ User/Group/Role management</li><li>▪ Single sign-on</li><li>▪ Centralised vs Decentralised</li><li>▪ Auditing (privilege, usage, escalation)</li><li>▪ MAC/DAC/RBAC (Mandatory Access Control/ Discretionary Access Control/ Role Based Access Control)</li></ul> <p>5.6 Understand the concepts of the following topics of forensics</p> <ul style="list-style-type: none"><li>▪ Chain of custody</li><li>▪ Preservation of evidence</li><li>▪ Collection of evidence</li></ul> <p>5.7 Understand and be able to explain the following concepts of risk identification</p> <ul style="list-style-type: none"><li>▪ Asset identification</li><li>▪ Risk assessment</li><li>▪ Threat identification</li><li>▪ Vulnerabilities</li></ul> <p>5.8 Understand the security relevance of the education and training of end users, executives and human resources</p> <ul style="list-style-type: none"><li>▪ Communication</li><li>▪ User awareness</li><li>▪ Education</li><li>▪ On-line resources</li></ul> <p>5.9 Understand and explain the following documentation concepts</p> <ul style="list-style-type: none"><li>▪ Standards and guidelines</li><li>▪ Systems architecture</li><li>▪ Change documentation</li><li>▪ Logs and inventories</li><li>▪ Classification<ul style="list-style-type: none"><li>▪ Notification</li></ul></li><li>▪ Retention/storage</li><li>▪ Destruction</li></ul>		