Goodheart-Willcox Publisher
18604 West Creek Drive • Tinley Park, IL 60477 • 800.323.0440 • www.g-w.com

Goodheart-Willcox Publisher

Correlation of **Principles of Cybersecurity** *1E* ©2020

to the CompTIA Security+ Certification Exam Objectives

for Exam Number: SY0-501

STANDARD	G-W CORRELATING PAGES
1.0 Threats, Attacks and Vulnerabilities	
1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.	pg 41–45 pg 46 head Keyloggers
1.2 Compare and contrast types of attacks.	pg 50 head Social Engineering pg 56 head Dumpster Diving pg 73 head Passwords pg 162–166 pg 272, paragraph 1 pg 291, paragraph 2 pg 292, paragraph 1 pg 303, paragraph 4 pg 329, paragraph 4 pg 343, paragraph 2 pg 362 head Types of Attacks pg 379–380 head Password-Cracking Methods pg 410, paragraph 1 pg 441, paragraph 2
1.3 Explain threat actor types and attributes.	pg 10–15
1.4 Explain penetration testing concepts.	pg 423 head White, Black, or Gray Box pg 424 head Passive Information Gathering
1.5 Explain vulnerability scanning concepts.	pg 205, paragraph 5–6
1.6 Explain the impact associated with types of vulnerabilities.	pg 46 head Zero-Day Vulnerability pg 170, paragraph 4 pg 222 Quick Look 7.1.1 pg 392, paragraph 2
2.0 Technologies and Tools	
2.1 Install and configure network components, both hardware and software based, to support organizational security.	pg 205 head Vulnerability Scanning Concepts pg 296 head VPN Protocol pg 303–308 pg 309–310 pg 322, paragraph 1 pg 337–339 pg 343–344

	pg 398–399 head Scripts
2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.	pg 140, paragraph 5 pg 192 head Analyzing Log Events pg 203–205 pg 265 head Packet Sniffer pg 273 Quick Look 8.2.1 pg 277–278 pg 310 pg 331–333
2.3 Given a scenario, troubleshoot common security issues.	pg 101 head Combining NFTS and Share Permissions pg 170, paragraph 2 pg 335 head Unencrypted
2.4 Given a scenario, analyze and interpret output from security technologies.	pg 308-309 pg 397, paragraph 1
2.5 Given a scenario, deploy mobile devices securely.	pg 46 head Firmware pg 223, paragraph 2 pg 224 head Protecting Data on a Mobile Platform pg 227, paragraph 4 pg 229 head GPS Metadata as a Security Concern pg 324-325
2.6 Given a scenario, implement secure protocols.	pg 81, paragraph 3–4 pg 281 head File Transfer Protocol pg 292, paragraph 5 pg 370 head Accessing Secure Data Through Browsers
3.0 Architecture and Design	
3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.	pg 37, paragraph 1 pg 149, paragraph 1 pg 433 head Additional Report Terminology
3.2 Given a scenario, implement secure network architecture concepts.	pg 19, paragraph 3 pg 20, paragraph 6 pg 274, paragraph 1 pg 293–296 heads VLAN, DMZ, Intranets and Extranets, VPN
3.3 Given a scenario, implement secure systems design.	pg 178–183 pg 201–202 pg 235, paragraph 3 pg 237–239 pg 331
3.4 Explain the importance of secure staging deployment concepts.	pg 20, paragraph 2 pg 390 head SDLC Stages

3.5 Explain the security implications of embedded systems.	pg 221, paragraph 5 pg 237–239
3.6 Summarize secure application development and deployment concepts.	pg 211 head Change-Management Systems pg 391 head Types of SDLCs pg 398, paragraph 1 pg 403 head SDK
3.7 Summarize cloud and virtualization concepts	pg 19, paragraph 2 pg 454–455 pg 455 head Public or Private pg 464–466 pg 469 head Sharing with Others pg 472–473
3.8 Explain how resiliency and automation strategies reduce risk.	pg 460, paragraph 3 pg 462 head Load Balancing and Scalability
3.9 Explain the importance of physical security controls.	pg 75 head What You Are pg 149–151
4.0 Identity and Access Management	
4.1 Compare and contrast identity and access management concepts	pg 74 head Multifactor Authentication pg 82 head Additional Access Levels
4.2 Given a scenario, install and configure identity and access services.	pg 81, paragraph 2 pg 82 , paragraph 2 pg 83, paragraph 1
4.3 Given a scenario, implement identity and access management controls.	pg 74 head Multifactor Authentication pg 76 head Security Error Rates Concerning Biometric Authentication
4.4 Given a scenario, differentiate common account management practices.	pg 88, paragraph 1 pg 196 head Auditing
5.0 Risk Management	
5.1 Explain the importance of policies, plans and procedures related to organizational security.	pg 167, paragraph 2 pg 170, paragraph 4 pg 434, paragraph 2 pg 506–508
5.2 Summarize business impact analysis concepts.	pg 235, paragraph 3–4 pg 240–241 pg 242, paragraph 2 pg 495 head MTBF pg 496 head MTTR pg 508, paragraph 4 pg 515, paragraph 3
5.3 Explain risk management processes and concepts.	pg 434–436

	pg 488, paragraph 1 pg 489, paragraph 1 pg 491–492
5.4 Given a scenario, follow incident response procedures.	pg 538-543
5.5 Summarize basic concepts of forensics.	pg 549, paragraph 1 pg 550, paragraph 3 pg 557, paragraph 1
5.6 Explain disaster recovery and continuity of operation concepts.	pg 20, paragraph 3 pg 470 head Legal Concerns pg 509, paragraph 4 pg 515 head Maintaining Additional Sites pg 517 head Using RAID
5.7 Compare and contrast various types of controls.	pg 148, paragraph 3
5.8 Given a scenario, carry out data security and privacy practices.	pg 62 head Health Insurance Portability and Accountability Act pg 528 head Media Sanitization
6.0 Cryptography and PKI	
6.1 Compare and contrast basic concepts of cryptography.	pg 356, paragraph 1 pg 359 head Stenography pg 362, paragraph 7 pg 365, paragraph 1
6.2 Explain cryptography algorithms and their basic characteristics.	pg 353, paragraph 4 pg 356–359 heads Symmetric Encryption, Asymmetric Encryption pg 378, paragraph 1 pg 378, paragraph 7
6.3 Given a scenario, install and configure wireless security settings.	pg 336 head Strongest Encryption
6.4 Given a scenario, implement public key infrastructure.	pg 357–359 head Asymmetric Encryption