Comparison of Exam Objectives – New exam SY0-301 vs. SY0-201

Why the exam is changing

Security+ is an ISO/ANSI accredited certification. CompTIA launched the last version of Security+ in 2008, and is on a 3-year schedule for exam review and update.

General changes to the objectives

Security+ SY0-301 distinguishes three types of security: application, data and host security. Objective domain 4.0, Application, Data and Host Security calls attention to this way of thinking about information security. There is new emphasis on operational risk—thinking about it and planning for it—that was not in SY0-201. This is primarily in domain 2.0, Compliance & Operational Security.

Below is a high level mapping of the upcoming SY0-301 exam objectives to objectives in the SY0-201 exam. This document is not exhaustive, but is intended to provide a starting point for analysis and curriculum development by courseware providers and trainers.

SY0-301 Exam Objectives	**SY0-201 - Objective references**
1.0 Network Security	
1.1 Explain the security function and purpose of network devices and technologies	2.3, 2.4
1.2 Apply and implement secure network administration principles	2.2, 2.3, 2.4
1.3 Distinguish and differentiate network design elements and compounds	2.2 (no cloud reference)
1.4 Implement and use common protocols	5.4
1.5 Identify commonly used default network ports (e.g. SFTP, TELNET)	Terms not found
1.6 Implement wireless network in a secure manner	Terms not found
2.0 Compliance and Operational Security	
2.1 Explain risk related concepts	
• Control types	Terms not found
• False positives	Terms not found
• Importance of policies in reducing risk	6.4
• Risk calculation	Terms not found
• Risks associated to Cloud Computing….	Terms not found
2.2 Carry out appropriate risk mitigation strategies	4.1 (but not as detailed as new exam)
2.3 Execute appropriate incident response procedures	6.3 (New exam has much more detail on forensics)
2.4 Explain the importance of security related awareness and training	6.6, minimally. Essentially 2.4 in the new exam is a new objective.

2.5 Compare and contrast aspects of business continuity	6.1, 6.2
2.6 Explain the impact and proper use of environmental controls	6.5
2.7 Execute disaster recovery plans and procedures	6.1, 6.2
2.8 Exemplify the concepts of confidentiality, integrity and availability (CIA)	5.1
3.0 Threats and Vulnerabilities	
3.1 Analyze and differentiate among types of malware	1.1
3.2 Analyze and differentiate among types of attacks	2.1
3.3 Analyze and differentiate among types of social engineering attacks	6.6
3.4 Analyze and differentiate among types of wireless attacks	2.7
3.5 Analyze and differentiate among types of application attacks	1.4
3.6 Analyze and differentiate among types of mitigation and deterrent techniques	3.9, 3.2, 3.7
3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities	4.1, 4.2 (but new exam is more detailed)
3.8 Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning	4.3
4.0 Application, Data and Host Security	
4.1 Explain the importance of application security	Terms not found
4.2 Carry out appropriate procedures to establish host security	1.3
4.3 Explain the importance of data security	Terms not found
5.0 Access Control and Identity Management	
5.1 Explain the function and purpose of authentication services	3.7
5.2 Explain the fundamental concepts and best practices related to authorization and access control	3.1, 3.9 (though more detail in new exam)
5.3 Implement appropriate security controls when performing account management	3.5
6.0 Cryptography	
6.1 Summarize general cryptography concepts	5.1
6.2 Use and apply appropriate cryptographic tools and products	5.3 (more detail in new exam)
6.3 Explain the core concepts of public key infrastructure	5.5
6.4 Implement PKI, certificate management and associated components	5.6