

**Expert Reference Series of IT Security White Papers**

---

# **The Security+ Certification**

---

[www.thesolutionfirm.com](http://www.thesolutionfirm.com)

## Security + Certification

Michael Gregg

Security+ certification requires you to pass a single exam, costing \$199. Although there's only one test, it covers a very wide range of security knowledge. If you are working toward the TICSA or CISSP exam, this would be a good first step. Preparing for Security + can help you fill in those knowledge gaps and be better prepared for subsequent exams. To help you along the road to security certification, we've prepared a blueprint of what you can expect to find on the exam.

### Test Objectives

The Security+ exam contains five domains:

- general security concepts
- communications security
- infrastructure security
- basics of cryptography
- operational/organizational security

Each of these domains is made up of topics and subtopics that must be mastered to successfully complete the exam. You may have heard that the Security+ exam is not that hard, but be forewarned; it covers a vast range of information. The exam entails all aspects of security and security related topics, so come fully prepared. Let's take a look at each of the five domains.

### General Security Concepts (30%)

This first section covers all the general security concepts. To successfully pass this section of the exam you will need to understand all of the various forms of attacks. If you have never experimented with a password cracker you may want to download John the Ripper or L0phtcrack. Do not run these applications at your workplace without the full consent of management. Also make sure that you download these from a trusted source such as [packet storm](#). Many sites run an MD5 checksum on these types of programs to verify that no one has added anything to them. We are talking Trojans here folks! The best place to experiment with these programs is on your home network or an approved test system.

You will also need to know about multi-factor authentication. If you have a bankcard you are familiar with multifactor authentication. Bankcards require two items to successfully access an account: Something you have, and something you know. Together these two items, the card itself and your PIN, allow you access to the account. General security concept subcategories include:

- Authentication
- Attacks
- Malicious Code
- Social Engineering
- Auditing

### Communications Security (20%)

Communications Security is an area of growing importance and the range of topics covered in this area makes that very clear. Are you keeping up to speed with wireless? If not, you may want to start reviewing 802.11 standards. Maybe you remember something called war dialing from the old days. That was where you would dial a range of phone numbers looking for an open modem. Today that practice has evolved in war driving. Its goal is to find unsecured wireless networks. According to on-line resources, there are plenty of unsecured networks out there. I hope yours is not one of them! All the wireless hacker needs is a laptop, wireless card, and maybe a Pringles can that has been fashioned into a powerful antenna. If you want to learn more about this growing trend checkout [wardriving.com](#).

Copyright 2007 © Superior Solutions, Inc. All rights reserved. All brand names and trademarks are TM and/or copyright by their respective owners. Reprints require expressed permission of the owner.

Other items in this section include the vulnerabilities of protocols such as FTP and Telnet. Both of these protocols transmit usernames and passwords in clear text. That's a big problem. Listed below are the seven subcategories included in the communications security portion of the exam.

- Remote Access
- Email
- Web
- Vulnerabilities
- Directory
- File Transfer
- Wireless

### **Infrastructure Security (20%)**

A good foundational knowledge of networks and network equipment will really help you pass this section of the exam. This includes firewalls, routers, switches, and hubs. Again, CompTIA is not expecting an in-depth knowledge, but a general understanding of the equipment and how it operates. You will want to review NAT, VLANs, RAS, and the items listed below.

- Devices
- Media
- Security Topologies
- Intrusion Detection
- Security Baselines

### **Basics of Cryptography (15%)**

How's your knowledge of symmetric vs. asymmetric algorithms? This is one area of the test you will need to brush up on if you are not actively involved in using these technologies. A good place to start would be to download and install a copy of Pretty Good Privacy at [pgp.com](http://pgp.com). An individual user license is free. Anyway, do you really want others to be able to read your email? The five subcategories of this section are listed here for your review.

- Algorithms
- Concepts of using cryptography
- PKI
- Standards and Protocols
- Key Management/Certificate Lifecycle

### **Operational/Organizational Security (15%)**

Some individuals don't consider this the glamorous portion of security. However, it is critical to the security of the organization. Items such as documentation can make or break effective security. Forensics and documentation go hand-in-hand. Without proper documentation, do you really think your case will hold up in court? Forensics is an area in security that is experiencing rapid growth. One good place to read more about this fascinating subject is the article [How the FBI Investigates Computer Crime](#).

Review the subcategories below to get a good idea of what is needed to master this domain.

- Physical Security
- Disaster Recovery
- Business Continuity
- Policy and Procedures
- Privilege Management
- Forensics
- Risk Identification

- Education
- Documentation

### **A Solid Starting Point**

Overall, the Security+ exam is a well-balanced entry-level certification. Look for the Security+ exam to become a benchmark in many of the same ways that A+ and Network+ have. If you have achieved an A+ or Network+ certification and are looking to add a security certification, this is a good choice. After all, CompTIA is one of the most well known exam vendors. They consistently develop and release well respected vendor neutral exams. Choosing this exam as your first security certification is a no-brainer!

### **About the Author**

Michael C. Gregg is the COO of Superior Solutions, Inc., a security assessment and training firm. His current responsibilities include performing security assessments and evaluations for corporate and government entities. He has served as the developer of high-level security classes, study guides, has taught classes for many Fortune 500 companies and contributed to many books, including the Syngress publication, *Hack the Stack*.

