

# Course overview

## g632eng Security+ Bridge Certification (2002 to 2008 Edition)

(g632eng)



### Overview and objectives

This self-study course is intended for CompTIA Security+ professionals seeking to certify with the latest edition of the exam (2008 Edition). CompTIA's Certification Update Policy allows candidates holding certification under the previous exam objectives to update their certification by taking a special Bridge exam (code BR0-001).

This course provides an overview of developments in security technologies and threats and detailed content to cover the topics tested in the Bridge Exam.

The course has been approved through the CompTIA Authorized Quality Curriculum program.

### Certification track

This course will prepare students to take the BR0-001 CompTIA Security+ Certification Bridge Exam, for the objectives released in October 2008.

Candidates taking the exam must already be certified with the 2002 edition of CompTIA Security+.



### Course prerequisites

You must have successfully completed the "CompTIA Security+ Support Skills" course and ideally have around 24 months' experience of network security administration. Specifically, you have the following skills and knowledge before starting this course:

- Differentiate and explain different methods of authentication and access control.
- Recognize and mitigate network and system threats and attacks.
- Securely administer and configure communication security protocols and products.
- Securely administer and configure network infrastructure.
- Understand the basics of cryptographic algorithms and technologies.
- Understand secure operational policies, such as disaster recovery, privilege management, and incident response.

# Course overview

## g632eng Security+ Bridge Certification (2002 to 2008 Edition)

(g632eng)



## Course contents

The course contains indexed study notes and review questions, exam objectives mapping, exam information, and a comprehensive glossary. The course also comes with an online practice exam.

- **Systems Security Domain** • Domain Objectives/Examples • Systems Security Threats • System Hardware and Peripherals • OS Hardening • Application Security • Web Browsers • Desktop Security Applications • Virtualization Technologies
- **Network Infrastructure Domain** • Domain Objectives/Examples • Ports and Protocols • Network Design • Network Security Tools • Infrastructure Vulnerabilities and Mitigations • Wireless Networking
- **Access Control Domain** • Domain Objectives/Examples • Best Practice Access Control Models • Security Groups and Roles • File and Print Services • Authentication Models • Physical Access Controls
- **Assessments and Audits Domain** • Domain Objectives/Examples • Vulnerability Assessments • Systems and Performance Monitoring • Intrusion Detection Systems • Audit Logs
- **Cryptography Domain** • Domain Objectives/Examples • Cryptography Concepts and Algorithms • Implementing PKI
- **Organizational Security Domain** • Domain Objectives/Examples • Disaster Recovery Planning • Redundancy Planning • Backup Strategies • Corporate Security Policy • Environmental Controls • Social Engineering