Today's world contains many people determined to break into computer systems for their own gain. Not one day goes by without a news story on the latest attempt. Whether they are agents of foreign governments, criminal elements or malicious individuals, they are all intent on obtaining data for their own gain.

IT environments are central, then, to every element of business and government as they look for ways to prevent and detect these risks. And as such environments evolve, they create more complex interdependencies which drive the need for more professional technical expertise and leadership. This is why Prometric created this exam.

We have also prepared this guide to help you get ready for Prometric's Cyber Security Essentials Exam. In it, you will find the following topics covered:

+ Exam Content Outline
+ How the Exam Was built
+ Study Strategy
+ Exam Taking Tips
+ Reference Material and Resources
Exam Content Outline

You will find that Cyber Security Essentials is comprehensive in the material that it covers. The Exam consists of seven major subject areas that span the following.

**Information Systems Security** – Means by which electronically stored information is kept confidential. Information Systems Security, also known as INFOSEC, often refers to the access controls to prevent unauthorized people from accessing an information system, which is accomplished through a combination of processes.

**Application Security** – Use of software, hardware and procedural methods to protect applications from hacker threats. Because applications are increasingly accessible over networks, they are vulnerable to a wide variety of threats.

**Governance** – Practices exercised by those responsible for an organization or enterprise. The overarching goal of governance is to provide an organization with a strategic direction to ensure that it reaches business objectives and that risks, including ever-increasing cyber security risks, are effectively managed.

**Compliance** – How well an organization adheres to the standards of good practice when it comes to managing cyber risks.

**Operational Security** - Identification and safeguarding of sensitive or critical information. In a well-run organization, management and users enhance operational security against cyber risks by instilling effective procedures and guidelines into the day-to-day operations.

**Network Security** – Procedures and policies adopted by an organization's computer network administrator to prevent unauthorized access or misuse of a computer network and systems attached to that network. It also refers to the systems put in place to ensure authorization of access to data in a network.

**Physical Security** – Procedures and polices that blunt unauthorized access to areas in a facility where computer and networking resources are housed. Some common types of physical security include door alarms, video cameras, locked doors and barrier fences.

**Environmental Security** – Protection of computer and networking resources from environmental damage from threats such as fire, water, smoke, dust, radiation and impact.

**Vulnerability Management** – Consolidated methodology and process for assessing, mitigating and protecting an organization's computer and networking resources, while also reducing the cost of security and compliance. Vulnerability management also includes assessing and planning for myriad threat scenarios, from environmental disaster to cyber attack.
How the Exam Was Built

*Cyber Security Essentials* was developed by Prometric in collaboration with senior IT engineers and technical staff from premier companies, spanning the globe, with more than 20 years of experience. These Subject Matter Experts (SMEs) who helped develop the exam hold excellent credentials including CISSP, CISA and CEH to name a few. They currently perform in a variety of fields, including computer hacking forensic investigation, ethical hacking, network security, digital forensics and cyber security.

Prometric's test design approach is founded in valid methods that follow well-established industry practices. Our services are in accordance with the four key measurement testing standards:

1. **The Standards for Educational and Psychological Testing (Standard 14)**
2. **ANSI/PCAC (GI 502)**
3. **ANSI/ISO/IEC 17024**
4. **NCCA/ICE (Standard 10)**

These standards influence how a job analysis is conducted by outlining specific tasks, including:

- Defining the job characteristics clearly;
- Justifying why aspects of a profession are important;
- Recruiting qualified SMEs to provide input during the study;
- Sampling individuals that represent the full spectrum of practitioners by covering all job titles, major practice areas, work settings, geographic regions, ethnicities, demographics, genders and work experiences;
- Developing a test specification for the construction of the examination; and
- Updating the test specifications periodically with new job analyses (every three to five years, depending on the dynamic nature of the profession).

All of our test design activities incorporate these standards, so you can trust that our methods have resulted in the development of the highest quality security exam. With *Cyber Security Essentials*, you have a vendor-neutral exam that affords you a flexible, affordable option while accurately measuring your competency in the content area described above.
Study Strategy and Where to Find Training Curriculum

Talk to people! Every organization has one or more expert in any security subject area you could imagine.

**Study Strategy**

Cyber Security Essentials is an affordable option that is just as comprehensive as other well-known entry-level security exams in the market place, such as CompTIA Security+ and GIAC Security Essentials, to name a few. There is a lot to know, and you should give yourself plenty of time to study. Begin by reviewing Prometric’s list of references and resources that are available on the website (also included in this guide). After looking over this list, you can start focusing on those references you realistically have time to absorb. Here are some other useful ideas:

- The Exam is 100 well-researched multiple-choice questions, and the questions went through a rigorous process before being placed in the Exam.
- You will have 2 hours to complete the Exam, and no breaks are included.
- There is no extra penalty for wrong answers. (Wrong answers are not subtracted from the right answers.)
- You need to get 180 “points” out of a possible 300 to pass. Prometric applies advanced statistical methodology to convert to a 3-digit scale that will allow the same ability level to be required to pass over time and across multiple versions of the test.
- The Exam questions force you to read them carefully and consider context.
- You should understand that the Exam tests your in-depth knowledge and your ability to integrate knowledge and experience, not your ability to merely memorize facts.
- Attack the Content Domains one at a time, remembering that you will want to review the material. Remember to make time for review.
- Assemble the material reflecting each Domain in turn.
- Read, review and repeat. Repetition and review are good.
- Identify those non-security areas in which you need deeper knowledge and get up to speed on them. We can't tell you what to study here, but you'll see your technical knowledge gaps as you study.
- Identify those security areas where you need additional help. Focus on them.
As you look over the sample Exam questions, you’ll see what we’re getting at. They include the following:

1. **A company needs to digitally sign all of the data sent to its customers. What should the administrator use to digitally sign the data?**
   - (A) Asymmetric Keys
   - (B) Standard Keys
   - (C) Symmetric Keys
   - (D) Quantitative Keys

2. **What standard does a Certificate Authority (CA) use to create a certificate?**
   - (A) X.509
   - (B) X.802
   - (C) X.423
   - (D) X.129

3. **The concept of comparing the best practices and performance metrics of other companies with similar processes is known as:**
   - (A) Benchmarking
   - (B) Gap Analysis
   - (C) Baselining
   - (D) Quantifying

4. **If an intrusion detection system wanted to only monitor web traffic, on what would the rules filter?**
   - (A) IP Address
   - (B) Port
   - (C) User Name
   - (D) Destination Name

5. **What security technique can be used to identify malicious HTTPS (Secure Hyper Text Transport Protocol) tunnels?**
   - (A) Detection inspection
   - (B) Context inspection
   - (C) Plain HTTP inspection
   - (D) SSL inspection

**Training Curriculum**
You are also fortunate that there are now lots of training courses at a host of IT training organizations who have strong partner relationships with Prometric, including New Horizons Learning Centers and Global Knowledge, to name just two. You will find that they have reputable training material and even cyber security "boot camps" that will help you along the way.
Exam-Taking Tips

+ Enter the Exam room as rested and relaxed as possible. Forget about last minute cramming. Passing Cyber Security Essentials depends on in-depth understanding. Cramming the night before won't help you. Rest will.

+ Pay attention to the testing center regulations and requirements. Prometric is serious about the security of the Exam and the testing environment, so expect a great deal of monitoring and scrutiny.

+ Study the questions carefully. No word is wasted. Every word is important. Remember that the "easy" questions might have a nuance you are not expecting. Remember also, these questions are highly researched. Every word in the question is there for a reason. On the flip side, try not to read into a question a meaning or context that is not literally in the question.

+ Look closely for key words, especially NOT, EXCEPT, FIRST and BEST.

+ Think the "big picture." Look for the most universal or general choice in the list of response options.

+ Try to eliminate the obviously wrong choices. Every choice you eliminate works in your favor.
Reference Materials and Resources

You will want to arm yourself with some of the more helpful texts. The authors of this document found the following books and online resources to be helpful. You are also fortunate that there are now lots of books hitting the CISSP marketplace. Just go to a bookseller of your choice (e.g., Amazon) and search on topics such as "CISSP."

Books

1. Amies, Alex; Sluiman, Harm; Liu, Guo Ning, Infrastructure as a Service Cloud Concepts, (2012) -Developing and Hosting Applications on the Cloud. IBM Press.


**Internet**
The Web is a fantastic source for material, too. A search with the “CISSP” key word, for example, will result in lots of material. In addition, a search on the Domain titles will uncover lots of material, too. Here are some of the better Web sources we recommend:

https://www.owasp.org - OWASP - The Open Web Application Security Project
http://www.postcastserver.com
http://www.n2net.net
http://www.pcmag.com/encyclopedia_term/0,1237,t=whitelist&i=54441,00.asp
http://netforbeginners.about.com
http://www.us-cert.gov
http://www.sans.edu/research/security-laboratory/article/it-separation-duties - SANS Technology Institute
http://www.openxtra.co.uk/articles/data-center-environmental
http://www.dna.gov
http://www.theiia.org
http://www.iert.org - The Internet Engineering Task Force (IETF)
http://www.domaintools.com
http://www.auditnet.org
http://searchvmware.techtarget.com
http://www.clir.org – Council on Library and Information Resources
Prometric, a wholly-owned subsidiary of ETS, is a trusted provider of technology-enabled testing and assessment. With more than 20 years’ experience, innovative testing methods, market-leading solutions and a secure worldwide network of more than 4,000 IT testing centers, you can count on us for your IT Certification program in cyber security.

Find Out More
Just visit www.prometric.com

Copyright© 2013 Prometric, Inc. All Rights Reserved.