Isaca’s security certifications

Somchai Patviboon
CISA,CISM,CRISC,CGEIT, Cybersecurity fundamentals, Cybersecurity audit

2016

CAREER PATH: CYBERSECURITY CERTIFICATIONS

CSX training and certifications offered for skill levels and specialties throughout a professional’s career.

CSX, ISACA

www.isaca.org/csx-certifications
3. Exam details
The Cybersecurity Fundamentals Certificate exam is an online, closed-book, remotely proctored exam. It covers five domains and includes a total of 75 questions. The number of questions in each domain depends on the weight assigned. The chart on the right displays the domains and the weights assigned to each domain.

Each multiple-choice question has four options with only one correct answer. You will be given 2 hours (120 minutes) to complete the exam. The passing score is 65%.

Individuals holding an ISACA certification (CISA/CISM/CGEIT/CRISC) may claim two CPE credits for each examination hour when a passing score is achieved. No CPE certificates will be provided upon passing the exam.

2. Cost of the Cybersecurity Fundamentals Exam
Each exam is priced at $150 USD. There is a discount available if you choose to purchase the exam with the Study Guide. Each retake exam is also priced at $150 USD.
Packet Analysis Certificate Exam

The CSX Packet Analysis Certificate Exam assesses candidates understanding of packet and protocol analysis. The two-hour exam is a real-time, hands-on exam which challenges students to demonstrate their skill set in a live environment.

This two-hour exam contains no multiple-choice questions or simulations and intentionally restricts access to the internet. Where applicable, man pages and help files are available.

Continuing Professional Education (CPE) Credit Count: 4.2 CPEs per examination hour) when a passing score is achieved.

Linux Application and Configuration

The Cybersecurity Nexus (CSX) Linux Application and Configuration (CLAC) course provides students an understanding of Linux operating systems, commands, and capabilities. Students will work with real Linux systems in real environments and will leverage commands, applications, and toolsets to complete tasks in a cybersecurity environment. Upon completion, students will be able to proactively leverage Linux to navigate, connect, and enhance business systems and networks – valuable traits in the cybersecurity field.

Continuing Professional Education (CPE) Credit Count: 20
CSX-P

Recognized as a Cybersecurity Practitioner.

Be recognized among the world’s most qualified cybersecurity professionals with ISACA’s CSX® Cybersecurity Practitioner Certification (CSX-P).

1. Apply now through the Comprehensive CSX® Cybersecurity Practitioner Certification Suite—a comprehensive training experience that includes in-depth training along with a fast-tracked exam and certification. You can train, test, and certify all online.
2. Join them—apply now through the Accelerated CSX® Cybersecurity Practitioner Certification Suite—a fast-tracked training and certification experience where you can train, test, and certify all in one speedy, 3-step process.

3 Step Process to Getting Your Certification

1. Practice Your Skills — Earn CPE Credits.
   - Take the 10-practice labs included in your own pace. The labs cover all 5 cybersecurity domains and are conducted in our exact live network environment. Each lab earns 0.5 Professional Education (PE) credits.

2. Take the 1-hour Online Challenge Assessment.
   - Complete five cybersecurity skills assessment questions conducted in the same live network environment you practiced in. If you pass all five challenges, you’ll qualify for the CSX-P certification and earn an additional 2 CPE credits.

3. Apply Immediately Online.
   - Upon successful completion of the 1-hour assessment, immediately create a CSX-P certification application and affirm at least one of the following statuses as a professional certified as a holder of the CSX® Certifications:
   - OR
     - Your 3 year’s experience in 3 or more of the 5 CSX-P cybersecurity domains which align with those of the globally accepted NIST Cybersecurity Framework:
       - Identify, Protect, Detect, Respond, and Recover
Course Bundle

CSX Penetration & Vulnerability Tester Pathway

Career Objective: Penetration Tester | Application Security Architect | Application Security Analyst | Senior Penetration Tester | Security Analyst

The CSX Penetration Testing training package provides students with the knowledge and skills required to perform cyber security penetration testing. Course content is enhanced by live lab environments, where you are tasked to identify, scan, and exploit real targets through leveraging multiple testing tools and techniques. Each lab sharpens your skills and prepares them for a career in penetration testing.

- A skills assessment will help identify strengths, weaknesses, and knowledge gaps to focus your learning.
- In the CSX Penetration Testing Overview Course, learn the comprehensive process of finding, understanding organizational weaknesses, and running vulnerability and applications tests.
- The CSX Vulnerability and Application Course, both the content and lab are aligned higher, increasing in difficulty, but providing more skill targets.
- In the CSX Exploitation Course, you will learn to detect and perform multi-hop application attacks, which create deeper points of penetration within a target system.
- Each 32-week focus area include highly tuned data within a live environment where you learn through hands-on application and real-time scanning.
- These certificate exams provide the opportunity to prove new skills and earn the following certificates: CSX Penetration Testing Overview (PTO) Certificate, CSX Vulnerability and Exploration (CVE) Certificate, CSX Advanced Exploitation (CAE) Certificate.
- Skim through access to test and your schedule 2/27.

Continuing Professional Education (CPE) Credit Count: 84

This training is recommended for individuals with a fundamental knowledge of cyber security including the skills covered in CSX Fundamentals, CSX Technical Foundations, and CSX Cybersecurity Foundations.
Small course - Beginner

Integrity and Hashing

DNS Packet Analysis

HTTP Packet Analysis

In-Depth Scanning

Introduction to Forensics Imaging

Network Scanning

Scanning for a Lost Asset

Securing Web Browsers

Server Backup

System Baselining

Packet Analysis

System Baselining

Mark Analysis

lets us detect if the corporate intellectual property is being smuggled from their

Price represents the tier membership

Buy Now

or pay later by invoice

continuing professional education (CPD) credit count: 2
Small course- intermediate
Small course- Advance

Testing Web Applications

Conduct testing against newly developed web applications to ensure they do not pose a risk.

Difficulty: Advanced

CSP Domain: Threat

Students will identify web application vectors, interact with bugs, and mitigate threats.

Continuing Professional Education (CPE) Credit Count: 2

Part of a comprehensive defense-in-depth implementation includes testing new capabilities and applications before implementing them into an organization's production network. This course teaches how students can conduct testing against newly developed web applications to ensure they do not pose a risk to organizational assets.

Continuing Professional Education (CPE) Credit Count: 2
Oct 2018

Ensure your organization has the controls in place to handle cyber threats and reduce risk.

Cybersecurity Audit

- The Cybersecurity Audit Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits. It provides security professionals with an understanding of the audit process, and IT risk professionals with an understanding of cyber-related risk and mitigating controls.
  - cybersecurity and audit’s role, cybersecurity governance, and cybersecurity operations.
Who Should Consider the Cybersecurity Audit Certificate and Training Program?

- **IT audit professionals and enterprises** who need additional guidance on auditing cybersecurity
- **Security professionals** who need an understanding of the audit process
- **Risk and assurance professionals** who need in-depth knowledge of cyber-related risk and mitigating controls
- **IT professionals** who want to learn more about what an IT auditor needs to consider when auditing cybersecurity

---

**WHAT YOU’LL LEARN**

- Understand security frameworks to identify best practices
- Define threat and vulnerability management
- Assess threats with the help of vulnerability management tools
- Build and deploy secure authorization processes
- Explain all aspects of cybersecurity governance
- Distinguish between firewall and network security technologies
- Enhance asset, configuration, change and patch management practices
- Manage enterprise identity and information access
- Identify application security controls
- Identify cyber and legal regulatory requirements to aid in compliance assessments
- Identify weaknesses in cloud strategies and controls
- Perform cybersecurity and third-party risk assessments
- Identify the benefits and risks of containerization
- And much more!
ISACA’s Comprehensive Cybersecurity Audit Certificate Program Includes

**Your Choice of Training**
(See next tab for options)

Choose from one of three training options, based on individual learning style and needs: an online-paced course, a virtual instructor-led course, or in-person training workshop. Onsite training is available for enterprises wishing to train staff at time in one central location.

**Companion Study Guide**

This handy guide introduces you to cybersecurity and audit’s role, cybersecurity governance, and cybersecurity operations. Includes case studies offering a deeper dive into specific technology topics and appendices offering specific cybersecurity audit guidance, frameworks, controls and testing steps.

**Cybersecurity Audit Certificate Exam Voucher**

Once you’ve completed your training, schedule complete this online, remote-proctored exam convenience. Earning a certificate, and accompanying digital badge, demonstrates your comprehensive knowledge of cybersecurity audit concepts, and the risks and controls critical to organization’s cybersecurity.

---

<table>
<thead>
<tr>
<th>ONLINE COURSE</th>
<th>VIRTUAL INSTRUCTOR LED TRAINING</th>
<th>ON-SITE VIA ISACA TRAINING WEEKS, EVENTS OR WORKSHOPS</th>
<th>ENTERPRISE TRAINING OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anyone who prefers online, independent learning at his or her own convenience. The Online is delivered via the ISACA Learning Management System (LMS), and is available 24/7 access from any with a computer and a high-speed Internet connection. It also includes online pre- and post-tests to help you determine your knowledge level before starting.</td>
<td>Enjoy the advantages of live training—interaction with both the instructor and other course attendees—without time away from the office or costly travel. The easy-to-use, live web-based training virtually connects you to live lectures, demonstrations, and hands-on instruction from any location with a high-speed Internet connection.</td>
<td>In-person live training courses are available throughout the year from ISACA. This includes training for individuals at conference workshops and ISACA training weeks.</td>
<td>ISACA offers customized training options that meet the needs of your organization—including expert-led group training accessible virtually, or on-site at a location most convenient for you. Contact us to learn more today.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Duration</th>
<th>6 hours, over 2 days</th>
<th>12 hours, over 2 days</th>
<th>12 hours, over 2 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuing Professional Education (CPE) Credits</td>
<td>7</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Individual Pricing</td>
<td>Includes a Study Guide and Certificate Exam voucher with each training option</td>
<td>Includes a Study Guide and Certificate Exam voucher with each training option</td>
<td>Includes a Study Guide and Certificate Exam voucher with each training option</td>
</tr>
<tr>
<td>Individual Pricing</td>
<td>$1,099 member</td>
<td>$1,499 member</td>
<td>Pricing Varies</td>
</tr>
<tr>
<td>Individual Pricing</td>
<td>$1,149 non-member</td>
<td>$1,249 non-member</td>
<td>Pricing Varies</td>
</tr>
</tbody>
</table>

---

Highlighted: Duration 5 and 30 minutes, self-paced
Highlighted: Individual Pricing Includes a Study Guide and Certificate Exam voucher with each training option
he exam includes 75 multiple-choice questions and the passing score is 65%. You will be given 2 ours (120 minutes) to complete the exam.

rogram Prerequisites
ile not required, professionals who possess a fundamental understanding of cybersecurity concepts and prior audit experience will be st positioned to succeed in this course and the included Cybersecurity Audit Certificate Exam. Other ISACA offerings that can help professionals gain knowledge in these areas include:

- CSX Cybersecurity Fundamentals Certificate, Study Guide, Online Course and other related training options
- Fundamentals of IS Audit and Assurance
Certifications

Certified Information Systems Auditor

A CISA certification showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.

Maintaining your CISA certification requires earning 20 CPE annually and 120 CPE over your set 3-year cycle and payment of the annual certification maintenance fee. Learn more about maintaining your certification and what qualifies as CPE at www.isaca.org/cisacpepolicy.
Social Media Risk and Control

Key cybersecurity controls related to social media applications within an organization should address the following areas:
- Understanding the extent to which social media is used by the organization
- Risks of compromise / inappropriate use of the organizations
- Social Media Accounts
- Risk of employee use of Social Media (Malware, Data Leakage)
- Understand relevant laws and regulations

CPE= 10 Hours
ISACA® Cybersecurity Audit Certificate

ISACA HEREBY CERTIFIES THAT

Somchai Patviboon

Has successfully demonstrated a comprehensive understanding of risk, controls and security knowledge necessary to perform cybersecurity audits and critical to an organization’s cybersecurity program, by passing the ISACA Cybersecurity Audit Certificate Exam.

15 May 2019
Date Issued

2019-345900
Certificate Number

©2019 ISACA. All Rights Reserved
Abstract

State of Cybersecurity 2019 reports the results of the annual ISACA global State of Cybersecurity Survey conducted November 2018. While some findings point to known trends, many survey results reinforce previous and findings—specifically, that the need for trained and experienced cybersecurity professionals outweights the supply. State of Cybersecurity 2019 provides a distinctive view of cybersecurity from the perspective of those who define the field—cybersecurity managers and practitioners. This is the first report based on the survey, which focuses on the current trends in cybersecurity workforce development, staffing, budget, and gender diversity.

---

**FIGURE 3—ORGANIZATIONS REPORTING UNFILLED CYBERSECURITY POSITIONS**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>58%</td>
</tr>
<tr>
<td>No</td>
<td>35%</td>
</tr>
<tr>
<td>Don't know</td>
<td>7%</td>
</tr>
</tbody>
</table>

**FIGURE 5—PERCENTAGE OF CYBERSECURITY APPLICANTS WHO ARE WELL QUALIFIED FOR THE POSITION FOR WHICH THEY ARE APPLYING**

<table>
<thead>
<tr>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 25%</td>
</tr>
<tr>
<td>25 - 50%</td>
</tr>
<tr>
<td>50 - 75%</td>
</tr>
<tr>
<td>75 - 100%</td>
</tr>
</tbody>
</table>

---

Which of the following factors do you feel are causing cybersecurity professionals to leave their job roles?

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better financial incentives (e.g., salaries or bonuses)</td>
<td>82%</td>
</tr>
<tr>
<td>Promotion and development opportunities</td>
<td>57%</td>
</tr>
<tr>
<td>Better work culture/environment</td>
<td>46%</td>
</tr>
<tr>
<td>Flexible work policies</td>
<td>37%</td>
</tr>
<tr>
<td>Opportunities to work with latest technologies (e.g., AI)</td>
<td>35%</td>
</tr>
<tr>
<td>Remote work possibilities</td>
<td>33%</td>
</tr>
<tr>
<td>Lower work stress levels</td>
<td>30%</td>
</tr>
<tr>
<td>Family situation changes (e.g., children born, marriage)</td>
<td>18%</td>
</tr>
<tr>
<td>Chance to work in new industry</td>
<td>16%</td>
</tr>
<tr>
<td>Other reasons</td>
<td>9%</td>
</tr>
<tr>
<td>More diverse workplace</td>
<td>8%</td>
</tr>
<tr>
<td>Retirement</td>
<td>8%</td>
</tr>
<tr>
<td>Switching careers (e.g., leaving cybersecurity entirely)</td>
<td>8%</td>
</tr>
</tbody>
</table>