INSIGHTS AND RESOURCES FOR THE

# CYBERSECURITY PROFESSIONAL

CSX™ CYBERSECURITY NEXUS

BY

ISACA®

*Trust in, and value from, information systems*

# In enterprise IT, there is a single point where everything that matters in information, technology and business converges: **Cybersecurity Nexus (CSX)**, a new security knowledge platform and professional program from ISACA.

**PROTECT AND DEFEND YOUR ORGANIZATION.**

When it comes to security breaches and cyber-attacks, it is often not a matter of if an organization will experience an attack, but when it will happen. Yet, an overwhelming number of organizations still feel ill-equipped to handle an attack and the need for skilled cybersecurity professionals continues to grow exponentially.

To help address the global cybersecurity skills crisis head on, ISACA has created Cybersecurity Nexus™ (CSX). CSX is helping shape the future of cybersecurity through cutting-edge thought leadership, as well as training and certification programs for the professionals who are leading it there. Building on the strength of ISACA's globally-recognized expertise, it gives cybersecurity professionals a smarter way to keep organizations and their information more secure.

With CSX, business leaders and cyber professionals can obtain the knowledge, tools, guidance and connections to be at the forefront of a vital and rapidly changing industry. Because Cybersecurity Nexus is at the center of everything that's coming next.

"It is often not until [businesses] have been hit that they realize there is an issue and a need to be proactive and to put resources into this area"

Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, FACS CP, director of information security and IT assurance, BRM Holdich

## Introducing CSX Skills-Based Cybersecurity Training And Performance-Based Certifications

More and more cybersecurity professionals are turning to ISACA's Cybersecurity Nexus™ (CSX) for the knowledge, tools and guidance they need to gain the skills and expertise to be successful in their jobs. And, when it comes to cybersecurity, it's not enough anymore to just show you have the knowledge, it's about proving you have the technical skills and ability to do the job from day one. Our new skills-based training and performance-based certifications are designed to help you build, test and showcase your skills in critical areas of cybersecurity.

CSX certifications are game-changers — the first vendor-neutral cybersecurity certifications based on the testing and validation of actual technical skill, ability and performance. Whereas other certifications available today test for knowledge in a question and answer format, CSX training and exams are conducted in a live, virtual "cyber lab" environment and test on whether or not an individual has the skills and technical savvy to do the job. Driven by PerformanScore™, a learning and development tool that captures live feedback as the user performs specific tasks in response to real-world scenarios, CSX certifications measure skills and abilities against job role competencies.

## CSX Certification Path

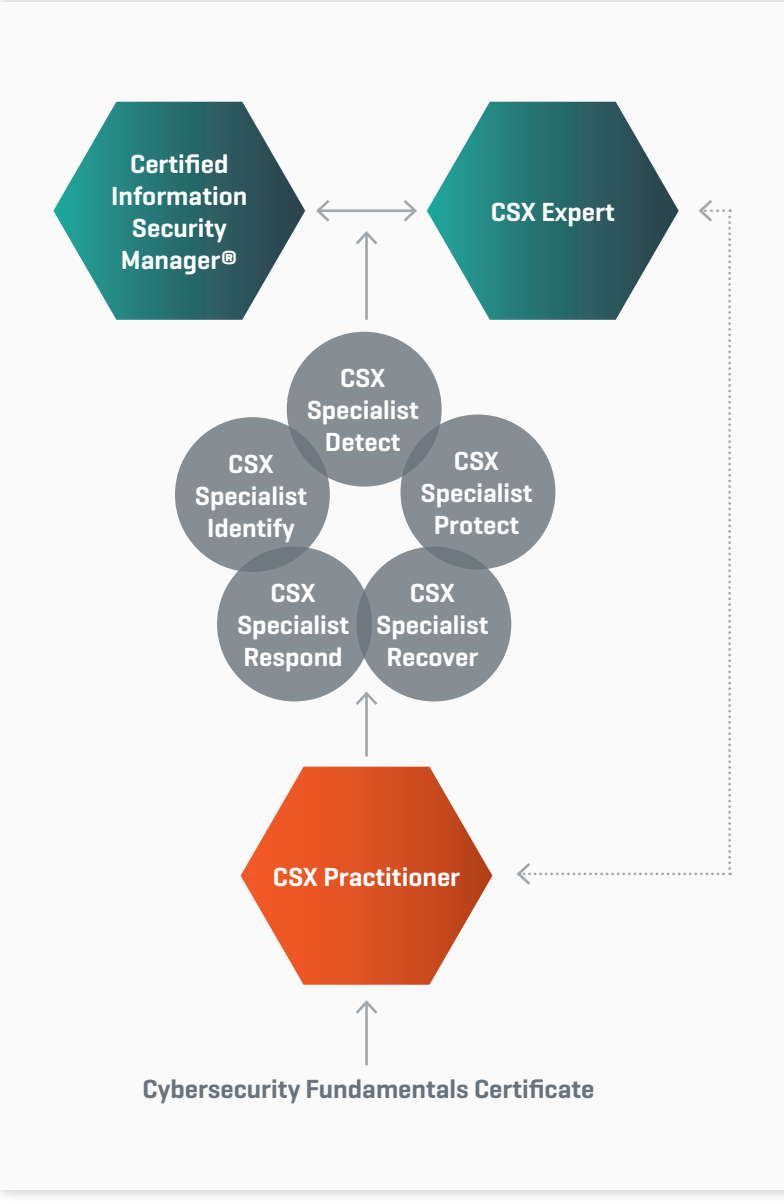
CSX certifications and training are designed to help you through every step of your career, no matter what your level of experience. With self-assessment tools and guidance on career management, we'll help you understand where you are now in your skills, where you want to take your career, and what you need to do to get there.

Our holistic program starts with the knowledge-based Cybersecurity Fundamentals Certificate for those who are new to the profession or looking to change careers, and centers on our performance-based certifications at the Practitioner, Specialist and Expert levels. These performance-based programs train, test and validate technical skill and ability and ensure you have the skills necessary to be successful in your role.

CSX certifications align to existing global cybersecurity frameworks and test the candidate's ability to perform tasks within the following cybersecurity areas in varying degrees of complexity:

- **Identify:** Identification of threats and vulnerabilities
- **Protect:** Protection of systems from outside threats
- **Detect:** Detection of threats and system vulnerabilities
- **Respond:** Response to, and mitigation of, cyber incidents
- **Recover:** Recovery from incidents and disasters

Each level of certification is differentiated by competency, and the levels are progressive in nature — with scenarios increasing in complexity and sophistication the higher the level. All levels assume an understanding of knowledge and concepts covered in Cybersecurity Fundamentals.



## CSX CERTIFICATIONS

### CSX | Practitioner

A CSX Practitioner certification demonstrates your ability to serve as a first responder, following established procedures, defined processes and working mostly with known problems on a single system. You'll show you have firewall, patching and anti-virus experience and can implement common security controls, perform vulnerability scans and some analysis.

**EXAM PREREQUISITES:**

> Related courses are not required to take the exam, but are recommended

**RELATED COURSES:**

Three hands-on training courses are offered to teach the skills needed at the CSX Practitioner level. Each course is 5 days and combines lecture with at least 50% hands-on lab exercise in a virtual cyber lab environment. Courses are available through leading global training partners.

**CSX | Practitioner Level 1: Identification and Protection**

The first course in the series focuses on key cybersecurity skills and includes foundational, real-world instruction in the Identify and Protect domains. Topics range from preliminary network scanning to security control implementation. Through the completion of multiple lab-reinforced modules, you'll learn how to apply industry-developed, experience-based methods to the identification of key networks and learn to develop appropriate protection mechanisms utilizing the basic concepts, methods and tools associated with cybersecurity controls.

**CSX | Practitioner Level 2: Detection**

The second course in the series goes deeper into skills focused in the Detect domain. You'll learn the basic concepts, methods and tools used to leverage cybersecurity controls in order to identify system events and non-event level incidents. By completing multiple lab-reinforced modules, you'll gain the skills necessary to detect potential network events and incidents. Topics range from incident packet analysis to IR report drafting and generation.

**CSX | Practitioner Level 3: Respond and Recover**

The final course in the Practitioner series provides hands-on instruction in the Respond and Recover domains. With course lecture backed up by lab sequences, you'll learn how to apply professional methodology to respond and recover from network incidents or disasters. You'll learn how to contain an event and protect assets and infrastructure and you'll discover the components and procedures required for a comprehensive incident response plan.

### CSX | Specialist

The CSX Specialist series offers you the opportunity to pursue a certification in a specialty area — allowing you to demonstrate deep knowledge and ability in that domain. Choose from five independent certifications: Identify, Protect, Detect, Respond or Recover. These certifications build on the skills developed in CSX Practitioner and test advanced concepts in each of the domains.

**EXAM PREREQUISITES:**

> CSX Practitioner certification

> Related courses are not required to take the exam, but are recommended

**RELATED COURSES:**

Each certification in the Specialist series is paired with one 5-day training course, designed to teach the skills needed to practice at a CSX Specialist level in that particular area. Each course combines lecture with at least 50% hands-on lab exercise in a virtual cyber lab environment. Courses are available through leading global training partners.

**CSX | Specialist: Identify**

This week-long course will help you gain an intermediate-level understanding of the concepts, skills and tools required to perform network asset and vulnerability identification. You'll learn how to analyze and assess cyber threats against multiple levels of infrastructure from host to system-level using industry-accepted methods and tools, as governed by the NIST and ISO publication guidelines.

**CSX | Specialist: Protect**

The CSX Specialist: Protect course offers practical instruction in the unique technical capabilities and governing policies that all members of a Computer Security Information Response Team (CSIRT) should maintain when protecting a network and its various components. The course covers areas such as: cybersecurity controls, control testing, vulnerability management, and plan maintenance.

**CSX | Specialist: Detect**

You'll learn how to distinguish network and system incidents and events with the CSX Specialist: Detect course. This course focuses on five key areas: intrusion identification, anomalous and malicious activity, attack analysis and reporting, system change remediation and defense mechanism enrichment. Upon completion, you'll know how to identify compromise indicators, assess potential damage, and provide appropriate data to first response teams.

### CSX | Specialist: Respond

The CSX Specialist: Respond course offers practical instruction on: incident response, scope determination, response plan implementation, digital forensics and incident documentation. Upon completion of the course, you'll be able to participate in attack analysis, determine and communicate the scope and severity of the event, execute and coordinate response plans, follow appropriate forensic processes and document information related to incident response.

### CSX | Specialist: Recover

You'll gain a deep understanding of the concepts, skills and tools required to fulfill tasks identified in organizational Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP). This course offers hands-on instruction in service restoration and associated support tasks, as well as on proper post-IR documentation methodologies, to ensure that appropriate changes are adapted to system-wide control documentation and organizational policy.

## CSX | Expert

A CSX Expert certification establishes your standing as a master-level security professional capable of identifying, analyzing, responding to and mitigating the most complex cybersecurity incidents — usually in intricate enterprise environments that pose significant exposure to attacks. CSX Experts are the authoritative source for all cybersecurity matters within an organization and approve cybersecurity controls. These individuals are ultimately responsible for root cause analysis and correlation for evaluating business impact. They work with senior management to maximize organizational cybersecurity successes and communicate business impacts related to cyber issues, and serve as team leaders for incident response and disaster recovery.

### EXAM PREREQUISITES:

> Related courses are not required to take the exam, but are recommended

### RELATED COURSE:

### CSX | Expert

With this week-long course, you'll gain the master-level technical capabilities to execute activities ranging from identification and analysis of new emerging threats, to vulnerability assessment, threat intelligence, metrics and incident detection or response — all the way up to performing detailed attack analysis and documentation of attack vectors/targets/scope of attack, response plans and post-incident monitoring of implemented cybersecurity controls.

## Get Certified and Set Yourself Apart

CSX certifications are testaments to real-life skills and excellence and show employers that you have not just the knowledge, but the ability to walk into an organization and actually do the job from day one.

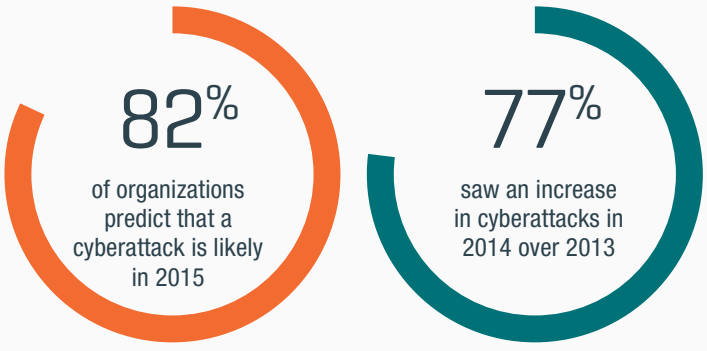
Globally accepted and recognized, CSX certifications:

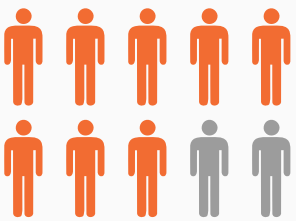
> Validate skills critical to real-life cybersecurity scenarios
> Signify higher levels of credibility to employers and organizations
> Increase professional recognition by peers and colleagues
> Provide credibility needed for career mobility

In addition, independent studies consistently rate ISACA's designations among the highest paying and highly regarded IT certifications, and CSX certifications are designed to carry on that tradition.

For more information on CSX skills-based training and performance-based certifications, please visit ***www.isaca.org/csx-certifications.***

## DID YOU KNOW



Nearly **8** out of **10** boards of directors are concerned with security

**56%** of enterprises spending more on cybersecurity in 2015

**SOURCE**: State of Cybersecurity: Implications for 2015, an ISACA and RSA Conference Survey | *www.isaca.org/state-of-cybersecurity-2015*

## Cybersecurity Fundamentals Certificate

The entry point into our cybersecurity program, our Cybersecurity Fundamentals offers a certificate in the introductory concepts that frame and define the standards, guidelines and practices of the industry. The certificate and related training are ideal for college/university students and recent graduates, those new to the field, as well as those looking to change careers.

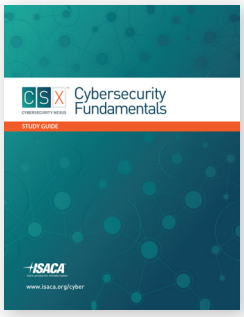
The Cybersecurity Fundamentals exam tests for foundational knowledge across five key areas:

- Cybersecurity concepts
- Cybersecurity architecture principles
- Cybersecurity of networks, systems, applications and data
- The security implications of the adoption of emerging technologies
- Incident response

The Certificate is aligned with the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE), which is compatible with global cybersecurity issues, activities and job roles. The Certificate is also aligned with the Skills Framework for the Information Age (SFIA).

The exam is available online, and may be taken from the privacy of your home or office at your convenience. Simply schedule the date and time that works for you, and your exam will be remotely proctored.

## Cybersecurity Fundamentals Study Guide




An excellent stand-alone publication for individual study of the core concepts and terms that frame and define the fast-changing and increasingly important field of cybersecurity, the guide was compiled and written by cybersecurity experts. The guide explores in detail the four key areas covered in the exam and Includes self-assessment questions and explanations of the answers.

For more information, or to register for the exam, go to ***www.isaca.org/cybersecuritycertificate.***

# EDUCATION & TRAINING

No one said becoming the best would be easy. Cybersecurity Nexus will help you achieve your career goals with rigorous, cutting-edge training and educational opportunities. From online training and virtual events, to in-depth courses and workshops and on-site training, you'll find what you need to build, grow and elevate your career, no matter what your level of experience may be.

In addition to the skills-based training courses offered with CSX certifications, we offer the following programs:

## Onsite Training

### Cybersecurity Fundamentals Online Course

Prepare to start or advance your role in cybersecurity with our new Cybersecurity Fundamentals Online Course — designed to help you grasp the principles that frame and define cybersecurity and understand the integral role of cybersecurity professionals in protecting enterprise data and infrastructure.

You'll enjoy the convenience of online learning through eight hours of instruction that covers the key areas of cybersecurity:

- Cybersecurity objectives and roles and the difference between cybersecurity and information security
- The Principles of Cybersecurity
- Information Security within Lifecycle Management
- Risks & Vulnerabilities
- Incident Response

Ideal for those preparing for a career or new to the field, or as a cybersecurity refresher course, this online learning can also help you showcase your new knowledge and skills by preparing you to obtain the Cybersecurity Fundamentals Certificate. The Course offers 8 hours of Continuing Professional Education.

### CSX Webinar Series

CSX offers a free, 60-minute webinar each month. Sessions are presented live by renowned subject matter experts who provide cutting-edge thought leadership, research, and advice on current and emerging cybersecurity threats, and discuss the tools necessary for succeeding in the ever-changing world of cybersecurity.

### Virtual Conferences

Enjoy the conference experience online with virtual exhibit halls, conference sessions, networking lounges and resource centers. It's a great and easy way to expand your knowledge, and it fits conveniently into busy schedules without travel time or expenses. In addition, ISACA members can earn up to five Continuing Professional Education credits.

## ON-SITE WORKPLACE TRAINING

Our on-site training programs bring expert cybersecurity instructors into the workplace to teach real-world courses, customized specifically for your employees. Onsite training offers you the opportunity to train your entire team in one or more sessions at one fixed price, with minimal downtime and without travel. In addition to enhancing workforce skills, on-site training enables attendees to earn valuable CPE hours towards maintaining certifications.

### AVAILABLE PROGRAMS:

**Cybersecurity Fundamentals**

The Cybersecurity Fundamentals onsite training course offers expert instruction on foundational areas of cybersecurity, stressing the importance of cybersecurity and the integral role of cybersecurity professionals. This two- or four-day course will help you: understand basic cybersecurity concepts and definitions; apply cybersecurity architecture principles; identify components of a cybersecurity architecture; understand malware analysis concepts and methodology; and recognize the methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.

**Implementing NIST Cybersecurity Framework Using COBIT 5**

This course is focused on the Cybersecurity Framework (CSF) — its goals, the implementation steps, and the ability to practically apply this information in your organization. Developed for individuals who have a basic understanding of both COBIT 5 and security concepts, and who are involved in improving the cybersecurity program for their enterprises.

**COBIT 5 Assessor for Security**

The COBIT 5 Assessor for Security course is modeled on our popular COBIT 5 Assessor Course, with a specific focus on cybersecurity. The course provides a basis for assessing an enterprise's process capabilities against the COBIT 5 Process Reference Model (PRM). Evidence-based to enable a reliable, consistent and repeatable way to assess IT process capabilities, this model helps IT leaders gain C-level and board member buy-in for change and improvement initiatives.

## Workshops

From fundamentals to advanced topics, CSX workshops can enhance your knowledge base and propel you toward your next CSX certification or career goal. Offered concurrently either before or after ISACA conferences and events, CSX workshops place special emphasis on key cybersecurity topics and offer more in-depth and hands-on experience than the standard session.

**Cybersecurity Fundamentals Workshop:**

The Cybersecurity Fundamentals Workshop offers expert instruction on foundational areas of cybersecurity, shows you how to: understand basic cybersecurity concepts and definitions; apply cybersecurity architecture principles; identify components of a cybersecurity architecture; understand malware analysis concepts and methodology; and recognize the methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies. This workshop is also a great way to prepare for the Cybersecurity Fundamentals Certificate exam.

For more information on all of our training and educational opportunities, please visit ***www.isaca.org/education***.

## EDUCATION/CONFERENCES

**Enhance your cybersecurity knowledge and skills at our global conferences, workshops and training events.**

CSX™ 2015 NORTH AMERICA
CYBERSECURITY NEXUS

### CSX 2015 North America Conference

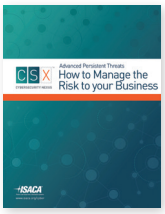
19-21 OCTOBER 2015 / WASHINGTON D.C.

Join the leading cybersecurity experts from around the world at the inaugural CSX 2015 North America conference on 19-21 October in Washington D.C. The conference will offer over 70 highly-insightful sessions, led by the top names in the industry and covering the most current knowledge, skills and tools available. You'll leave with insights and takeaways for every level of expertise and experience, and enjoy outstanding networking and social events while you're there.

**For more information and to register to attend, please visit *www.isaca.org/cyber-conference*.**

## RESEARCH & PUBLICATIONS

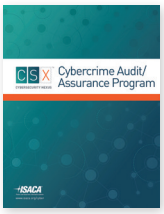
**Find the latest research and expert thinking on standards, best practices, emerging trends and beyond.**




> Advanced Persistent Threats: How To Manage the Risk To Your Business


> Transforming Cybersecurity


> Responding to Targeted Cyberattacks



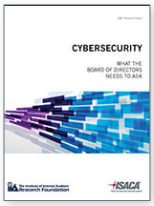

> Cybercrime Audit/ Assurance Program


> Implementing the NIST Cybersecurity Framework


> Security Mobile Devices


> Advanced Persistent Threat Awareness Study Results


> Overview of Digital Forensics




> Cybersecurity: What the Board of Directors Needs to Ask


> State of Cybersecurity: Implications for 2015


## The Nexus

Stay ahead of the ever-changing cyber landscape with our new CSX newsletter, The Nexus.

**Sign up to receive the newsletter free at *www.isaca.org/cyber.***

ISACA®
*Trust in, and value from, information systems*


3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

**Phone:** +1.847.253.1545

**Fax:** +1.847.253.1443

**Email:** info@isaca.org

***www.isaca.org***


To learn more visit us at ***www.isaca.org/cyber***

**Provide feedback:**
*http://www.isaca.org/ISACA-insights*

**Participate in the ISACA Knowledge Center:**
*www.isaca.org/knowledge-center*

**Follow ISACA on Twitter:**
*https://twitter.com/ISACANews*

**Join ISACA on LinkedIn:**
*http://linkd.in/ISACAOfficial*

**Like ISACA on Facebook:**
*www.facebook.com/ISACAHQ*