MID-CAREER ROADMAP

Cybersecurity certifications and skills

INFOSEC™

Cybersecurity certifications and the job market

The demand for cybersecurity professionals continues to grow, providing experienced IT and cybersecurity professionals with opportunities to upskill and advance their careers. Experience is a crucial factor for career progression, but so are certifications.

Earning a relevant certification demonstrates to potential employers that you possess the specific qualifications they're seeking. In fact, 87% of hiring managers say IT and cybersecurity credentials are an important factor in finding qualified individuals. As you progress in your career, your aspirations may shift. Certifications can equip you with the knowledge and skills to transition into new and exciting cybersecurity specializations. By showcasing your commitment to continuous learning expertise, you can also grab the attention of hiring managers.

However, even experienced professionals can have difficulty choosing between the many IT and security certifications. This guide is here to help.

What to expect in this ebook

Using the knowledge and experience we've gained training cybersecurity professionals for two decades, we'll break down the in-demand skills and the certifications employers rely on to help vet current and future employees.

Investing in the right certifications can open doors to new opportunities, higher salaries and increased job satisfaction. Read on to find the right certifications for your career journey.

448,033
U.S. cybersecurity job listings

87%
of employers say IT and cybersecurity credentials are important

54%
of cybersecurity professionals receive certification exam reimbursements

In-demand cybersecurity skills

Before exploring specific certifications, let's get a clear picture of the skills that are most sought after by today's employers. We can gather valuable insights from the most recent ISC2 Cybersecurity Workforce Report, which asked hiring managers what they are most looking for in cybersecurity professionals:

Cloud computing security: As more organizations move their data and applications to the cloud, securing these cloud environments is critical.

Communication skills: Strong communication is essential for any cybersecurity role. You'll need to clearly explain complex technical concepts to technical and non-technical audiences.

Risk assessment, analysis and management: Many cybersecurity roles are responsible for identifying potential security risks, analyzing their likelihood and impact and implementing effective mitigation strategies.

Security analysis: Being able to analyze large amounts of security data and identify threats is crucial for proactive defense.

Security engineering: Evaluating, implementing and monitoring security controls is a primary aspect of an effective cybersecurity program.

Governance, risk management and compliance (GRC): Having a strategic understanding of the GRC landscape helps to quantify overall risk and determine acceptable levels for your organization.

Application security: With the rise of web and mobile applications, it is important to secure them throughout the development life cycle.

Security administration: Day-to-day tasks like managing firewalls, VPNs, patching systems and mobile device security are essential for a smooth-running program.

SecOps: The ability to bridge the gap between security and operations teams is becoming increasingly important.

Identity and access management (IAM): Controlling who has access to what systems and data is a fundamental security principle.

The good news is that the certifications explored in this guide directly target these in-demand skill sets. We've consolidated the list of in-demand skills into six areas: cloud certifications, management certifications, technical certifications, risk and compliance certifications, application security certifications and communication certifications. We will cover each of the six on the following pages.

CLOUD

ISC2 CCSP

The ISC2 Certified Cloud Security Professional (CCSP) validates your technical skills in designing, managing and securing data, applications and infrastructure across modern cloud environments — the top set of skills that hiring managers are looking for. The CCSP is one of a portfolio of cybersecurity certifications managed by ISC2 that range from entry-level to more advanced, role-specific designations.

ISC2 recommends a minimum of five years of experience before you take the CCSP exam, but this can be lowered to three years with the right combination of education or an existing ISC2-approved credential.

What will I learn?

The CCSP curriculum encompasses six domains that provide a comprehensive understanding of cloud security:

- **Cloud concepts, architecture and design:** Covers the fundamental concepts of cloud computing and cloud security architecture
- **Cloud data security:** Covers best practices for securing data in the cloud, including encryption, key management and data life cycle management
- **Cloud platform and infrastructure security:** Covers security considerations for cloud platforms, infrastructure components and virtualization technologies
- **Cloud application security:** Covers securing cloud-based applications throughout the development lifecycle
- **Cloud security operations:** Covers topics like access control, federated identity and managing authentication systems
- **Legal, risk and compliance:** Covers the legal and regulatory landscape of cloud computing and how to ensure compliance

What type of jobs can I get?

Earning your CCSP can open doors to a wide range of cloud security careers, including:

- **Cloud architect**
- **Cloud administrator**
- **Cloud consultant**
- **Cloud security engineer**
- **Cloud security analyst**
- **Cloud specialist**

CLOUD

AWS Certified Security - Specialty

Amazon Web Services (AWS) is the leader in the cloud services market. Combining that with cloud security's demand in the job market makes the AWS Security certification a great potential cybersecurity credential.

The AWS Security certification is considered one of the most advanced certifications within the AWS ecosystem. It is perfect for professionals looking to advance their careers by demonstrating their expertise in cloud security. AWS provides a clear pathway for professionals to develop foundational skills, explore different roles and ultimately specialize in security if they choose.

Foundational

The AWS Certified Cloud Practitioner may be a good start if you have no IT or cloud experience.

Associate

Solutions Architect is a popular Associate-level certification requested by employers.

Professional

Once you earn the Associate level, a Professional-level certification further validates your expertise.

Specialty

As you advance in your career, consider earning a Specialty certification like AWS Security.

What will I learn?

This certification covers a range of domains that are crucial for securing AWS environments:

- **Threat detection and incident response:** Covers identifying and mitigating potential threats to AWS infrastructure
- **Security logging and monitoring:** Covers how to design, implement and troubleshoot a logging solution
- **Infrastructure security:** Covers how to design and apply security measures that protect the underlying infrastructure of the AWS cloud
- **Identity and access management:** Covers managing secure access to ensure only authorized entities interact with your AWS resources
- **Data protection:** Covers the mechanisms and best practices for encrypting and safeguarding data within the AWS ecosystem
- **Management and security governance:** Covers how to establish and enforce policies that govern the secure operation and compliance of AWS cloud environments

What type of jobs can I get?

Holding an AWS security certification can lead to a variety of in-demand security rules, such as:

- **Cloud security engineer**
- **Security operations engineer**
- **AWS security consultant**
- **AWS solutions architect**
- **Cloud architect**
- **Cloud governance, risk and compliance specialist**

CLOUD

Microsoft Azure Security Engineer Associate

Azure holds a strong position as the number two cloud service provider, making the Azure Security Engineer Associate certification highly relevant and sought after. This certification demonstrates a professional's ability to implement security controls, maintain security posture and manage identity and access within Azure environments.

Starting at the Associate level, this certification lays the groundwork for a career in Azure security. It is designed for those who have foundational knowledge and are looking to specialize further. The path continues in the Expert-level certification, which further validates one's mastery over Azure's security capabilities.

Fundamentals

Azure Fundamentals may be a good start if you have no IT or cloud experience.

Associate

Azure Administrator and Azure Security Engineer are popular Associate-level certifications requested by employers.

Expert

Once you pass the Associate level, an Expert-level certification further validates your expertise.

What will I learn?

This certification encompasses four domains essential for Azure security:

- **Manage identity and access:** Covers how to manage identities, provide secure access to applications and handle user privileges
- **Secure networking:** Covers implementing network security controls and managing secure internet protocols to protect against threats
- **Secure compute, storage and database:** Covers how to apply security, implement secure storage solutions and manage database security
- **Manage security operations:** Covers configuring and using security tools to monitor the health of Azure environments and responding to security incidents

What type of jobs can I get?

This Microsoft certification opens doors to exciting cloud security roles focused on Azure, including:

- **Azure security engineer**
- **Cloud security analyst**
- **Cloud security consultant**
- **Azure security architect**
- **Security operations center (SOC) analyst**

MANAGEMENT

ISACA CISM vs. ISC2 CISSP

When it comes to management-level cybersecurity certifications, two industry leaders stand out: ISACA's Certified Information Security Manager (CISM) and ISC2's Certified Information Systems Security Professional (CISSP).

ISACA CISM

The CISM certification has grown in popularity over the past five years as an alternative (or addition) to the CISSP certification. The CISM is less technical and more management-focused than the CISSP.

What will I learn?

- **Information security governance:** Covers establishing and enforcing effective information security policies and frameworks
- **Information security risk management:** Covers identifying, assessing and prioritizing information security risks
- **Information security program:** Covers how to develop, implement and maintain a comprehensive information security program aligned with organizational needs
- **Incident management:** Covers how to detect, contain and recover from security incidents

What type of jobs can I get?

- **Information security manager**
- **IT security director**
- **Security program manager**
- **Information security officer (ISO)**

ISC2 CISSP

The CISSP is the most requested certification in U.S. job openings. It is broader than the CISM and more technical, as it validates a more comprehensive set of information security concepts and best practices.

What will I learn?

- **Security and risk management:** Covers concepts like the CIA triad and managing organizational risk
- **Asset security:** Covers how to classify information and supporting assets for proper security controls
- **Security architecture and engineering:** Covers security models, architectures and design principles
- **Communication and network security:** Covers secure network architecture to protect communications
- **Identity and access management:** Covers implementing and managing authorization mechanisms
- **Security assessment and testing:** Covers testing security measures to ensure they function correctly
- **Security operations:** Covers day-to-day security operations and resources
- **Software development security:** Covers how to apply security controls to software development processes.

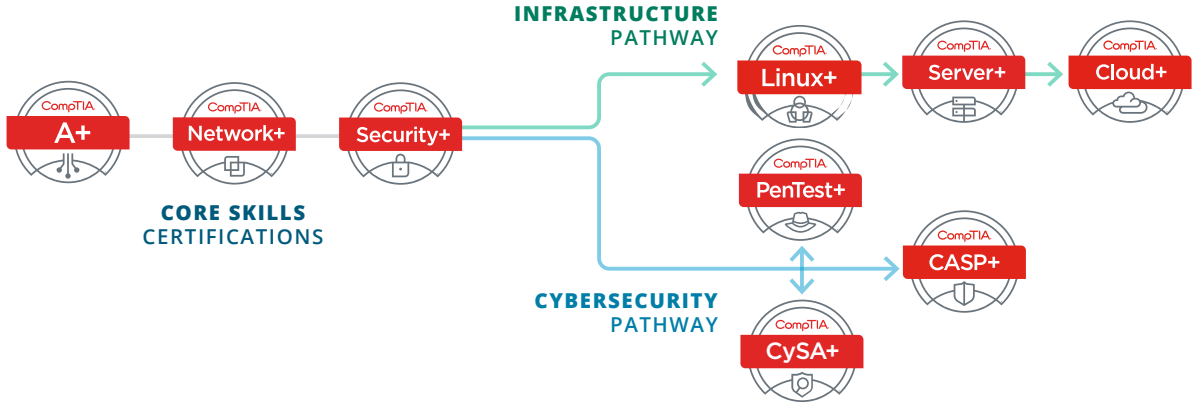
What type of jobs can I get?

- **Security manager**
- **IT manager/director**
- **Security engineer**
- **Chief information security officer (CISO)**

TECHNICAL

CompTIA CySA+, PenTest+ and CASP+

The CompTIA Security+ certification is the most popular cybersecurity certification in the world — and a stepping stone into more specialized technical certifications. It's no surprise, then, that CompTIA's other certifications are among the most in-demand from hiring managers and cybersecurity professionals.



What will I learn?

- **CySA+:** The CySA+ certification focuses on incident detection, prevention and response through continuous security monitoring. It emphasizes the importance of behavioral analytics to networks and devices to combat security threats.
- **PenTest+:** The PenTest+ certification focuses on penetration testing and vulnerability management. It validates your ability to plan and execute all stages of a pentest, including meeting legal requirements and communicating findings to stakeholders.
- **CASP+:** The CASP+ certification (soon to be renamed SecurityX) is an advanced technical certification aimed at security architects and senior security engineers. It validates your ability to design and implement secure solutions in complex enterprise environments.

What type of jobs can I get?

CySA+

- Cybersecurity analyst
- Threat intelligence analyst
- Security engineer
- Application security analyst

PenTest+

- Penetration tester
- Vulnerability assessment analyst
- Ethical hacker
- Information security analyst

CASP+

- Enterprise security architect
- Security operations manager
- Information security manager
- Senior security engineer

RISK AND COMPLIANCE

ISC2 CGRC

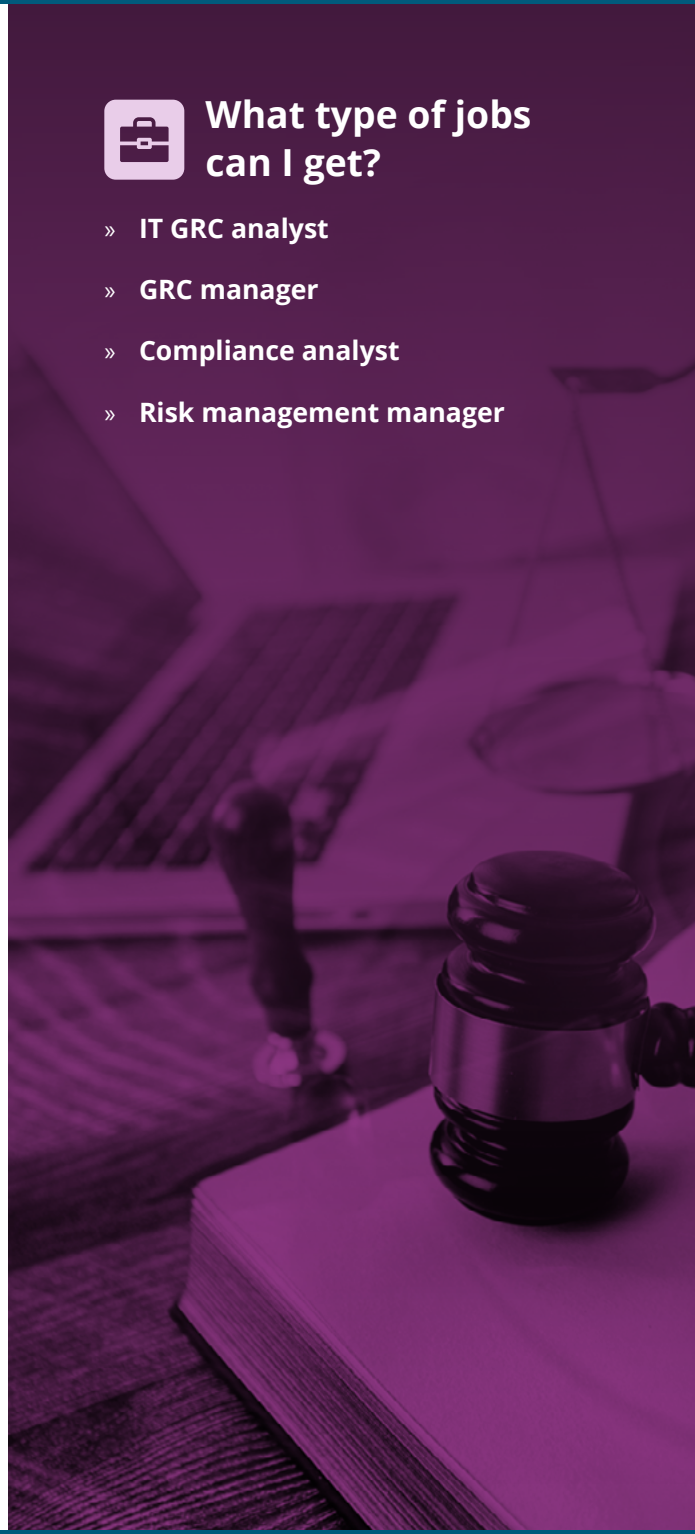
The ISC2 CGRC certification is tailored for IT, information security and assurance practitioners who focus on integrating governance, performance management, risk management and regulatory compliance within an organization. To qualify, candidates need at least two years of work experience in one or more of the seven domains covered by CGRC.

What will I learn?

- **Information security risk management program:** Covers how to establish a framework for managing security risks
- **Scope of the information system:** Covers the scope, architecture and purpose of an information system, as well as the type of information processed and its impact level on confidentiality, integrity and availability
- **Selection and approval of security and privacy controls:** Covers selecting and tailoring security and privacy controls, developing a continuous control monitoring strategy, and reviewing and approving a security plan
- **Implementation of security and privacy controls:** Covers implementing selected controls in accordance with current industry standards
- **Assessment/audit of security and privacy controls:** Covers audits, their preparation and how to move from initial assessment and auditing to executing remediation action plans, policies and final reports
- **Authorization/approval of information systems:** Covers compiling security and privacy approval documents, determining system risk and treatment options, and approving an information system
- **Continuous monitoring:** Covers determining the impact of changes to an information system, including supply chain risk analysis, revising monitoring strategies and decommissioning a system

What type of jobs can I get?

- **IT GRC analyst**
- **GRC manager**
- **Compliance analyst**
- **Risk management manager**



RISK AND COMPLIANCE

ISACA CISA

The Certified Information Systems Auditor (CISA) is the most popular ISACA certification and is a standard for IT audit professionals. It requires candidates to have five years of professional information systems auditing, control or security work experience. CISA is part of a broader ecosystem that includes other risk and governance certifications like CRISC, CGEIT and CDPSE (as well as CISM, mentioned above).

CISA

The most popular information systems auditing certification.

CRISC

Validates skills in risk management and using an agile-based approach to security.

CGEIT

Validates skills in IT enterprise governance required for corporate leadership.

CDPSE

Validates skills in creating and implementing technical privacy solutions.

What will I learn?

- **Information systems auditing process:** Covers a comprehensive understanding of the IT audit process
- **Governance and management of IT:** Covers how IT governance frameworks are implemented and how they impact auditing
- **Information systems acquisition, development and implementation:** Covers how to identify, assess and mitigate IT risks
- **Information systems operations and business resilience:** Covers the IT life cycle and associated security controls
- **Protection of information assets:** Covers best practices for securing and controlling IT operations

What type of jobs can I get?

- **Internal auditor**
- **Information systems auditor**
- **Information risk analyst**
- **IT security officer**
- **IT risk and assurance manager**

APPLICATION SECURITY

ISC2 CSSLP

The Certified Secure Software Lifecycle Professional (CSSLP) certification validates your experience in incorporating secure practices into all phases of the software development life cycle (SDLC). It's a top certification for individuals and employees of organizations focused on developing secure software. It emphasizes the importance of integrating security from the start to the end of the software creation process.

What will I learn?

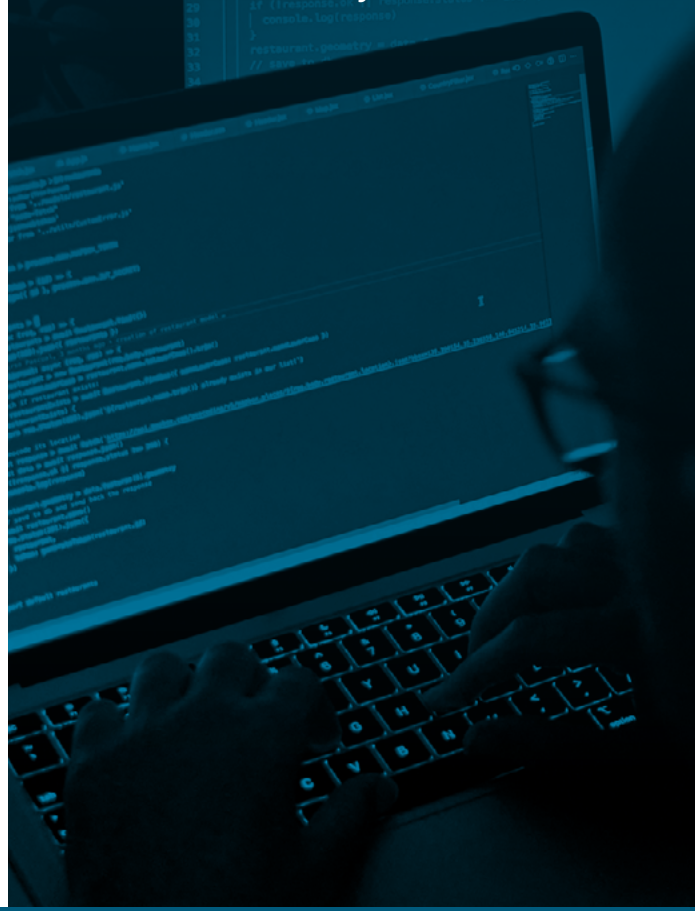
The CSSLP exam covers eight key domains of secure software development:

- **Secure software concepts:** Covers the core principles of secure software development, including confidentiality, integrity, availability and other security fundamentals.
- **Secure software lifecycle management:** Covers managing the lifecycle of a software project, including secure change management, patch management and configuration management.
- **Secure software requirements:** Covers gathering, analyzing and documenting a project's security requirements, including practices such as threat modeling and requirement traceability
- **Secure software architecture and design:** Covers identifying and mitigating design-level risks, creating secure architecture and ensuring proper error handling and encryption
- **Secure software implementation:** Covers secure coding guidelines, data handling and input validation to implement software securely and minimize risks associated with coding errors
- **Secure software testing:** Covers various testing methods, including static, dynamic and penetration testing
- **Software deployment, operations, and maintenance:** Covers topics such as secure installation, logging, monitoring and incident response.
- **Secure software supply chain:** Covers the secure acquisition of software, vendor risk management, software quality assurance and secure procurement practices

What type of jobs can I get?

Earning the CSSLP certification positions you for success in a variety of application security rules, including:

- **Secure software developer**
- **Application security specialist**
- **Software assurance analyst**
- **Security compliance analyst**
- **Software security architect**



COMMUNICATION

PMI PMP

Although the Project Management Professional (PMP) certification from the Project Management Institute (PMI) isn't a cybersecurity-specific credential, it holds immense value within the IT and cybersecurity realm. With over 1 million certified professionals globally, the PMP equips you with the essential skills and knowledge to manage any project effectively, regardless of industry.

In the world of cybersecurity, where projects can involve complex deployments, intricate incident response activities or large-scale security awareness initiatives, the ability to manage projects efficiently can mean the difference between success and failure. The PMP certification empowers cybersecurity professionals to lead and oversee these projects with confidence, ensuring successful outcomes that align with business objectives.

What will I learn?

Earning the PMP certification demonstrates your mastery of the core principles and best practices of project management, broken down into these domains:

- **People:** Covers in-depth knowledge of everything from building a team to ensuring they're properly motivated and continually trained.
- **Process:** Covers the administrative side of project management, including budgeting, creating project governance structure and addressing stakeholder goals and concerns
- **Business environment:** Covers proving the value of projects to the company, planning and managing project compliance and supporting enterprises experiencing organizational changes

What type of jobs can I get?

The PMP certification strengthens your candidacy for various it and cybersecurity project management roles, including:

- **IT project manager**
- **Security project manager**
- **Cybersecurity project manager**
- **Information security project manager**
- **IT security implementation manager**

Finding your career path

The certifications explored above represent some of the most popular and well-respected credentials within the cybersecurity industry. They provide a strong foundation of knowledge and validate your skills to potential employers. However, it's important to remember that this list is not exhaustive. There are numerous other cybersecurity certifications available, each catering to specific areas of expertise.

The path you choose will depend on your individual career goals and interests. If you have a particular area of cybersecurity that you're interested in, pursuing certifications in that specialty is an excellent approach. On the other hand, don't feel pressured to lock yourself into a single career path from the outset.

The ESG report, The Life and Times of Cybersecurity Professionals, found that gaining experience across different cybersecurity domains is a successful strategy for career advancement. Peers also agreed that "attending more training sessions" and "pursuing more security certifications" were among the best techniques to advance your career.

The most important takeaway

Remember, the cybersecurity industry is large and always changing. Embrace lifelong learning, explore areas of the field that interest you and leverage certifications to showcase your expertise. With dedication and the right guidance, you'll find a successful and fulfilling future here.

Sample of potential career paths to consider

Technical security

There are dozens of possibilities here, ranging from working in a Security Operations Center (SOC) monitoring threats to more proactive roles like penetration tester or threat hunter. You can also work in digital forensics investigating crimes, as a security engineer establishing controls or as an architect designing systems.

Governance, risk and compliance

This is a much-needed area that many overlook. Although these roles typically require more experience, consider pursuing roles like IT auditor, risk manager or compliance manager. Certifications offered by ISACA are well suited for this path.

Management

Security teams need both hands-on managers and strategic managers (like CISOs). If you enjoy managing teams and looking at the larger picture of organizational security, you can work towards these roles.

Privacy

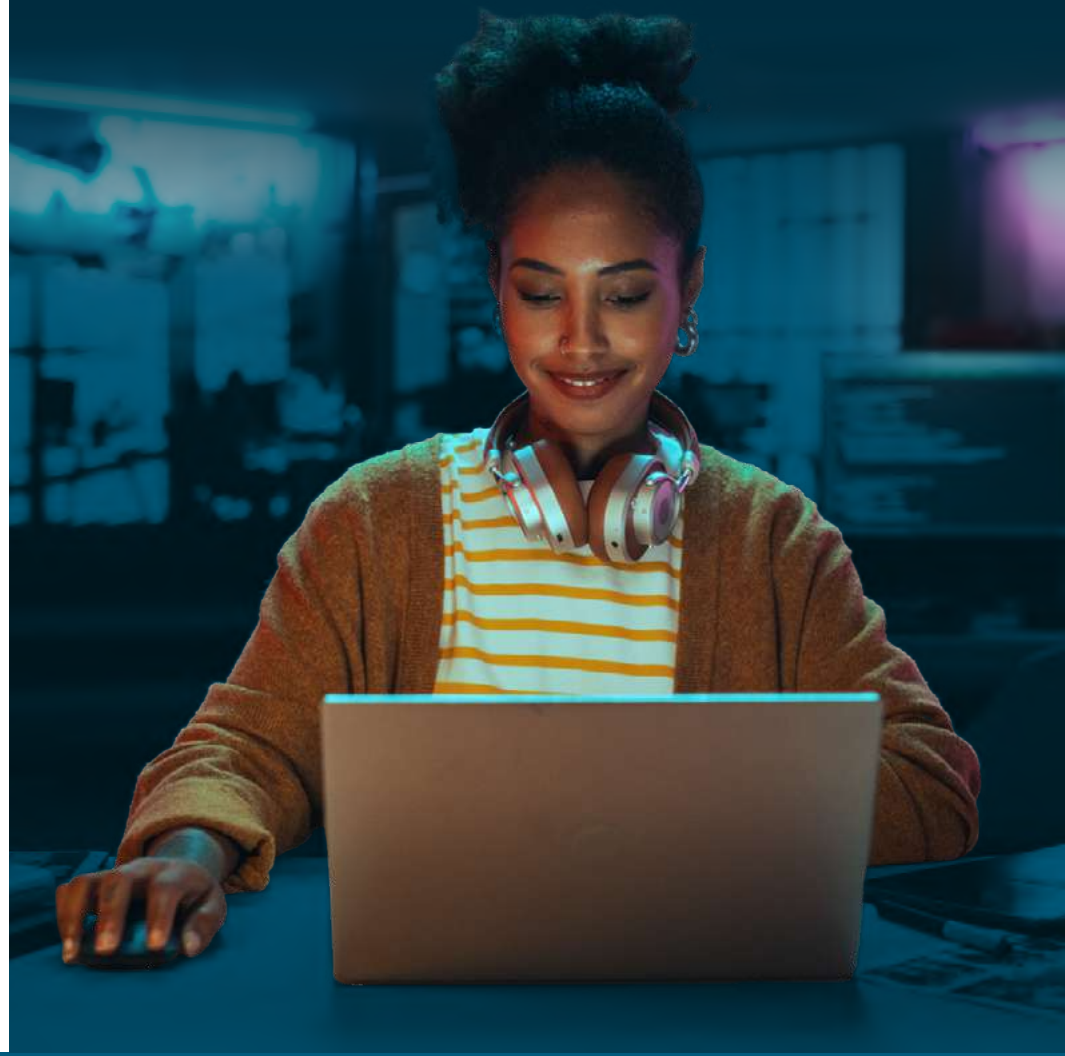
The IAPP offers certifications specifically geared towards data privacy compliance, a rapidly growing field. This can be an entire career path or a skillset you add to an existing role.

Additional resources

- Infosec Resource Center
- Infosec webcasts and events
- Cyber Work Podcast
- Infosec YouTube channel

Ready to get certified?

Browse the Infosec course library or speak with a career guide to learn more about your training options.



About Infosec

Infosec's mission is to put people at the center of cybersecurity. Through role-guided security training, our platforms — Infosec IQ, Infosec Skills and Infosec Boot Camps — help individuals and organizations protect their data, mitigate risk and empower employees. From security awareness for your accounting team to secure coding training for your developers, we'll help you deliver the right security education to protect your employees and organization.

Learn more at infosecinstitute.com.