INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

CIPP/US, CIPT & CIPM Boot Camp

Infosec's six-day authorized CIPP/US, CIPT and CIPM boot camp provides privacy professionals with the essential knowledge and understanding of U.S. privacy laws, technology concerns, and privacy policies and frameworks necessary to successfully pass all three certification exams.

Course description

- **The CIPP/US certification** focuses on U.S. privacy laws and regulations. You will learn about cross-sector limits on the collection and use of data and about specific regulations for the medical, financial, education, telecommunications and marketing sectors. The course also covers laws governing access to private information by law enforcement and national security agencies, issues related to workplace privacy and important state privacy laws.
- **The CIPT certification** focuses on core privacy concepts and essential elements of embedding privacy in information technology. The course covers privacy considerations for every stage of the information life cycle as well as effective privacy-enhancing techniques and technologies, including access management, data encryption and privacy-by-design principles. You will also learn about online services and technologies with specific privacy requirements and considerations, such as social media, cloud computing, and web browser privacy and security.
- **The CIPM certification** focuses on privacy and data protection practices in the development, measurement and improvement of a privacy program. The course covers organizational-level privacy program governance, development, implementation and measurement of a privacy program framework as well as the application of the privacy operational life cycle.

Boot camp at a glance

What you'll learn

- ✓ Introduction to U.S. privacy environment
- ✓ Privacy fundamentals and privacy in the information life cycle
- ✓ The privacy program operational life cycle

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 6-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Exam Pass Guarantee
- 100% Satisfaction Guarantee
- CIPP/US, CIPT and CIPM exam vouchers
- One year IAPP membership
- Six days of expert, live CIPP/US, CIPT and CIPM training
- Immediate access to Infosec Skills — including a bonus boot camp prep course — from the minute you enroll to one year after your boot camp
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Knowledge Transfer Guarantee

Who should attend

- Chief privacy officers (CPOs) and other senior information management professionals in both the U.S. public and private sectors or those employed by any organization with business or policy interests in the U.S.
- Privacy managers, legal compliance officers and risk managers
- Members of a privacy or compliance team
- Intermediate-level privacy professionals and entry-level candidates who are transitioning from non-privacy roles or who are entirely new to the privacy profession
- Information management professionals in the U.S. financial services, healthcare or telecommunications industries who seek to broaden their expertise into a general information privacy scope
- Corporate managers who are responsible for privacy within their teams, such as human resources, procurement, marketing and customer relations
- Non–privacy professionals who serve or support a privacy or compliance team and who need to achieve a consistent level of privacy education
- Information security professionals (CISO, CISSP)
- Information auditing and IT governance professionals (CISA, CISM)
- IT project/program managers
- Enterprise system architects (CTO, CIO)
- Business process professionals (purchase decision makers for IT services and products)
- Software, network, database and system professionals, including architects, designers, developers, engineers and administrators
- Anyone who wants to secure a place in the information economy

What you"ll learn

- The U.S. legal system: definitions, sources of law and the U.S. sectoral model for privacy enforcement
- U.S. federal laws for protection of personal data: FCRA and FACTA, HIPAA, GLBA and COPPA
- U.S. federal regulation of marketing practices: TSR, DNC, CAN-SPAM, TCPA and JFPA
- U.S. state data breach notification: California SB-1386 and select state laws
- Regulation of privacy in the U.S. workplace: FCRA, EPP, ADA and ECPA plus best practices for privacy and background screening, employee testing, workplace monitoring, employee investigation and termination of employment
- Using industry-standard guidelines for the collection, use, disclosure, retention and destruction of personal information
- Recognizing IT risks and mistakes organizations make when embedding privacy in the IT environment
- Privacy considerations for IT systems and applications
- Using established methods for end-user notification and choice through IT system and product interfaces
- Implementing system controls for identity and access management (IAM)
- Selecting appropriate privacy-enabling technologies
- Understanding requirements for identifiability, authentication and anonymization
- Understanding and addressing online privacy threats and challenges
- Understanding privacy considerations in evolving technologies (cloud computing, biometrics, IoT and more)
- Organizational privacy concerns, including creating a company vision, structuring the privacy team and communicating with stakeholders
- Developing and implementing a privacy program framework
- The privacy operational life cycle

What our students are saying

Incredible! I have attended classes where the instructor just read PowerPoints — our instructor added so much additional information to the class and knows the field of security inside and out! I was very pleased with his knowledge and instructional skills.

Sheree Moore
Mobile County Public Schools

I went to West Point for my bachelor's, Columbia for my master's and had multiple Army-led courses, and this ranks as one of the best, most engaging courses that I have ever had.

William Jack
Deloitte Consulting, LLC

The instructor was able to take material that prior to the class had made no sense and explained it in real-world scenarios that were able to be understood.

Erik Heiss
United States Air Force

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

CIPP/US, CIPT & CIPM details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6
Morning session	Introduction Structure of U.S. law and enforcement models	Access to private information by government and courts	Importance of privacy in IT environment	Privacy-enabling technologies and controls Common privacy techniques	Organizational level Developing framework	Stage I: Assess Stage II: Protect
Afternoon session	Regulating collection and use of data in the private sector	Workplace privacy State privacy laws	Privacy fundamentals Privacy in the information life cycle	Privacy in online environment Privacy and emerging technologies	Implementing framework Metrics	Stage III: Sustain Stage IV: Respond
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth boot camp prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

Day 1: U.S. laws, models and collecting data

- Course Introduction
- Structure of U.S. law and enforcement models
  - Common privacy principles
  - U.S. law sources, definitions and authorities
  - Legal liability in the U.S.
  - U.S. approach to protecting privacy and security of information
- Regulating collection and use of data in the private sector
  - Federal trade commission privacy and security enforcement actions
  - HIPAA and other healthcare privacy regulations
  - Privacy in financial sector
  - FERPA (education)
  - Privacy protection laws for telecommunications and marketing

Day 2: Access, privacy and state laws

- Access to private information by government and courts
  - Law enforcement access to financial data and communications
  - Laws related to national security
  - Privacy issues in civil litigation
- Workplace privacy
  - General workplace privacy concerns
  - Human resources management
  - Relevant U.S. agencies and laws
  - Employee background screening
  - Employee monitoring and investigations

- » Employee termination
- » State privacy laws
  - » Federal vs. state authority
  - » Marketing laws
  - » Financial data and data security laws
  - » Overview of data breach notification laws

Day 3: Privacy fundamentals and life cycle

- » Importance of privacy in IT environment
  - » Privacy and regulatory compliance requirements
  - » Privacy expectations
  - » Risks to IT environments
  - » Common mistakes
  - » Privacy vs. security
  - » Governance and role of IT professionals
- » Privacy fundamentals
  - » Important privacy documents (notices and relevant security and privacy policies)
  - » Relevant standards and frameworks
  - » SDLC privacy and security
  - » Privacy considerations in enterprise architecture (incident response, cross-border data transfers and Privacy Impact Assessments)
  - » Core privacy principles
- » Privacy in the information life cycle
  - » Stages of the information life cycle
  - » Privacy considerations for collection of information
  - » Privacy considerations for use of information
  - » Privacy considerations for disclosure of information
  - » Privacy considerations for retention of information
  - » Privacy considerations for destruction of information

Day 4: Privacy technologies, techniques and controls

- » Privacy-enabling technologies and controls
  - » Privacy challenges for enterprise IT architecture
  - » Identity and access management (IAM)
  - » Protecting credit card information
  - » Privacy and security controls for remote access and mobile devices
  - » Data encryption types, standards and implementation
  - » Automated data retrieval and audits
  - » Data masking and obfuscation
  - » Implementing DLP
  - » Privacy considerations for customer-facing applications
- » Common privacy techniques
  - » Authentication
  - » Identifiability of data
  - » Privacy-by-design principles
- » Privacy in online environment
  - » Online privacy expectations and requirements
  - » Privacy challenges with social media
  - » Common online threats and safeguards
  - » E-commerce and advertising
  - » Web tracking technologies (cookies, beacons and more)
  - » Machine-readable languages for privacy policies
  - » Web browser privacy and security features
  - » Secure web protocols (SSL/TLS, HTTPS)
- » Privacy and emerging technologies
  - » Cloud computing privacy and security concerns
  - » Wireless communications
  - » Principles of location-based technologies and services
  - » IoT and other smart technologies
  - » Electronic surveillance
  - » Biometrics

Day 5: Privacy program governance

» Organizational level
  » Creating a company vision
  » Establishing a privacy program
  » Structuring the privacy team
» Developing the privacy program framework
  » Developing privacy policies, standards and guidelines
  » Defining privacy program activities
» Implementing the privacy policy framework
  » Communicating the privacy framework to stakeholders
  » Ensuring alignment with laws and regulations
» Metrics
  » Identifying intended audience for metrics
  » Defining reporting resources
  » Defining privacy metrics
  » Identifying systems/application collection points

Day 6: Privacy operational life cycle

» Stage I: Assess
  » Documenting current baseline
  » Processors and third-party vendor assessment
  » Physical assessments
  » Mergers, acquisitions and divestitures
  » Conducting analysis and assessments
» Stage II: Protect
  » Data life cycle
  » Information security practices
  » Privacy by design
» Stage III: Sustain
  » Measure
  » Align
  » Audit
  » Monitor
» Stage IV: Respond
  » Information requests
  » Privacy incidents

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC