

Updated on 07/28/2026

[Sign Up](#)

CDPSE Certification Training

3 days (21 hours)

Overview

The CDPSE certification validates technical expertise in privacy by design, privacy governance, risk management, and privacy engineering. It is designed for professionals who design, deploy, and secure data protection solutions in demanding business and technical environments.

Our CDPSE Certification training course provides structured preparation for the official exam and the requirements of the ISACA framework. You will reinforce the key concepts of the program, with a curriculum designed for intermediate-level participants.

You will learn to connect the principles of privacy governance, privacy risk management and compliance approaches, mastery of the data lifecycle management, and privacy engineering practices. The goal is to help you think like a candidate ready for certification and like a practitioner capable of securing data processing operations.

The course also emphasizes reading the exam questions, analyzing use cases, consolidating cross-functional knowledge, and practicing with scenarios similar to those on the certification exam. This will better equip you to identify the right approaches, prioritize controls, and justify your technical choices.

By the end of this course, you'll have a clear understanding of the areas being assessed, an effective study method, and a solid foundation to approach the CDPSE exam with confidence.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the scope and structure of the CDPSE exam.
- Master the four domains of the ISACA framework and their requirements.
- Apply the principles of privacy by design to architectures and processes.
- Identify the risks, controls, and evidence expected in a compliance approach.
- Effectively prepare for the exam through targeted exercises and scenario-based activities.

Target Audience

- Compliance Manager
- Cybersecurity Auditor
- Security architect
- Data Protection Officer
- Data Governance Consultant

Prerequisites

- General knowledge of cybersecurity and data governance.
- Previous experience in privacy, compliance, or risk management.
- Understanding of PIA, data lifecycle, and security controls.
- Proficiency in reading technical and regulatory documents in English.
- Professional experience in an environment involving the protection of personal data.

Technical Requirements

- A recent computer with an up-to-date web browser and at least 8 GB of RAM.
- A stable Wi-Fi or Ethernet connection for remote sessions.
- A working microphone and headset for virtual classes.
- A PDF reader and an office suite compatible with Microsoft Office or equivalent.
- A user account to access the training materials, quizzes, and exercises.

CDPSE Training Program

[Day 1 - Morning]

Certification Fundamentals

- Understand CDPSE's role within the ISACA ecosystem.
- Identify the exam's objectives, format, and methodological expectations.
- Connect the certification to privacy, governance, and risk issues.
- Map out the four domains of the certification framework and their relative weight.
- Adopt a preparation strategy tailored to an intermediate level.
- Hands-on workshop: Initial assessment of current knowledge and identification of areas for improvement.

[Day 1 - Afternoon]

Privacy Governance and Organization

- Analyze the principles of privacy governance and their operational implementation.
- Examine the concepts of privacy by design, transparency, and consent.
- Define roles, responsibilities, and decision-making processes related to privacy.
- Integrate the management of third parties, subcontractors, and the supply chain.
- Link privacy policies, documentation, and program management.
- Hands-on workshop: guided review of a governance case study and identification of expected controls.

[Day 2 - Morning] Risks

and Compliance

- Define a structured and traceable privacy risk management approach.
- Identify threats, vulnerabilities, and impacts related to data processing.
- Use PIAs and risk assessments as decision-making tools.
- Understand compliance, auditability, and evidence requirements.
- Implement indicators for monitoring, control, and remediation.
- Hands-on workshop: developing a risk analysis matrix based on a business scenario.

[Day 2 - Afternoon] Data

Lifecycle

- Master the stages of data lifecycle management from collection to destruction.
- Define rules for classification, inventory, and flow mapping.
- Apply the principles of data minimization, use limitation, and data quality.
- Manage data retention, archiving, sharing, and transfers.
- Prepare expected responses to use cases related to AI and analytics.
- Hands-on workshop: reconstructing a data lifecycle and identifying control points.

[Day 3 - Morning]

Privacy engineering and technical controls

- Link privacy engineering issues to application and cloud architectures.
- Examine controls related to IAM, encryption, hashing, and logging.
- Understand the impacts of APIs, cloud-native services, and endpoints.
- Integrate hardening, patch management, and monitoring practices.
- Apply security technologies to real-world compliance use cases.
- Hands-on workshop: analyzing a technical architecture and identifying data protection controls.

[Day 3 - Afternoon]

Review and exam preparation

- Review cross-cutting concepts across the four domains with a focus on synthesis.
- Identify common pitfalls in certification questions.
- Practice the method of eliminating options and justifying answers.
- Reinforce key vocabulary and the relationships between concepts.
- Develop a personalized study plan for the final weeks leading up to the exam.
- Hands-on workshop: assessment quiz and detailed feedback on a sample mini-exam question similar to those on the certification exam.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methods.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.