

ISACA

CDPSE — Certified Data Privacy Solutions Engineer Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

24 HOURS

3 DAYS

At a glance

COURSE	CDPSE — Certified Data Privacy Solutions Engineer
TRACK	ISACA
DOMAIN	Cyber Security
LEVEL	Intermediate
DURATION	24 hours (about 3 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Four domains, mapped one-for-one to ISACA's CDPSE exam content outline and taught in the same order, so nothing on the exam is left uncovered.

The outline that defines the current CDPSE took effect for exams on 2 June 2025, with ISACA's matching preparation materials released on 2 April 2025. This was a structural change, not a reweighting: the credential moved from three domains to four, separating privacy governance from privacy risk management and compliance, and leaving privacy engineering as much the largest single domain at 39%. No further revision has been announced. Each domain below carries its published weighting, and we give it classroom time in proportion.

CDPSE is the privacy certification that expects you to build something. Policy literacy is assumed; the questions turn on how a requirement survives contact with a technology stack — what you tag, what you encrypt, what you delete, and what you can prove afterwards.

Domain 01 — Privacy Governance

The rules you are working to, and the operating machinery that keeps them running day to day. 20% of the exam.

- Personal information: what counts, what is sensitive, and how definitions shift between regimes
- Privacy principles, including privacy by design, consent and transparency
- Privacy laws and regulations, and reconciling obligations that overlap or conflict
- Privacy documentation: policies, standards, guidelines and notices that reflect real practice
- Organisational culture, structure and responsibilities, and where privacy accountability sits
- Vendor and supply chain management, from due diligence to contractual privacy terms
- Privacy incident management, and the notification clocks that start when one occurs
- Data subject rights and requests, and building a process that can actually answer them in time

Domain 02 — Privacy Risk Management and Compliance

Treating privacy as a risk discipline, then proving to someone else that you did. 18% of the exam.

- Risk management processes and policies, and integrating privacy risk with enterprise risk
- Privacy-focused assessments, including the privacy impact assessment and when one is required
- Privacy training and awareness, targeted at the roles that actually handle personal data
- Privacy threats and vulnerabilities, from re-identification to excessive internal access
- Risk response, and choosing between remediation, restriction and stopping the processing
- Privacy frameworks and mapping controls across more than one of them at once
- Evidence and artefacts: the records that demonstrate compliance rather than assert it
- Programme monitoring and metrics, and reporting privacy posture to people who must act on it

Domain 03 — Data Life Cycle Management

Personal data from the moment it arrives to the moment it is genuinely gone. 23% of the exam.

- Data inventory, dataflow diagrams and classification, and keeping them accurate as systems change
- Data quality, including accuracy and the correction obligations that follow from it
- Data use limitation, purpose specification and the discipline of secondary-use decisions
- Data analytics considerations: aggregation, data warehousing and artificial intelligence workloads

- Data minimisation applied at collection rather than retrofitted afterwards
- Data disclosure and transfer, including cross-border transfer mechanisms
- Data storage, retention and archiving, and retention schedules systems can enforce
- Data destruction, and verifying deletion across backups, replicas and downstream copies

Domain 04 – Privacy Engineering

The largest domain, and the reason this credential exists: implementing privacy in the technology itself. 39% of the exam.

- Infrastructure and platform technology, from legacy estates to cloud computing
- Devices and endpoints, connectivity, and the personal data that accumulates at the edge of the estate
- The secure development lifecycle, and privacy requirements that arrive before the first commit
- APIs and cloud-native services, and controlling what they expose by default
- Privacy-related security controls: asset management, identity and access management, patch management and hardening
- Communication and transport protocols, encryption and hashing, and monitoring and logging without over-collecting
- Consent tagging and tracking technologies, including cookie management, and carrying a consent decision through every system that touches the record
- Anonymisation and pseudonymisation, and being honest about which one you have achieved
- Privacy-enhancing technologies, and where they are ready for production use
- Artificial intelligence and machine learning considerations, including training data and model outputs

Who should take this

Privacy engineers, security engineers and architects who own privacy requirements, software and data engineers building systems that process personal data, IT and cloud practitioners working under a privacy programme, and privacy officers and analysts who need to specify technical controls rather than describe them.

ISACA requires three or more years of cumulative work experience performing the tasks of a CDPSE professional — privacy governance, privacy risk management and compliance, data life cycle work and privacy engineering — gained within the ten years before the certification application. There are no experience waivers or substitutions. You can sit the exam before you have the experience: candidates have five years from the date they pass to submit the certification application.

You will need working technical knowledge of how data moves through systems. You do not need to be a lawyer.

The exam

The CDPSE is set and awarded by ISACA. It is computer-based, delivered at authorised PSI testing centres worldwide or by remote proctoring.

- 120 multiple-choice questions
- Three and a half hours, 210 minutes
- A scaled score of 450 or higher is required to pass, on a scale of 200 to 800
- Available in English and Simplified Chinese

The exam registration is purchased separately from ISACA. We arrange it on your behalf and send you the details, and you book your own exam date. Certification also requires an application, an application processing fee, adherence to ISACA's Code of Professional Ethics, and continuing professional education to maintain.

How we deliver it

Four days, classroom or online live, or at your office for a private group. Teaching blocks are followed by design work: the group takes a system, maps the personal data through it, and specifies the controls that would make it defensible. Domain checkpoints each day, and a full-length timed mock on the final afternoon.

Mapped to the ISACA CDPSE exam content outline effective 2 June 2025. Taught from Hacky Security's own curriculum by instructors who hold the certification and build privacy controls for a living.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/cdpse/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.