CDPSE offers concise exam content outline areas designed to keep you at the top of your game and improve business performance. These statements and domains are the results of extensive research and feedback from IT privacy subject matter experts from around the world.

The statements in the below exam content outline are intended to depict the tasks performed by individuals who have significant experience and responsibilities in assessing, building and implementing comprehensive privacy solutions and the knowledge required to perform these tasks. They are also intended to serve as a definition of the roles and responsibilities of IT privacy professionals.

To qualify for early adoption of the CDPSE certification, you must meet the following requirements:

- Have 5 years of work experience performing the work described within the exam content outline below.
- Experience must be earned in a minimum of two CDPSE Exam Content Outline Domains below.

Experience waivers: Holding one of the following certifications: CISA, CISM, CGEIT, CRISC, CSX-P, FIP reduces the work experience requirements to 3 years.

For purposes of these statements, the terms "enterprise" and "organization" or "organizational" are considered synonymous.

Exam Content Outline

Domain 1: Privacy Governance (34%)

A. Governance
    1. Personal Data and Information
    2. Privacy Laws and Standards across Jurisdictions
    3. Privacy Documentation (e.g., Policies, Guidelines)
    4. Legal Purpose, Consent, and Legitimate Interest
    5. Data Subject Rights
B. Management
    1. Roles and Responsibilities related to Data
    2. Privacy Training and Awareness
    3. Vendor and Third-Party Management

4. Audit Process
5. Privacy Incident Management

C. Risk Management
    1. Risk Management Process
    2. Privacy Impact Assessment (PIA)
    3. Threats, Attacks, and Vulnerabilities related to Privacy

Domain 2: Privacy Architecture (36%)

A. Infrastructure
    1. Technology Stacks
    2. Cloud-based Services
    3. Endpoints
    4. Remote Access
    5. System Hardening
B. Applications and Software
    1. Secure Development Lifecycle (e.g., Privacy by Design)
    2. Applications and Software Hardening
    3. APIs and Services
    4. Tracking Technologies
C. Technical Privacy Controls
    1. Communication and Transport Protocols
    2. Encryption, Hashing, and De-identification
    3. Key Management
    4. Monitoring and Logging
    5. Identity and Access Management

Domain 3: Data Cycle (30%)

6. Data Purpose
    1. Data Inventory and Classification (e.g., Tagging, Tracking, SOR)
    2. Data Quality and Accuracy
    3. Dataflow and Usage Diagrams
    4. Data Use Limitation
    5. Data Analytics (e.g., Aggregation, AI, Machine Learning, Big Data)
7. Data Persistence
    1. Data Minimization (e.g., De-identification, Anonymization)
    2. Data Migration
    3. Data Storage
    4. Data Warehousing (e.g., Data Lake)
    5. Data Retention and Archiving
    6. Data Destruction