CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER

CDPSE

Duration: 4 days; Instructor-led (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The CDPSE: Certified Data Privacy Solutions Engineer course is an intensive, four-day examination preparation program to prepare individuals who are planning to sit for the Certified Data Privacy Solutions Engineer (CDPSE) exam. The course focuses on the three domains covered in the CDPSE Review Manual and includes class lectures, group discussions/activities, exam practice and answer debriefs. The course is intended for individuals with familiarity with and experience in the field of data privacy.

AUDIENCE

IT professionals experienced in the governance, architecture, and lifecycle of data privacy at a technical level.

PREREQUISITES

Before attending this accelerated course, you should have:

- 5 years' work experience performing the work described within the exam content outline • Experience in at least 2 of the exam domains If you have achieved one of the following certifications, then you'll need only 3 years' work experience:
- CISM: CISM Certified Information Security Manager
- CISA: CISA Certified Information Systems Auditor
- CRISC: Certified in Risk and Information Systems Control
- CGEIT: Certified in the Governance of Enterprise IT
- CSX-P: Certified Cybersecurity Practitioner

METHODOLOGY

This course includes presentations, hands-on labs, demonstrations, videos, and knowledge checks

COURSE OBJECTIVES

Participants in the CDPSE Exam Preparation course will be provided instruction designed to provide the following:

- An understanding of the format and structure of the CDPSE certification exam.
- A knowledge of the various topics and technical areas covered by the certification.
- Practice with specific strategies, tips and techniques for taking and passing the exam.
- Opportunities to execute practice questions with debriefs of answers.

COURSE CONTENTS

Module 1: Privacy Governance (Governance, Management and Risk Management)

- Identify the internal and external privacy requirements specific to the organization's governance and risk management programs and practices.
- Participate in the evaluation of privacy policies, programs, and policies for their alignment with legal requirements, regulatory requirements, and/or industry best practices.
- Coordinate and/or perform privacy impact assessments (PIA) and other privacy-focused assessments.
- Participate in the development of procedures that align with privacy policies and business needs.
- Implement procedures that align with privacy policies.
- Participate in the management and evaluation of contracts, service levels, and practices of vendors and other external parties.
- Participate in the privacy incident management process.
- Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation.
- Collaborate with other practitioners to ensure that privacy programs and practices are followed during the design, development, and implementation of systems, applications, and infrastructure.
- Develop and/or implement a prioritization process for privacy practices.
- Develop, monitor, and/or report performance metrics and trends related to privacy practices.
- Report on the status and outcomes of privacy programs and practices to relevant stakeholders.
- Participate in privacy training and promote awareness of privacy practices.
- Identify issues requiring remediation and opportunities for process improvement.

Copyright © 2021 by GemRain Consulting Sdn. Bhd.

Module 2: Privacy Architecture (Infrastructure, Applications/Software and Technical Privacy Controls)

- Coordinate and/or perform privacy impact assessment (PIA) and other privacy-focused assessments to identify appropriate tracking technologies, and technical privacy controls.
- Participate in the development of privacy control procedures that align with privacy policies and business needs.
- Implement procedures related to privacy architecture that align with privacy policies.
- Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation
- Collaborate with other practitioners to ensure that privacy programs and practices are followed during the design, development, and implementation of systems, applications, and infrastructure.
- Evaluate the enterprise architecture and information architecture to ensure it supports privacy by design principles and considerations.
- Evaluate advancements in privacy enhancing technologies and changes in the regulatory landscape.
- Identify, validate, and/or implement appropriate privacy and security controls according to data classification procedures.

Module 3: Data Lifecycle (Data Purpose and Data Persistence)

- Identify the internal and external privacy requirements relating to the organization's data lifecycle practices.
- Coordinate and/or perform privacy impact assessments (PIA) and other privacy-focused assessments relating to the organization’s data lifecycle practices.
- Participate in the development of data lifecycle procedures that align with privacy policies and business needs.
- Implement procedures related to data lifecycle that align with privacy policies.
- Collaborate with other practitioners to ensure that privacy programs and practices are followed during the design, development, and implementation of systems, applications, and infrastructure.
- Evaluate the enterprise architecture and information architecture to ensure it supports privacy by design principles and data lifecycle considerations.
- Identify, validate, and/or implement appropriate privacy and security controls according to data classification procedures.
- Design, implement, and/or monitor processes and procedures to keep the inventory and dataflow records current.

Copyright © 2021 by GemRain Consulting Sdn. Bhd.