Program Overview

Overview

Certified in Data Protection™ (CDP) is a comprehensive global training and certification program which leverages international security standards and privacy laws to teach candidates on how to protect personal and business data based on risks residing inside or outside of the information systems.

CDP is a registered certification designed and administered by Identity Management Institute (IMI).

Who should become CDP

Anyone concerned with the protection of personal or business data who would like to receive a comprehensive training which addresses all global data protection risks and be recognized as an expert in the data protection industry must consider CDP as a recognized information security certification.

Why become a CDP Professional

The *Certified in Data Protection* designation is the first industry certification introduced by Identity Management Institute (IMI) which addresses data protection risks with a global and comprehensive approach.

CDP was created because we believe that data security and privacy are interconnected yet current industry information security certifications are focused on specific aspects of data protection and offer limited value. For example, some certification programs focus on system security risks and others just address privacy of consumer information. Although specialized certifications offer great value within the scope of their programs, a comprehensive data protection training and certification program such as CDP is required and necessary for professionals who increasingly deal with many interconnected and global information protection risks.

Program Overview

Also, many of the global data security standards and privacy laws overlap to some extent which can be addressed cohesively in the comprehensive CDP data protection training program to educate candidates on how to address risks and compliance requirements efficiently. As such, CDP proposes a unique yet simplified data protection framework called KAGE to guide candidates in their data protection education and practices.

Definition of Data, Security, and Protection Terms

Data is a collection of facts such as numbers, words, measurements, observations or description of things which a business entity may consider to protect in order to reduce business risks. When data is processed, organized, structured or presented in a given context so as to make it useful, it is called information. Information is an organized yet limited subset of the data set.

Security is the degree of resistance to, or protection from, harm. Security enables protection of assets which happens to be technical in nature due to the fact that data often resides and moves in a digital format. Security and protection are very similar yet not the same. The amount of security measures defines the level of protection, and, the feeling of protection rises with rising security measures. Security may include technical tools to ensure protection from certain harm such as anti-virus software or firewalls, however, protection is more than just security and includes data life cycle management, business processes, and compliance.

In conclusion, Data includes all information pieces but information does not include all data elements. And, security is only one element which enables Protection of data. Therefore the term Data Protection is a more comprehensive term which is inclusive of all data elements and security measures based on risks.

Critical Risk Domains™ (CRD)

Identity Management Institute is the independent international organization which developed and administers the CDP designation and uses Critical Risk Domains™ (CRDs) to maintain the CDP training program and certify professionals worldwide. The

Program Overview

following CRDs are based on international standards which form the basis for managing the CDP program:

1. Governance and Management
2. Risk Assessment
3. Access Controls
4. System Security
5. Vendor Risks
6. Incident Management
7. Operations Security
8. Privacy & Compliance
9. Data Management
10. Business Continuity

CRD Descriptions

1. *Governance and Management* - Data protection governance refers to an organization's oversight and practices by a committee of the Board of Directors and/or Executive Management to provide strategic direction and support the data protection management team to achieve its objectives. The oversight team must identify the data protection leaders, review and approve the data protection program, and require an annual report regarding the state of data protection risk management and compliance.
   Data protection management refers to the identification of enterprise data as well as the development of the necessary documentation related to policies, procedures, and standards for protecting the data assets. To achieve their goals, Certified in Data Protection (CDP) experts leverage international standards, regulatory compliance requirements, and the KAGE framework, as well as risk assessment, enforcement, audit, and training processes.
2. *Risk Assessment* - CDPs periodically use a systematic process to evaluate potential data protection risks facing their organizations which may relate to confidentiality, availability, and integrity of data protection objectives. The results of the risk assessment are used to define a risk mitigation plan and improve the data protection strategy.

Program Overview

3. *Access Controls* - As enterprise data must be accessed for various business reasons, access to data must be authorized and intended for the business needs. Access controls are the system or process features that control who can access which resources and under what circumstances. Access controls also ensure accounts are monitored continuously or at least on a regular interval to detect unusually high risk activities. Access rights must be reconciled and certified at least annually.
4. *System Security* - This critical risk domain refers to the controls programmed into the networks and systems to support and enforce the data protection goals and objectives such as network traffic management, forced and periodic password changes, session timeout, etc. This domain also refers to the security guarantees during the System Development Life Cycle (SDLC), system acquisition, and system implementation. Security controls must be tested each time a system is procured, an application program is changed or introduced, or when related systems including databases and operating systems are maintained to ensure security controls are not impacted. In addition, evolving risks around mobile and cloud computing, remote access, privacy, cyber crime, and BYOD may have data protection implications which must be addressed.
5. *Vendor Risks* - Data protection risks may be transferred to third parties when various operations are outsourced to trusted vendors. In such cases, data protection requirements must be documented in the signed contractual agreements to ensure the vendor understands the security policies. In addition, a clause must be included in the contract to allow the company to audit and review the vendor's compliance with the agreed upon data protection requirements. Vendor on-boarding and subsequent audits are necessary to ensure their compliance.
6. *Incident Management* - Upon detection or reporting of a data protection incident, CDPs must follow a systematic and documented process to contact the appropriate parties for assistance and determine cause and effect of the incident. Following their initial assessment, CDPs must follow the established incident management plans to remediate and notify affected parties. It is necessary to have a documented, approved, and updated incident management plan in order to address all business risks and compliance requirements on a timely basis including lessons learned.

Program Overview

7. *Operations Security* - Data protection risks are not limited to information systems. There are non-system risks which must also be managed. Such risks may be around the on-boarding or termination process (background checks and collection of physical items), risk education, confidentiality of documents when using shared printers, and privacy of information when such information must be disclosed to others to name a few. Some operations security risks may ultimately affect system controls. For example, social engineering, social media activities, pretexting, and phishing scams, as well as violations from acceptable use policies may expose the company to risks.
8. *Privacy & Compliance* - CDPs must ensure that their organizations and data users ensure compliance with three general areas; policies, contracts, and regulations. In particular, privacy risk assessments must be performed either independently or in conjunction with another risk assessment project. The privacy management components such as policies, procedures and user training must be addressed in the data protection program.
9. *Data Management* - This domain refers to the process of properly classifying and handling data during data life cycle; initiation, retention, sharing, and disposal. There are many reasons why data should only be collected and created as necessary to meet the business needs. Data should also be retained securely and as long as necessary, shared securely and with the least number of parties possible fairly and lawfully, and disposed of according to international security standards.
10. *Business Continuity* - Business Continuity Plan and Disaster Recovery Plan ensure that business operations and systems can recover as quickly as possible and support business operations during incidents including security operations. This is directly related to the “availability” objective of data protection which includes backup, recovery, and testing for key data, systems, and business processes.

Certification Requirements

The requirements for becoming a CDP can be found on the website at:

http://www.identitymanagementinstitute.org/cdp/