KORNERSTONE
Training. Makes a differece.
a TRAINOCATE company

Certified Cloud Security Professional, CCSP®

D6 - Legal & Compliance

Domain 6 – Legal & Compliance

Domain Objectives

Cloud Security - Legal and Compliance

•Understand how to identify the various legal requirements and unique risks associated with the cloud environment with regard to legislation and conflicting legislation, legal risks, controls, and forensic requirements

• Describe the potential personal and data privacy issues specific to personal identifiable information within the cloud environment

• Define the process, methods, and required adaptations necessary for an audit within the cloud environment

• Describe the different types of cloud-based audit reports

• Identify the impact of diverse geographical locations and legal jurisdictions

• Differentiate between cloud to enterprise risk management and its implications

• Explain the importance of cloud contract design and management for outsourcing a cloud environment

• Identify appropriate supply-chain management processes

Domain Agenda

MODULE	NAME
1	Understand Legal Requirements and Unique Risks Within the Cloud Environment
2	Understand Privacy Issues, Including Jurisdictional Variances
3	Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment
4	Understand Implication of Cloud to Enterprise Risk Management
5	Understand Outsourcing and Cloud Contract Design
6	Execute Vendor Management

International Legislation Conflicts

- Appraisal of legal issues relevant to cloud computing
  - OECD, APEC, EU Data Protection, ePrivacy
  - Legal controls

E-Discovery

- Challenges
- Considerations & responsibilities
- Reducing risk
- E-discovery in cloud environments (3 examples)
  - SaaS-based
  - Hosted eDiscovery (provider)
  - Data stored in the cloud
- Forensics requirements
  - ISO-27037, 27041, 27042, 27043, 27050 standards

Privacy & Jurisdictional Variances

- Borderless
- Difference between contractual and regulated PII
- Mandatory Breach Reporting

Some reasons for regulation of PII

- Due care is undertaken and ensured
- Apply adequate protections
- Increased protection of customer and consumers
- Ensure appropriate mechanisms and controls are implemented
- Reduce likelihood of malformed/fractured practices
- Establish a baseline level of controls and processes
- Create a repeatable and measurable approach to regulated data and systems
- Continued alignment with statutory bodies and fulfillment of professional conduct requirements
- Transparency between customers, partners, and related industries

Contractual Components

- Scope of processing
- Use of subcontractors
- Removal/Deletion of data
- Appropriate/Required data security controls
- Location(s) of data
- Return of data/Restitution of data
- Audits/Right to audit subcontractors

Cloud Security Audit

- Internal & External Audits
- Impact of requirements programs of cloud use
- Assurance challenges of cloud and virtualization
  - Audit scope statements
- Types of Audit reports
  - SOC I, II, III (service organization controls)
  - CSA STAR (security, trust & audit registry)
    - EuroCloud Star Audit, China C-Star (ref standard)
- Restrictions of audit scope
- Gap analysis

Cloud Audit Goals

- Ability to understand, measure, and communicate the effectiveness of cloud service provider controls and security to organizational stakeholders/executives
- Proactively identify any control weaknesses or deficiencies
- Obtain levels of assurance and verification as to the cloud service provider's ability to meet the SLA

ISO-27018 (Privacy for Cloud Consumer Data)

- Consent
- Control
- Transparency
- Communication
- Independent and yearly audit

Internal ISMS (ISO-27001)

- Information Security Management System
- Internal information security controls system
  - 14 domains
- Policies

Cloud Computing Security Policies

- Password Policies
- Remote Access
- Encryption
- Third-Party Access
- Segregation of Duties
- Incident Management
- Data Backup

Identification and involvement of relevant stakeholders

- Stakeholder identification challenges
- Communication coordination

- Specialized compliance requirements for highly-regulated industries
- Impact of distributed IT models
  - Communication / clear understanding
  - Coordination / management of activities
  - Governance of processes /activities
  - Coordination Is key
  - Reporting

Cloud & Enterprise Risk Management

- Risk profile, risk appetite
- Difference between data owner / controller and data custodian / processor
  - Data Subject means an individual who is the subject of personal data.
  - Data Controller means a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
  - Data Processor means any person who processes the data on behalf of the data controller.
  - Data Stewards responsible for data content, context, and associated business rules.
  - Data Custodians are responsible for the safe custody, transport, storage of the data, and implementation of business rules.
  - Data Ownership or Data Owners hold legal rights and complete control over a single piece or set of data elements.

SLA Management - metrics

Components and considerations –

- Availability
- Performance
- Security Privacy of the Data
- Logging and Reporting
- Disaster Recovery Expectations
- Location of the Data
- Data Format/Structure
- Portability of the Data
- Identification and Problem Resolution
- Change Management Process
- Dispute Mediation Process
- Exit Strategy

Cloud SLAs – more considerations

- Uptime guarantees
- SLA penalties
- Penalty exclusions
- Suspension of service
- Provider liability
- Data protection requirements
- Disaster recovery
- Security requirements

Key SLA elements

- Assessment of risk environment
- Risk profile
- Risk appetite
- Responsibilities
- Regulatory requirements
- Risk mitigation
- Different risk frameworks

- Quality of Service (QoS)

- Risk Management
- Metrics for Risk management

Outsourcing & contract design

- Business requirements
- Vendor management
  - Risk management (understanding risk exposure)
  - Supply Chain Management
    - Standards (ISO-28000)
    - Risk and impact assessment
- Accountability
- Frameworks & Standards
- Contract management