Cloud Data Security

CCSP Series - Chapter # 2

Cloud Data Security Overview

Shared Responsibility Framework

- **CSP:** Protects infrastructure, physical security
- **Consumer:** Manages application/data-level security

Consumer's Accountability

- Securing data remains the consumer’s duty
- Implementing adequate security measures is essential

Cloud Data Lifecycle

Data Lifecycle Stages

- **Create:** Data generated or modified
- **Store:** Data saved for retrieval
- **Use:** Data accessed for processing
- **Share:** Data access permissions granted
- **Archive:** Data stored long-term
- **Destroy:** Data permanently deleted

Lifecycle Security Controls

- Ensure protection at each phase
- Address phase-specific risks

Describe Cloud Data Concepts

1 Key Concepts and Personnel

- Involvement varies from C-level to operational staff
- Understanding the cloud data lifecycle is vital

2 Importance of the Cloud Strategy

- Aligns with business needs
- Incorporates security models for data management

Data Creation and Classification

Creation Phase Controls

- Data classified upon creation
- Manual or system-level classification supported

Storage Phase Controls

- Data-in-transit protections (e.g., TLS, VPN)
- Policies for data storage locations
- Access control and encryption management

Data Use and Sharing

Use Phase Controls

- Manage data flow with DLP and IRM
- Review access controls and accountability logs

Share Phase Controls

- Access authorization and grant procedures
- Reactive controls like DLP and IRM for unauthorized sharing

Data Archiving and Destruction

1 Archive Phase Controls

- Data encryption practices, key rotation, and media durability
- Consideration for long-term retrieval and format obsolescence

2 Destroy Phase Controls

- Balance data value against destruction methods
- Refer to NIST SP 800-88 for media sanitization

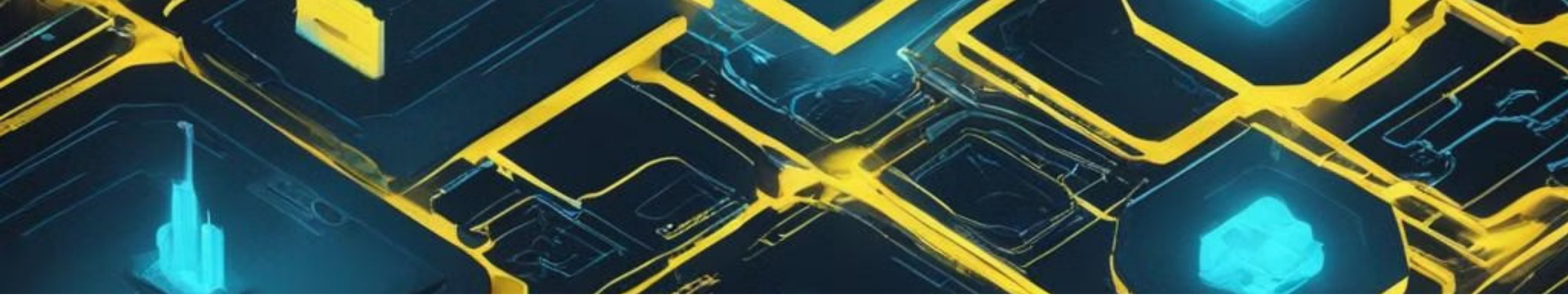
Data Dispersion and Data Flows

Data Dispersion Benefits

- Data split into chunks across physical devices
- Erasure coding for data reconstruction

Managing Data Flows

- Document with Data Flow Diagrams (DFDs)
- Capture data movements and regulatory compliance elements



Cloud Storage Types

IaaS, PaaS, SaaS Storage Explained

- Different models offer unique storage options
- Ephemeral, Volume, Object, and more
- Selection based on business and security requirements

Data Security Strategies

1 Encryption and Key Management

- **Apply at various layers:** storage, application, database
- Manage keys with practices such as key escrow

2 Hashing for Integrity Assurance

- One-way encryption for data integrity checks
- Supports nonrepudiation with proper implementation

Data Obfuscation and Masking

Obfuscation Methods

- Substitution, Shuffling, and more
- Realistic output data that retains no sensitive attributes

Masking Techniques

- Hiding specific elements based on use cases
- Used for 'minimum necessary' data exposure

Data De-identification and Anonymization

Anonymization Techniques

- Remove or substitute identifiable data
- Essential for meeting privacy regulations

Pseudonymization

- Replace sensitive data with index values
- Supports re-identification under controlled conditions

Tokenization

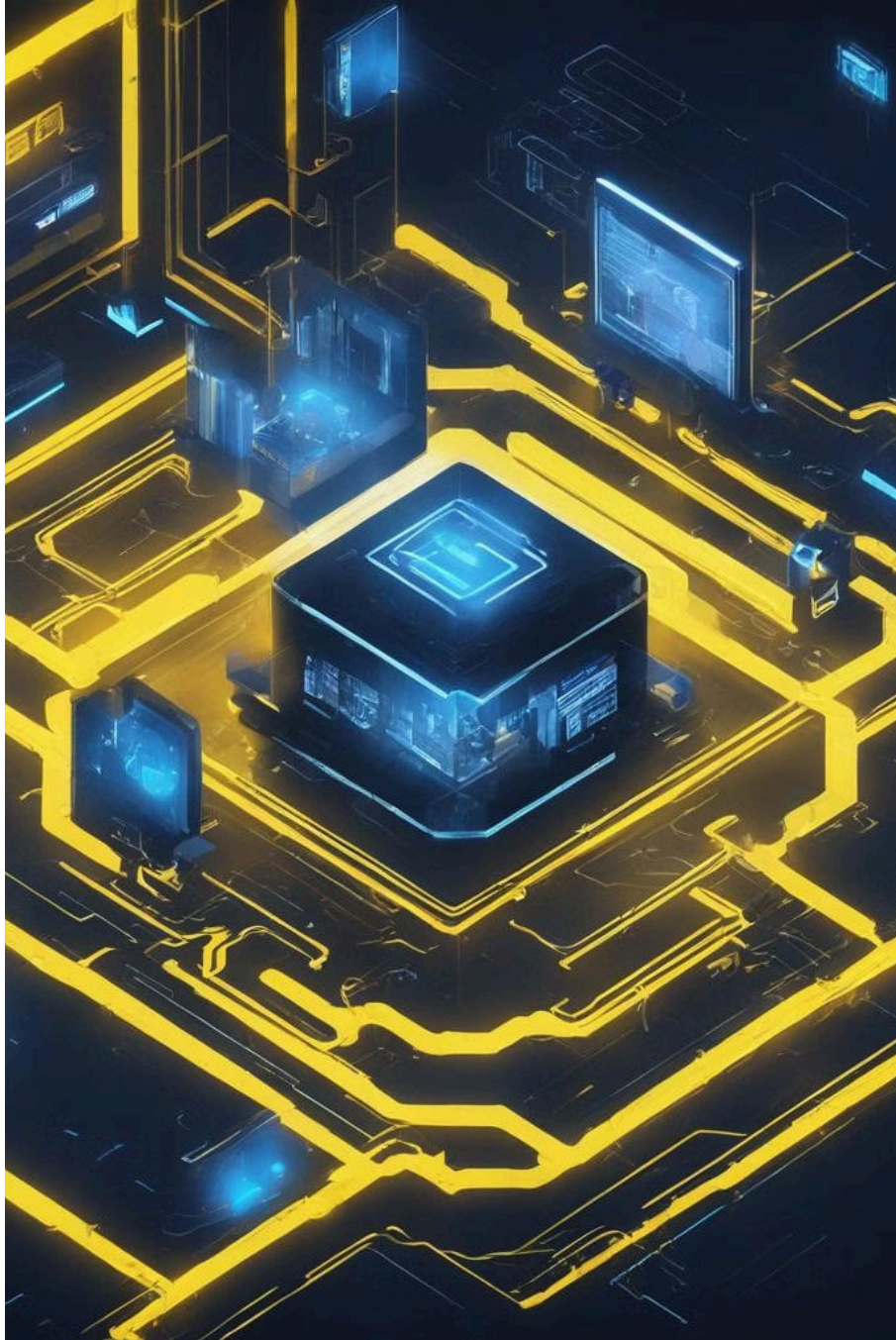
Implementing Tokenization

- Replaces sensitive data with tokens
- Essential for secure online transactions

Data Loss Prevention

Key Components of DLP

- Discovery, Monitoring, and Enforcement
- Crucial for protecting against data breaches



Keys and Secrets Management

Essential Practices

- Classify and protect access to cryptographic keys
- Log and monitor access to prevent misuse

Data Governance and Compliance

1 **Data Discovery Necessity**

- Identify sensitive data for protection strategies

2 **Data Retention, Deletion, Archiving**

- Balance between retention schedules and legal requirements
- Incorporate defensible data destruction practices

Audit Trails and Accountability

Ensuring Auditability

- Implement logging and monitoring for user actions
- Support nonrepudiation and legal investigations

Traceability of Data Events

- Accurately track data-related activities
- Enable investigation and response to security incidents

Information Security Buzz

Discover more at our InfoSec Knowledge Hub