COMPX527 Week 3 Lecture 1 & 2

Cloud Security Fundamentals

Overview

- Assignment 1
- What is different in Cloud?
- Cloud threat actors
- Top threats to Cloud Computing
- Strengthening Cloud Security
- Security Reference Model
- Shared Responsibility Model

What is different in cloud?

- Multi-Tenancy
- Loss of control of data
- Regulations and Compliance
- No transparency
- Virtualization Layer
- Everything is a service (XaaS)
- Shared responsibility for security

New Characteristics lead to New Attacks

Cloud Threat Actors

- Cloud provider staff
- Third-party providers
- Competitors
- Cyber Attackers
- Insiders
- Governments
- Cloud Brokers

Cloud Security Threats

- Data Breach
  - A data breach is the unauthorized exposure of sensitive and private data to a party that is not entitled to have it
  - It can be from two sources
    - Accidental exposure
    - Direct attack by someone
- Data Loss
  - occurs when the data that an organization relies on becomes lost, unavailable, or destroyed when it should not have been
  - Common reasons:
    - Lost of encryption keys
    - Accidental deletion
    - Corruption of data

Top Threats to Cloud Computing- Cloud Alliance Report

- Misconfiguration and Inadequate change control
- Identity and Access Management
- Insecure interfaces and APIs
- Inadequate selection/implementation of cloud security strategy
- Insecure third-party resources
- Insecure software development
- Accidental cloud disclosure
- System vulnerabilities
- Limited cloud visibility/observability
- Unauthenticated resource sharing
- Advanced Persistent Threats

https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

Top Threats to Cloud Computing

- Misconfiguration and Inadequate Change Control
  - Incorrect settings or sub-optimal setup of cloud computing resources
  - Not accounting for changes to the application as it develops
  - Can be caused by a lack of system knowledge or malicious activity
- Identity and Access Management (IAM)
  - The probability of a data or system breach increases dramatically for an environment where there are insufficient controls over the identity and credential systems used for access.

Top Threats to Cloud Computing

- Insecure Interface or APIs
  - Interfaces or APIs become insecure if they are not properly designed and managed, such that they can be used to circumvent the policies and controls
- Inadequate Cloud Security Strategy
  - Poor planning and critique of available cloud technologies
  - Be aware of risks and threats and choose appropriate cloud services and design to mitigate these risks
- Insecure Third-Party Resources
  - Third-party resources include those from cloud service providers, SaaS products, and open source code

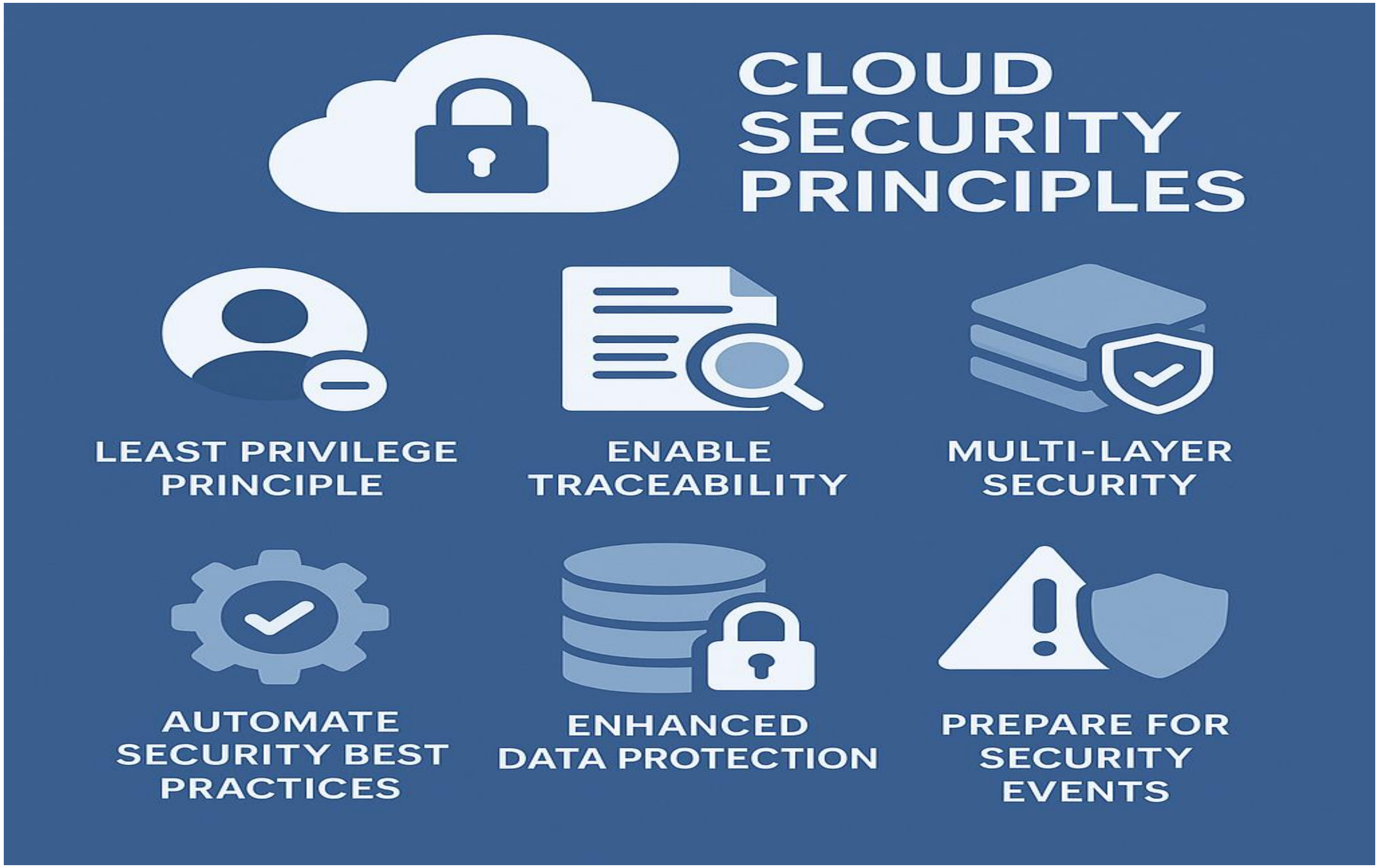
Top Threats to Cloud Computing

- Insecure Software Development
  - The complexity of software and cloud technologies can introduce vulnerabilities
- Accidental Cloud Data Disclosure
  - Insecure development, access management, and misconfigurations can cause data to become exposed
- System vulnerabilities
  - System vulnerabilities are vulnerabilities present in the underlying system or operating system that expose it to compromise and put all services on it at risk

Top Threats to Cloud Computing

- Limited Cloud visibility
  - Limited cloud visibility occurs when an organization cannot effectively visualize and analyze whether cloud service usage is safe or malicious
- Unauthenticated Resource Sharing
  - Cloud resources are left open to compromise without proper user authentication or following the principle of least privilege.
- APT
  - APT are those where attackers target systems with the intent of establishing themselves and stealing data over the long term
  - Commonly state-sponsored
  - Sophisticated design of attacks that can last months and even years

Strengthening Cloud Security


CLOUD SECURITY PRINCIPLES
LEAST PRIVILEGE PRINCIPLE
ENABLE TRACEABILITY
MULTI-LAYER SECURITY
AUTOMATE SECURITY BEST PRACTICES
ENHANCED DATA PROTECTION
PREPARE FOR SECURITY EVENTS

Strengthening Cloud Security

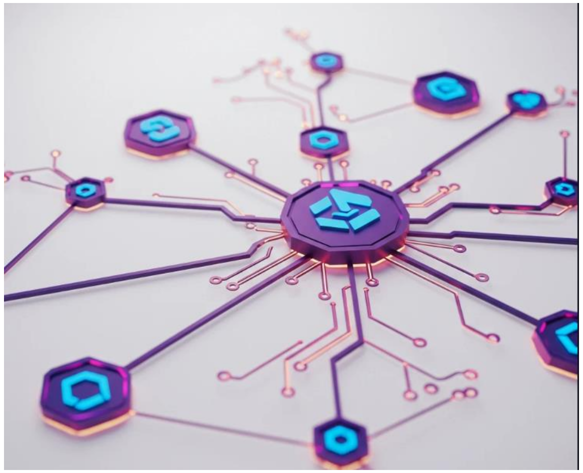
- Least privilege principle and enforcement
  - Apply separation of duties with appropriate authorization for each interaction with your AWS resources.
  - Start by denying access to everything and grant access as needed.

Strengthening Cloud Security

- Multi-layer security
  - Apply a defense-in-depth approach with other security controls.
- Automate security best practices.
  - Automated software-based security mechanisms improve the ability to securely scale more rapidly and cost-effectively.

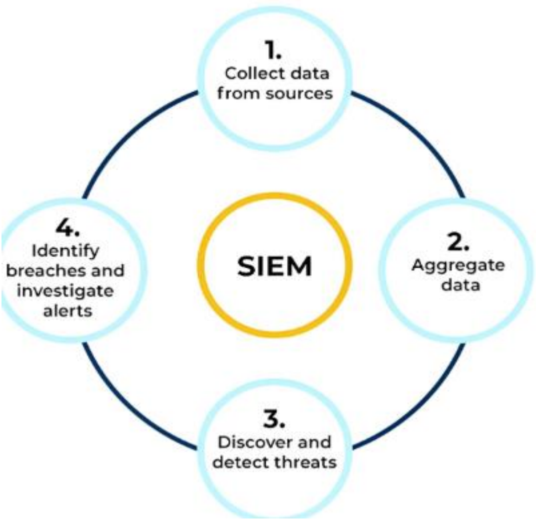
Strengthening Cloud Security

- Enable Traceability
  - Monitor, alert, and audit actions and changes to the environment in real time.
- Enhanced data protection
  - Classify your data into sensitivity levels and, where appropriate, use mechanisms like encryption and access control.



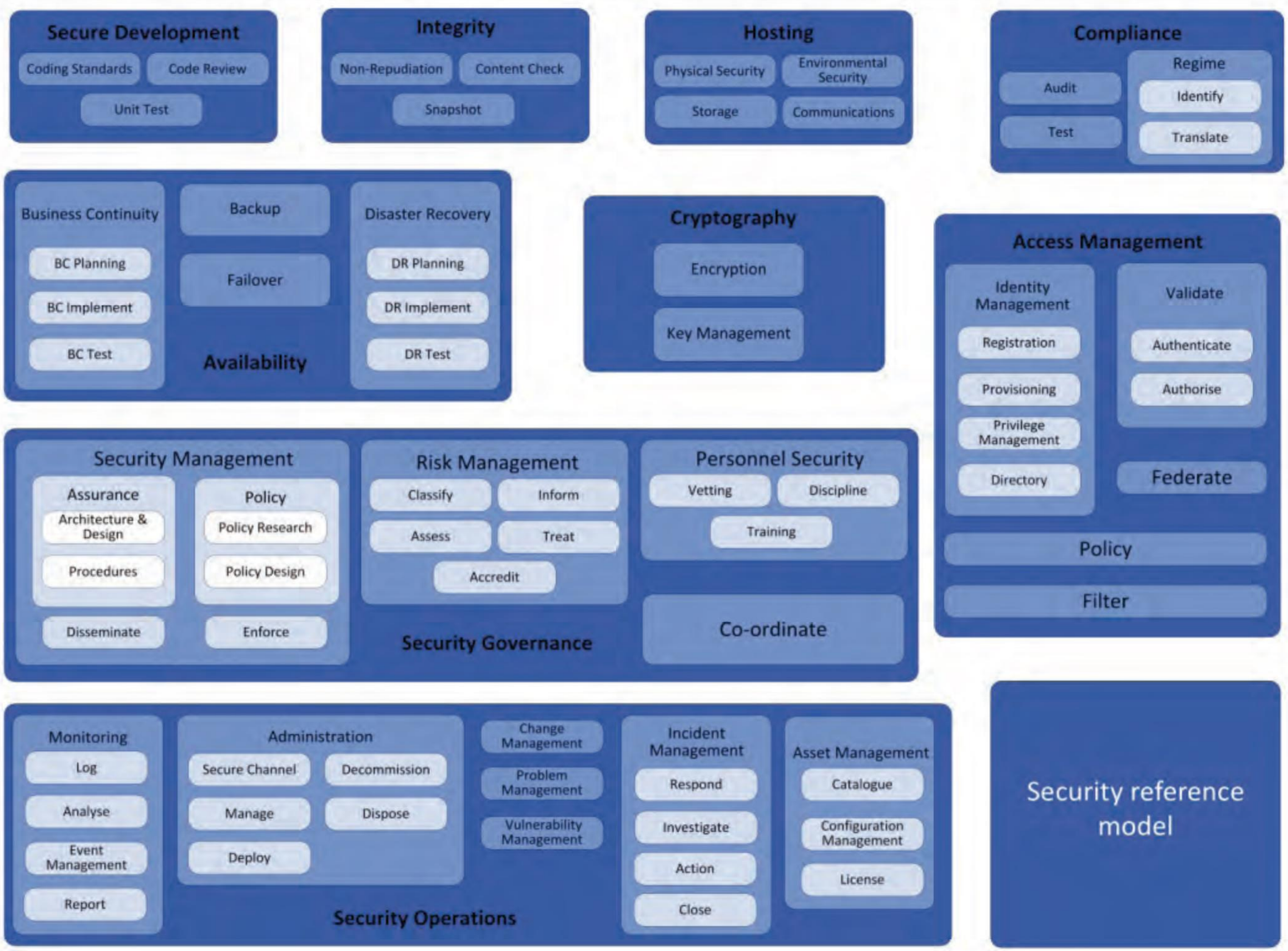
Strengthening Cloud Security

- Prepare for security events
  - Run incident response simulations and use tools with automation for early detection, investigation, and recovery.
  - For example: Security information and event management (SIEM)- responsible for continuously collecting and analyzing data


1. Collect data from sources
2. Aggregate data
3. Discover and detect threats
4. Identify breaches and investigate alerts
SIEM

https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/

Security Reference Model



Secure Development
Coding Standards
Code Review
Unit Test

Integrity
Non-Repudiation
Content Check
Snapshot

Hosting
Physical Security
Environmental Security
Storage
Communications

Compliance
Audit
Test
Regime
Identify
Translate

Availability
Business Continuity
BC Planning
BC Implement
BC Test
Backup
Failover
Disaster Recovery
DR Planning
DR Implement
DR Test

Cryptography
Encryption
Key Management

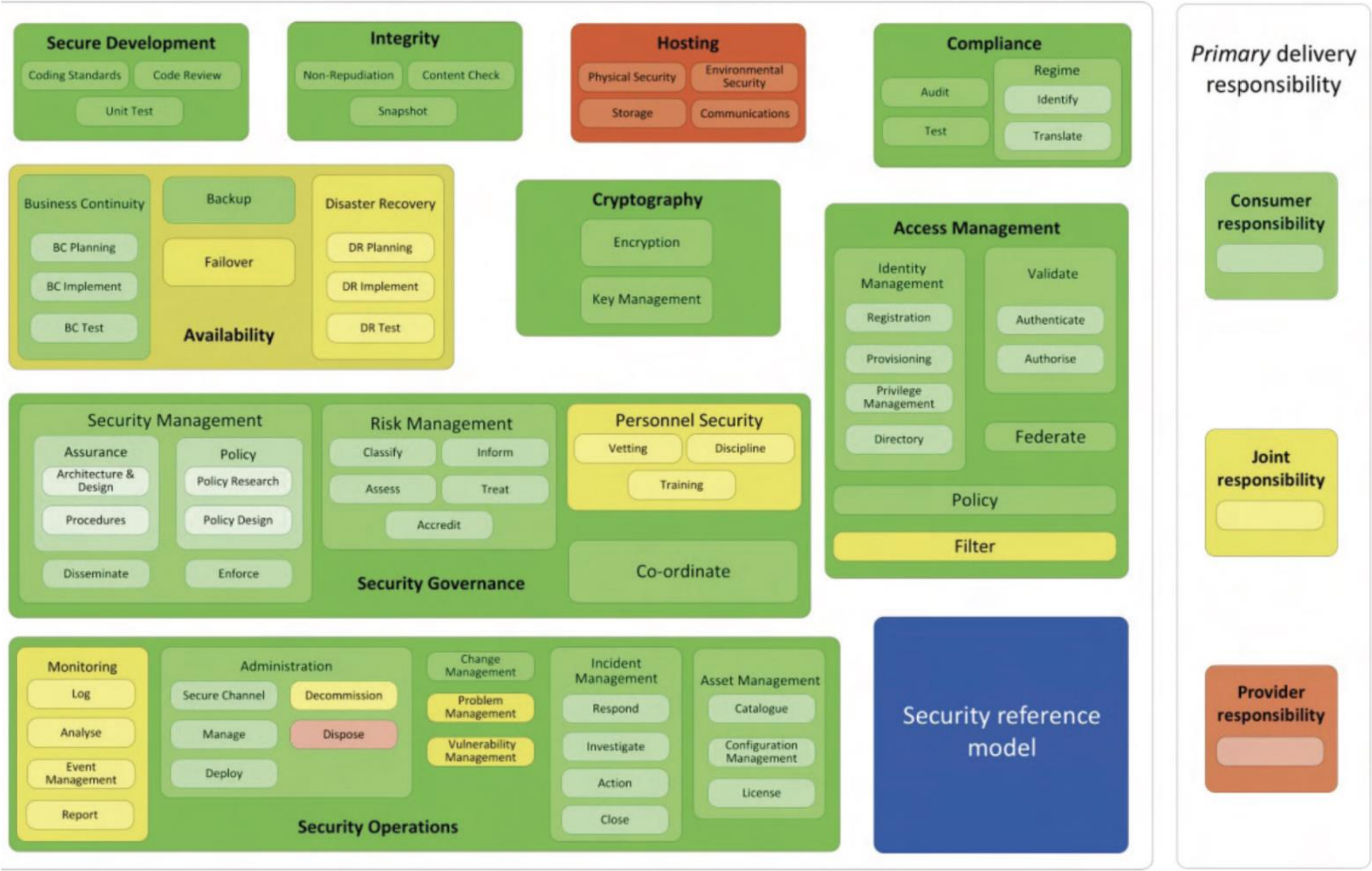
Access Management
Identity Management
Registration
Provisioning
Privilege Management
Directory
Validate
Authenticate
Authorise
Federate
Policy
Filter

Security Governance
Security Management
Assurance
Architecture & Design
Procedures
Disseminate
Policy
Policy Research
Policy Design
Enforce
Risk Management
Classify
Inform
Assess
Treat
Accredit
Personnel Security
Vetting
Discipline
Training
Co-ordinate

Security Operations
Monitoring
Log
Analyse
Event Management
Report
Administration
Secure Channel
Decommission
Manage
Dispose
Deploy
Change Management
Problem Management
Vulnerability Management
Incident Management
Respond
Investigate
Action
Close
Asset Management
Catalogue
Configuration Management
License

Security reference model

Shared Responsibility in IaaS



Secure Development
Coding Standards
Code Review
Unit Test

Integrity
Non-Repudiation
Content Check
Snapshot

Hosting
Physical Security
Environmental Security
Storage
Communications

Compliance
Audit
Test
Regime
Identify
Translate

Availability
Business Continuity
BC Planning
BC Implement
BC Test
Backup
Failover
Disaster Recovery
DR Planning
DR Implement
DR Test

Cryptography
Encryption
Key Management

Access Management
Identity Management
Registration
Provisioning
Privilege Management
Directory
Validate
Authenticate
Authorise
Federate
Policy
Filter

Security Governance
Security Management
Assurance
Architecture & Design
Procedures
Disseminate
Policy
Policy Research
Policy Design
Enforce
Risk Management
Classify
Inform
Assess
Treat
Accredit
Personnel Security
Vetting
Discipline
Training
Co-ordinate

Security Operations
Monitoring
Log
Analyse
Event Management
Report
Administration
Secure Channel
Decommission
Manage
Dispose
Deploy
Change Management
Problem Management
Vulnerability Management
Incident Management
Respond
Investigate
Action
Close
Asset Management
Catalogue
Configuration Management
License

Security reference model

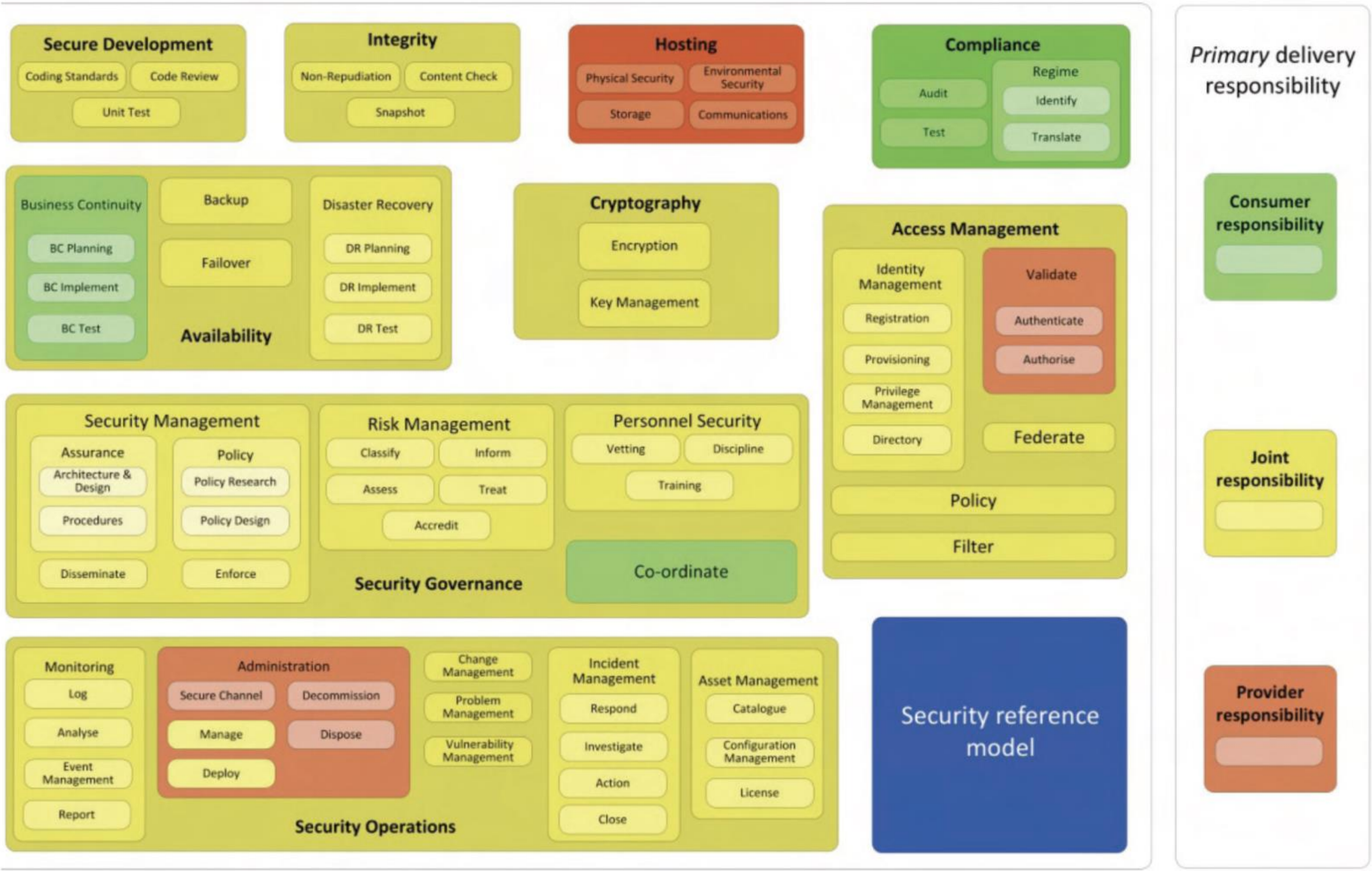
Primary delivery responsibility

Consumer responsibility

Joint responsibility

Provider responsibility

Shared Responsibility in PaaS



Secure Development: Coding Standards, Code Review, Unit Test

Integrity: Non-Repudiation, Content Check, Snapshot

Hosting: Physical Security, Environmental Security, Storage, Communications

Compliance: Audit, Test, Regime (Identify, Translate)

Availability: Business Continuity (BC Planning, BC Implement, BC Test), Backup, Failover, Disaster Recovery (DR Planning, DR Implement, DR Test)

Cryptography: Encryption, Key Management

Access Management: Identity Management (Registration, Provisioning, Privilege Management, Directory), Validate (Authenticate, Authorise), Federate, Policy, Filter

Security Governance: Security Management (Assurance (Architecture & Design, Procedures), Policy (Policy Research, Policy Design), Disseminate, Enforce), Risk Management (Classify, Inform, Assess, Treat, Accredit), Personnel Security (Vetting, Discipline, Training), Co-ordinate

Security Operations: Monitoring (Log, Analyse, Event Management, Report), Administration (Secure Channel, Decommission, Manage, Dispose, Deploy), Change Management, Problem Management, Vulnerability Management, Incident Management (Respond, Investigate, Action, Close), Asset Management (Catalogue, Configuration Management, License)

Security reference model

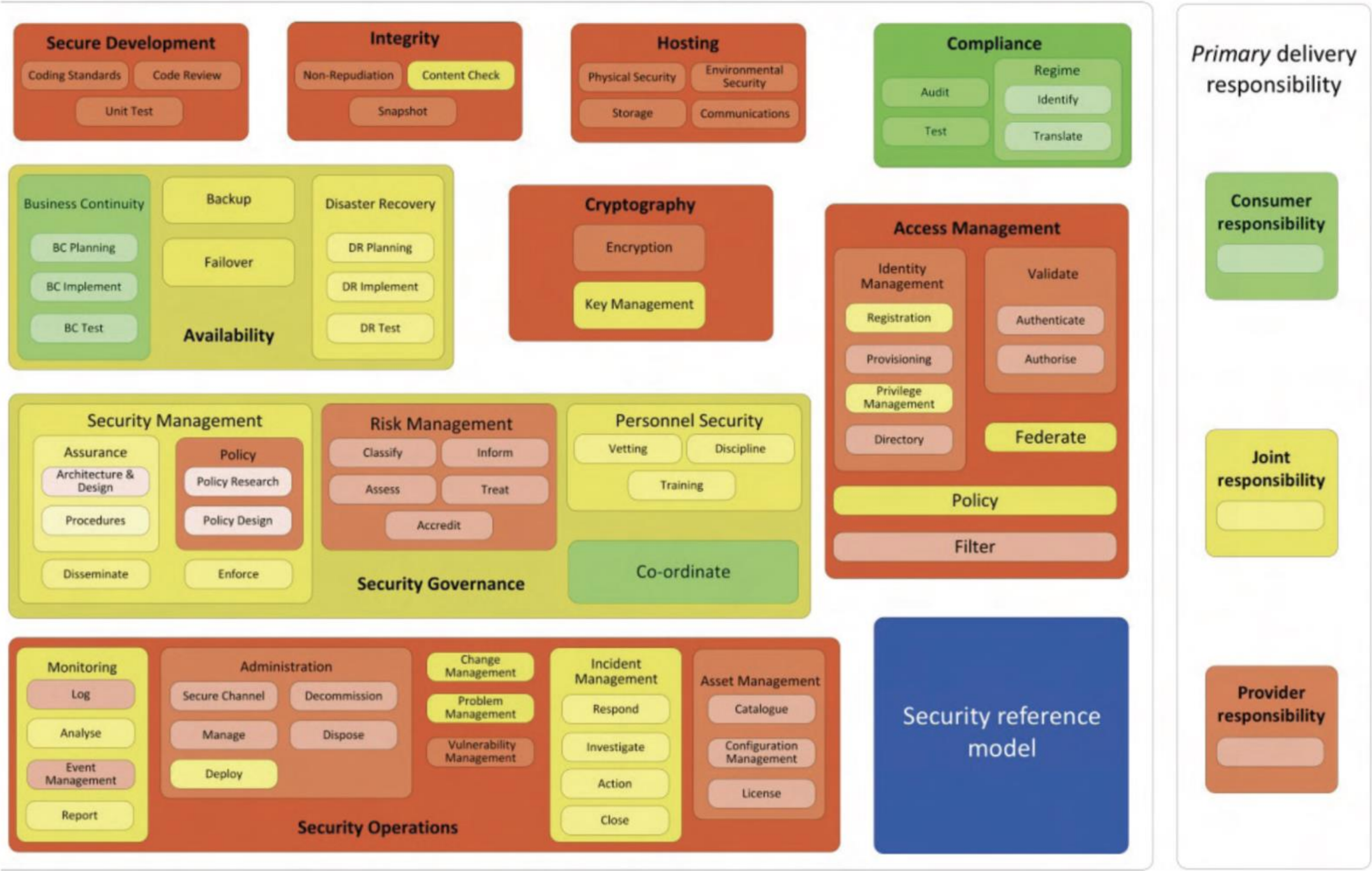
Primary delivery responsibility

Consumer responsibility

Joint responsibility

Provider responsibility

Shared Responsibility in SaaS



Secure Development: Coding Standards, Code Review, Unit Test

Integrity: Non-Repudiation, Content Check, Snapshot

Hosting: Physical Security, Environmental Security, Storage, Communications

Compliance: Audit, Test, Regime: Identify, Translate

Availability: Business Continuity: BC Planning, BC Implement, BC Test; Backup; Failover; Disaster Recovery: DR Planning, DR Implement, DR Test

Cryptography: Encryption, Key Management

Access Management: Identity Management: Registration, Provisioning, Privilege Management, Directory; Validate: Authenticate, Authorise; Federate; Policy; Filter

Security Governance: Security Management: Assurance: Architecture & Design, Procedures; Policy: Policy Research, Policy Design; Disseminate; Enforce; Risk Management: Classify, Inform, Assess, Treat, Accredit; Personnel Security: Vetting, Discipline, Training; Co-ordinate

Security Operations: Monitoring: Log, Analyse, Event Management, Report; Administration: Secure Channel, Decommission, Manage, Dispose, Deploy; Change Management; Problem Management; Vulnerability Management; Incident Management: Respond, Investigate, Action, Close; Asset Management: Catalogue, Configuration Management, License

Security reference model

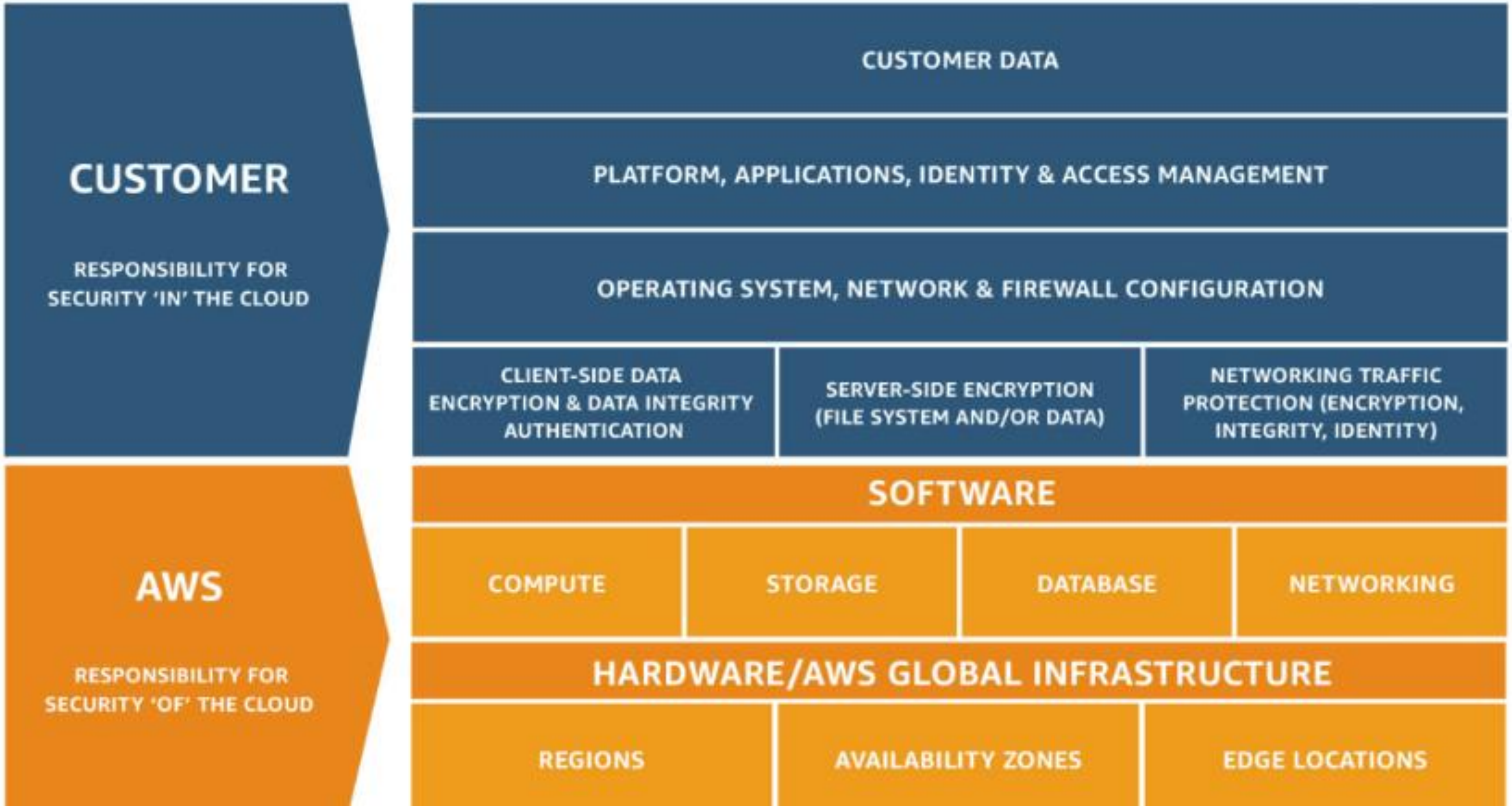
Primary delivery responsibility

Consumer responsibility

Joint responsibility

Provider responsibility

AWS Shared Responsibility Model



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/shared-responsibility-model.html

Q and A