ISC2 CCSP preparation notes

Certified Cloud Security Professional - 2020

Michiel Kalkman

Business Requirements Analysis

1. Inventory of Assets
   - Surveys, audits, interviews, automation, etc
2. Valuation of Assets
   - Do not put a $10 lock on a $5 bicycle
   - Data owner is the business manager in charge of the data
3. Determination of Criticality
   - Tangible assets - Cars in a Car Rental Agency
   - Intangible assets - Music copyright for a Label
   - Processes - Register failure in a fast food restaurant
   - Data paths - Logistical coordination, Cargo to Carriers
   - Personnel - Surgeon in a surgery
4. Identify Single Points of Failure (SPOF)

Criticality - SPOFs

SPOF - Single Point of Failure

- Not all SPOFs are part of critical assets
- Any chokepoint in a process, procedure or production chain
- Solutions
  - Add redundancies in case of failure
  - Create alternative processes in case of failure
  - Cross training personnel to handle multiple roles
  - Consistent and thorough data backup with quick restore
  - Load sharing/balancing for IT assets

Various

- Virtual sprawl / virtualization sprawl

Data Dispersion

- Data dispersion permits data to be replicated throughout a distributed storage infrastructure **through policy**
- Dispersion is **automated**
- Dispersion increased Availability
- **Chunking** : storing multidimensional data in multi-dimensional rectangular chunks to speed up slow accesses at the cost of slowing down fast accesses
- Programs that access chunked data can be oblivious to whether or how chunking is used.

Data Lifecycle Stages

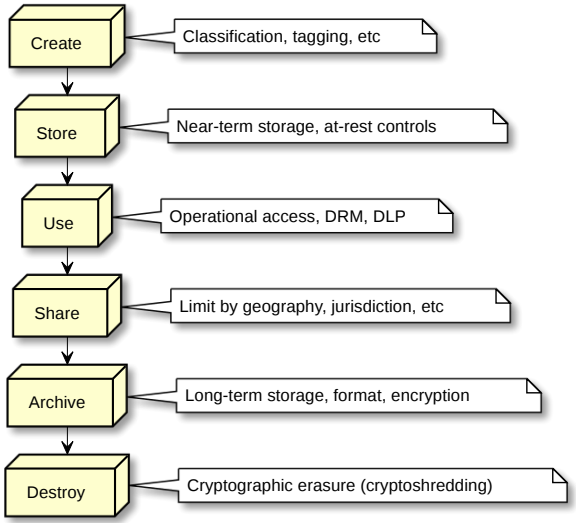

Figure 1: Data Lifecycle Stages

Data States

Data can exist in the following states, each of which requires different security controls.

Formal term	Meaning
In transit	On the wire, in flight
At rest	On disk, in storage
In use	In memory (RAM, CPU cache, etc)

Actors

Data subject	An individual who is the focus of personal data
Data owner	Holds the legal rights and complete control over a single piece of data elements. The data owner also can define distribution and associated policies
Data controller	A person who alone or jointly with others determines the purposes for which and the manner in which any personal data is processed
Data processor	Any person other than an employee of the data controller who processes the data on behalf of the data controller
Data steward	Responsible for data content, context, and business rules
Data custodian	Responsible for safe custody, transport, and storage of data, and implementation of business rules

- Custodian is responsible for technical controls (CIA, audit trails, etc)
- Steward is responsible for business controls (metadata, governance, compliance)

Various

- Data dispersal in the cloud

Data Center Site Infrastructure Tier Standard Topology

Feature	Tier I	Tier II	Tier III	Tier IV
Active components supporting load	N	N+1	N+1	2N or 2N + 1
Distribution paths	1	1	1 active, 1 alternate	2 active
Concurrently maintainable	—	—	Yes	Yes
Fault tolerant	—	—	—	Yes
Compartmentalization	—	—	—	Yes
Continuous cooling	—	—	—	Yes

- Tier I: Basic Data Center Site Infrastructure
- Tier II: Redundant Site Infrastructure Capacity Components
- Tier III: Concurrently Maintainable Site Infrastructure
- Tier IV: Fault-Tolerant Site Infrastructure

Datacenter considerations

- 12 hours of fuel for all four tiers
- Raised floor height at least 24 inch (= ~60.96 cm)

Environmental controls

	min	max
Temperature	18 °C/ 64.4 °F	27 °C / 80.6 °F
Humidity	40%	60%

Datacenter physical design

- Security redundancy is in layers, not repetition
- Driveways that wind and curve, include bollards
- Guest access through a controlled access point
- Placement of hazardous or vital components away from personnel or vehicles
- Interior physical access controls (badging, keys, turnstiles, etc)
- Specific physical protections for sensitive assets (safes, etc)
- Inventory tracking mechanisms (RFID etc)
- Fire detection and suppression systems
- Sufficient power for all functions in the event of power disruption

Threat modeling - STRIDE

Promoted and further developed by Microsoft. Describes threats by attributes.

- **Spoofing** - Impersonation (e.g. IP or user)
- **Tampering** - With data inputs, outputs or stored
- **Repudiation** - Inability to deny action compromised
- **Information Disclosure** - Data leakage or breach
- **Denial of Service** - Loss of Availability
- **Elevation of Privilege** - Raise user privilege above authorized level

Testing

- **SAST** - Static Application Security Testing
  - White-box test, source available, no execution
  - Example, null pointer dereference, quality issues
- **DAST** - Dynamic Application Security Testing
  - Black-box test, examination at runtime
  - Example, environment configuration, protocol parsing issues

ISO 27034-1 Standards for Secure App Development

ONF (Organization Normative Framework) is essentially organizational or Company guidelines/matrix/repository on securing applications controls and process.

ANF (Application Normative Framework) is a subset or mapping of the ONF that contains the information specific to an application.

ONF has many ANFs, each ANF only one ONF

SDLC Phases

	SDLC (CCSP)	NIST SP 800-64	NIST SP 800-160
1.	**Defining**	Initiation	Concept
2.	**Designing**	Development	Development
3.	**Developing**	Implementation	Production
4.	**Testing**	Operation	Utilization
5.	**Secure Operations**		Support
6.	**Disposal**	Disposal	Retirement

- Material refers to *NIST SP 800-64*, this has been superceded by *NIST SP 800-160 Systems Security Engineering*

OWASP Top-10

	2013	2017
1	Injection	Injection
2	Broken Authentication and Session Mgmt	Broken Authentication
3	Cross-Site Scripting (XSS)	Sensitive Data Exposure
4	Insecure direct object references	XML External Entities
5	Security Misconfiguration	Broken Access Control
6	Sensitive Data Exposure	Security Misconfiguration
7	Missing function-level Access Control	Cross-Site Scripting
8	Cross-Site Request Forgery (XSRF)	Insecure Deserialization
9	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities
10	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring

Multi-tenancy / Resource Sharing

- **Reservations** - guaranteed minimum resources for tenants
- **Limits** - guaranteed maximum resources for tenants
- **Shares** - prioritized distribution of remainder resources after Reservations, up to Limits

Time / Frequency Concepts

MAD	Maximum Allowable Downtime	Cannot be down longer than this
MTD	Maximum Tolerable Downtime	Equivalent to **MAD**
RTO	Recovery Time Objective	We want to be back up this soon
MTTR	Mean Time To Recovery	Average recovery length
RPO	Recovery Point Objective	We can afford to lose this much.
MTBF	Mean Time Between Failures	Average failure rate
RSL	Recovery Service Level	Service level during recovery

Maintenance Mode

Maintenance Mode is used when changes (updates, configuration) are made to the Operating System in Root/Ring-0 (Hypervisor).

- **Disable alerts**
- **Continue logging**
- Customer access (starting new VMs) is blocked
- Live-migrate running VMs to other hosts
- Administrator access only, possibly restricted to physical console
- Follow vendor guidance and best practices

ISO 22237 Protection and Availability Classes

- Protection Class 1: Public or semi-public area.
- Protection Class 2: Accessible to all authorized personnel, employees and visitors.
- Protection Class 3: Restricted to specified employees and visitors, those with access to Class 2 only must be accompanied by Class 3 personnel.
- Protection Class 4: Even stricter, need to demonstrate need for access.

Disaster Recovery / Business Continuity

- *Business Continuity* efforts - maintaining critical operations during an interruption in service
- *Disaster Recovery* efforts - resuming operations after an interruption due to disaster
- An *event* is an unscheduled adverse impact to operations. An *event* is distinguished from a *disaster* by its duration
- BIA lists assets (criticality, value, etc), input for BC/DR

BCDR Plan

- A list of items from the Asset Inventory deemed critical
- The circumstances under which an Event or Disaster is declared
- Who is authorised to make the declaration
- Essential point of Contact
- Detailed Actions, Taskss and Activities

BCDR Plan - Notes

- Authorized party also declares cessation of BCDR activities
- This should only be done once there is a high degree of confidence that all safety and health hazards are cleared, operations is back to normal
- Doing this too soon can exacerbate the disaster or create a new one

BCDR Testing

- Tabletop testing, no impact
- Dry run, minor impact
- Full test, major impact

Change Management (CM)

- CM starts with baselining
- Security controls included in the basesline
- Baseline should suit largest number of systems in the organization
- Can have multiple baselines if required
- Continually test baselines to detect deviations
- An adversarial, unresponsive exception process will undermine security

CM process

- CM process is part of an organisation's governance

CSA - STAR

- Security
- Privacy

OECD - Organization for Economic Cooperation and Development

Privacy and Security Guidelines

Aims to globally protect privacy through a practical, risk-management-based approach. Should follow these principles:

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness

GDPR - National laws compliant with EU GDPR

European Free Trade Area (EFTA)

- Switzerland
- Lichtenstein
- Norway
- Iceland

Rest of the world

- Argentina
- Australia — Privacy Act 1988, since 2014 Australian Privacy Principles
- New Zealand
- Japan
- Canada — PIPEDA
- Androrra
- Israel
- Uruguay

GDPR - General Data Protection Regulation

Updated 95/46/EU Privacy Directive to include:

- Consent
- Transfers abroad
- The right to be forgotten
- Access requests
- Home state regulation
- Increased sanctions
- Establishing the role of the **data protection officer**

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Gramm–Leach–Bliley Act (GLBA)

- Financial Services Modernization Act of 1999
- It repealed part of the Glass–Steagall Act of 1933, removing barriers in the market among banking companies, securities companies and insurance companies that prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an insurance company.

Sarbanes–Oxley Act (Sarbox, SOX)

AKA,

- Public Company Accounting Reform and Investor Protection Act
- Corporate and Auditing Accountability, Responsibility, and Transparency Act

Drove development by American Institute of Certified Public Accountants (AICPA) of,

- SSAE 16 and SOC audit reports
- In technology SaaS companies, the SOC 2 audit is purchased to provide an assurance on various aspects of the software including security, availability, and processing integrity

Preparing for legal actions

- **Legal hold** When a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and ensure the preservation of relevant documents.
- **E-Discovery** Any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence.
- **Spoliation** The intentional or accidental destruction or alteration of data either on "legal hold" or lawfully requested.
- **Production** Presenting the requested data to the court or requesting party.

e-Discovery Stages

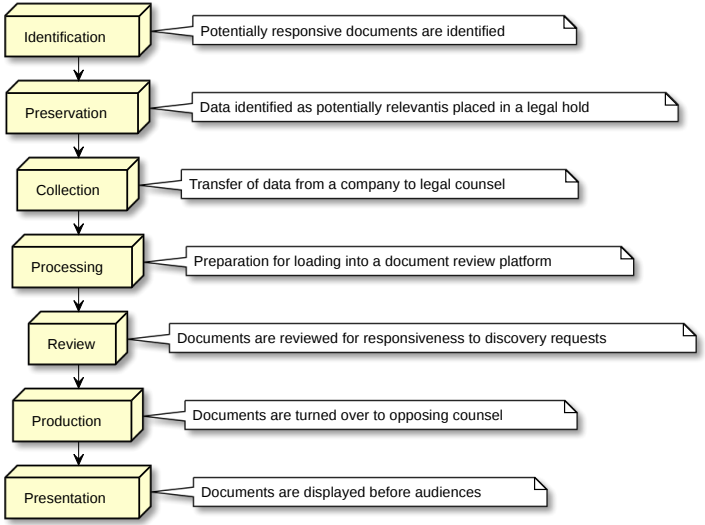

Figure 2: Stages

Investigation types (USA)

- **Operational** in-house
- **Civil** two parties settle a disagreement in court, just needs over 50% proof ("preponderance of evidence")
- **Criminal** jury or judge must find "beyond a reasonable doubt"

Police are constrained by the Fourth Amendment, private citizens are not (unless working as agents of the government). Part of the Bill of Rights. It prohibits unreasonable searches and seizures. In addition, it sets requirements for issuing warrants: warrants must be issued by a judge or magistrate, justified by probable cause, supported by oath or affirmation, and must particularly describe the place to be searched and the persons or things to be seized

Shared responsibility model

Concern	**IaaS**	**PaaS**	**SaaS**
Governance, Risk, Compliance	Customer	Customer	Customer
Data Security	Customer	Customer	Customer
Application Security	Customer	Customer	*Shared*
Platform Security	Customer	*Shared*	Provider
Infrastructure Security	*Shared*	Provider	Provider
Physical Security	Provider	Provider	Provider

Data Rights Management (DRM)

Mechanisms

- Rudimentary Reference Check
- Online Reference Check
- Local Agent Check
- Presence of Licensed Media
- Support-Based Licensing

Provides

- Persistent Protection
- Dynamic Policy Control
- Automatic Expiration
- Continuous Auditing
- Replication Restrictions
- Remote Rights Revocation
- Might provide more

Federated Identity Management

Technologies used for federated identity include,

- SAML (Security Assertion Markup Language)
- OAuth - Authorization
- OpenID - Authentication
- Security Tokens
  - Simple Web Tokens
  - JSON Web Tokens
  - SAML assertions
- Web Service Specifications
- Windows Identity Foundation
- XACML - Authorization

Various

- SAML — the most commonly used federation. XML-based framework to communicate user authentication, authorization, and attributes. Authentication tokens are digitally signed XML, moved over TLS.
- WS-Federation, federation within the broader WS-Security or WS-* framework.
- OpenID Connect — based on OAuth, lower security.
- OAuth — widely used for web and mobile access. Users can grant websites or applications access to their information on websites, without giving them the passwords.
- Also included in the exam question pool but with less emphasis:
  - Shibboleth — heavily used in education settings, based on SAML, open & free
  - XACML — eXtensible Access Control Markup Language. It's an Attribute-Based Access Control system. Attributes associated with a user or action or resource are inputs to the access-control decision.

OpenID

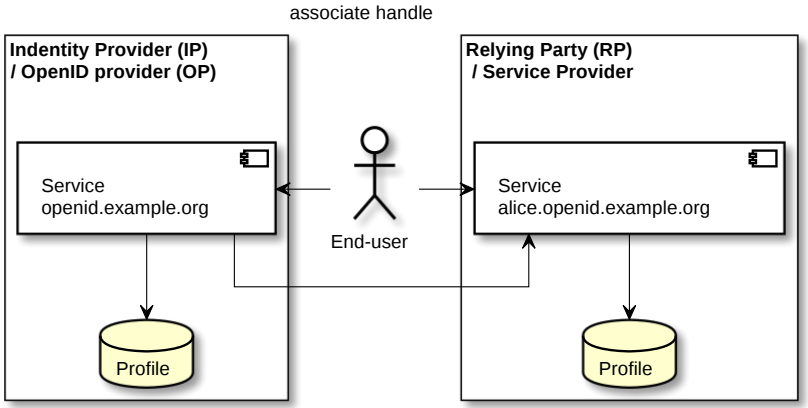

Figure 3: OpenID

PCI-DSS

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council (PCI-SSC).

The standard was created to increase controls around cardholder data to reduce credit card fraud.

Validation of compliance is performed **annually or quarterly**, either by an external Qualified Security Assessor (QSA) or by a firm-specific Internal Security Assessor (ISA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

PCI-DSS Control objectives

1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

PCI-DSS Process

Each requirement/sub-requirement is additionally elaborated into three sections.

- **Requirement Declaration**
- **Testing Processes**
- **Guidance**

PCI-DSS Requirements

1. Installing and maintaining a firewall configuration to protect cardholder data
2. Changing vendor-supplied defaults for system passwords and other security parameters
3. Protecting stored cardholder data
4. Encrypting transmission of cardholder data over open, public networks
5. Protecting all systems against malware and performing regular updates of anti-virus software
6. Developing and maintaining secure systems and applications
7. Restricting access to cardholder data to only authorized personnel
8. Identifying and authenticating access to system components
9. Restricting physical access to cardholder data
10. Tracking and monitoring all access to cardholder data and network resources
11. Testing security systems and processes regularly
12. Maintaining an information security policy for all personnel

PCI-DSS Compliance levels

- Level 1 – Over 6 million transactions annually
- Level 2 – Between 1 and 6 million transactions annually
- Level 3 – Between 20,000 and 1 million transactions annually
- Level 4 – Less than 20,000 transactions annually

Each card issuer maintains their own table of compliance levels.

Tokenization

Format-preserving tokens

Format-preserving tokens maintain the look and feel of the original payment card data. For example:

- Payment Card Number: `4222 2221 2221 2221`
- Format Preserving Token: `4222 8765 2345 2221`

Non-format-preserving tokens

Non-format preserving tokens don't resemble the original data and could include both alpha and numeric characters. For example:

- Payment Card Number: `4222 2221 2221 2221`
- Non-format Preserving Token: `25c92e13-80f6-415f-9d65-3395a32u0223`

System and Organization Controls (SOC)

History

1. Statements on Auditing Standards - **SAS 70**
2. Statements on Standards for Attestation Engagements 2011-2017 - **SAE 16**
3. Statements on Standards for Attestation Engagements 2017-now - **SAE 18**

SOC Overview

Three reports, created by AICPA (American Institute of Certified Public Accountants).

	What it reports on	Who uses it
SOC 1	Internal controls over financial reporting	User auditor and user controller's office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Shared under NDA by management, regulators, etc
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Shared publicly

The SOC 1 and SOC 2 reports come in two forms: Type I and Type II.

- Type I reports evaluating whether proper controls are in place at a specific point in time.
- Type II reports are done over a period of time to verify operational efficiency and effectiveness of the controls.

SOC notes

- SOC 1 covers financial controls
- SOC 1 and SOC 2 have Type 1 and Type 2 (1 = point in time, 2 = periodic)
- SOC 2 details should be usable by IT staff, regulators, and business partners
- SOC 2 covers any of the Five **Trust Services**,
  - Security (mostly access control)
  - Availability
  - Processing Integrity (complete, accurate, timely, authorized)
  - Confidentiality
  - Privacy
- SOC 3 is a public summary (pass/fail) of SOC 2

Standards and Regulations

Main ISO standards

- 27001 — Defines ISMS
- 27002 — Defines **controls and best practices** for ISMS
- 27005 — Information security risk management
- 27034 — Application security
  - ONF or Organizational Normative Framework
  - ANF or Application Normative Framework
- 28000 — Supply chain (and other 2800*)
- 31000 — Risk management framework

FIPS 140-2

NIST issued the FIPS 140 series to coordinate the requirements and standards for cryptography modules that include **both hardware and software components**.

Level	Description
Level 1	No physical requirements
Level 2	Tamper-evident
Level 3	Tamper-resistant
Level 4	Tamper-responsive

FIPS 140-2 is a requirements document that sets the minimum strength level for data encryption used in **Sensitive But Unclassified (SBU)** USA/Federal operating environments.

Common Criteria

Assurance levels

EAL1	Functional	Tested
EAL2	Structural	Tested
EAL3	Methodical	Tested and Checked
EAL4	Methodical	Designed, Tested and Reviewed
EAL5	Semiformal	Designed and Tested
EAL6	Semiformal	Verified Design and Tested
EAL7	Formal	Verified Design and Tested

IAM - Identity

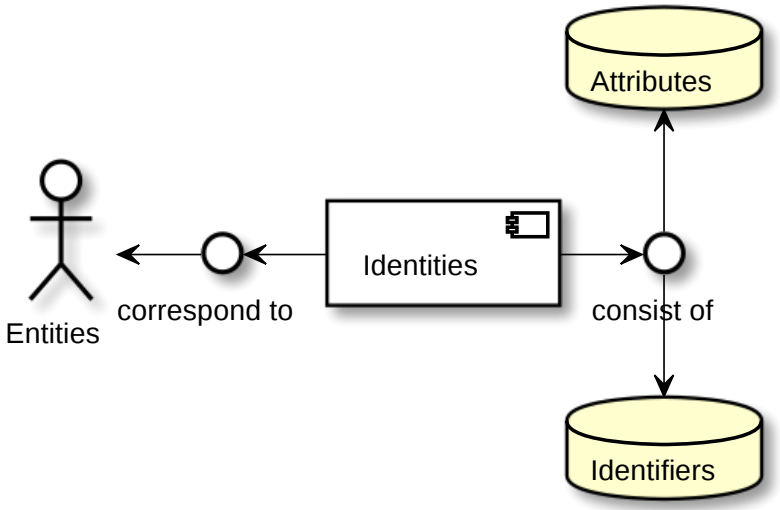

Figure 4: Identity

IAM - Components

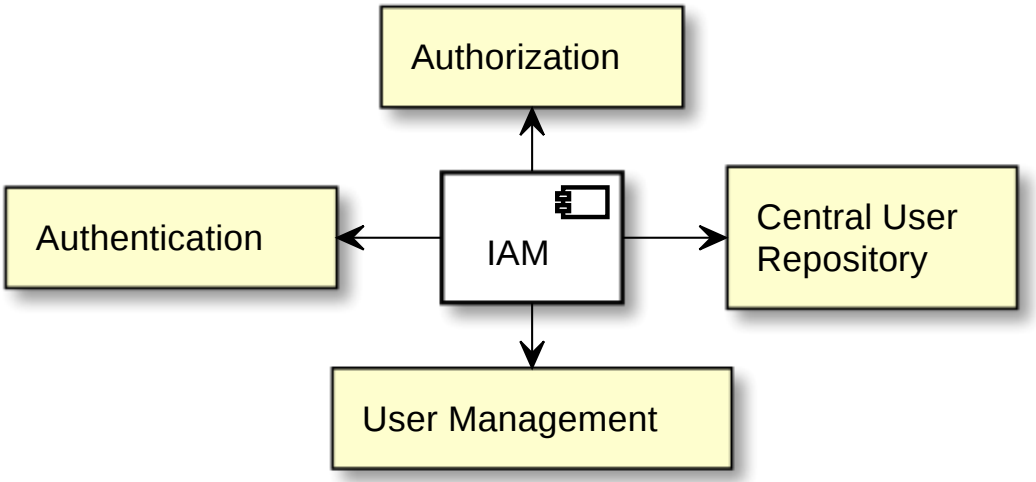

Figure 5: Components

IAM - Functionality

1. Identity Management
   - Provisioning is the first phase
2. Access Management
   - Authentication
   - Authorization
   - Policy Management
   - Federation
     - Built on SAML
     - WS-Federation
     - OAuth
     - OpenID Connect
   - Identity Repositories
     - X.500, LDAP, AD, Metadata replication

SIM, SEM, SIEM

- **SIM** Security information management: *Long-term storage* as well as analysis and reporting of log data.
- **SEM** Security event manager : *Real-time monitoring, correlation* of events, notifications and console views.
- **SIEM** Security information and event management : *Combines SIM and SEM* and provides real-time analysis of security alerts generated by network hardware and applications.

Privacy Shield

- The EU–US Privacy Shield is a framework for regulating **exchanges of personal data for commercial purposes** between the EU and the US
- One of its purposes is to enable US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect EU citizens
- The EU–US Privacy Shield is a replacement for the International Safe Harbor Privacy Principles (declared invalid 2015)
- On the US side Privacy Shield is enforced by the **FTC**

Non-EU companies can also use a contractual relationship for processing personal data from the EU.

Virtualization

- Hypervisor Type-1 : Bare metal (Hardware / Ring 0)
- Hypervisor Type-2 : Paravirtualizard (Software / Ring 2)

Review

Levels

	Levels	One is	High is
CSA STAR	3	LOW	Continuous, automated 3rd party monitoring
ISO 22237	4	LOW	Demonstrate need for access
PCI-DSS	4	HIGH	6M+ transactions/year
FIPS 140-2	4	LOW	Tamper-responsive
Common Criteria	7	LOW	Formal - Verified Design, Tested
Uptime Institute	4	LOW	Fault-tolerant site infrastructure

Cloud Security Operations

- Understand how redundancy is implemented in the design of cloud datacenters
- Know the four tiers of datacenter redundancy published by the Uptime Institute
- Training and awareness - know which element best support training efforts
- Understand the different between DAST and SAST