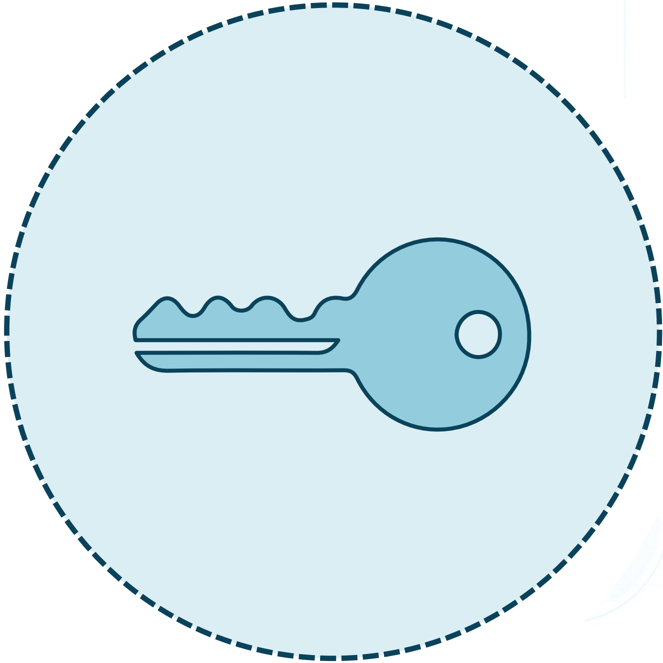
The CIA Security Triad



- Confidentiality
- Integrity
- Availability

Confidentiality

- Protect sensitive data from unauthorized parties
- Encryption
  - Data in transit
  - Data at rest
- Plaintext + encryption key = ciphertext

Integrity

- Can we trust the data?
- Has it been tampered with or corrupted?
- Hashing
  - Feed data into a 1-way hashing algorithm
  - A unique hash value results
  - Future comparisons should match if nothing has changed

Availability

- Can we get to the system/data?
- Redundancy
  - Facility
  - Network connections
  - Power
  - Computing devices
  - Disk storage

Personally Identifiable Information (PII)

- Anything that can uniquely identify an individual
  - One more pieces of information
- Data privacy
  - Collection
  - Transmission
  - Storage
  - Sharing
  - Usage

Personally Identifiable Information (PII)

- Web browser cookie (depends on contents)
- Personal home or e-mail address
- Credit card number
- IP address
- GPS data for user location

PII Audit Assurance Review

- PII policy review
- Evaluate PII-related control efficacy
- Report on deficient PII controls

Protected Health Information (PHI)

- Similar to PII but focused on the medical industry
- Past and current health information
- Future health details related to
  - Care
  - Payment

Protected Health Information (PHI)

Name	Social security number	Medical records
Blood type	Phone number	E-mail address
Account numbers	IP address	Lab test results

Protected Health Information (PHI)

- PHI or not?
  - Medical tracking devices worn on patients
  - Information used by healthcare provider?
    - If yes, then it is PHI
  - As long as information cannot be traced to an individual, it is not PHI

General Data Protection Regulation (GDPR)

- Legislative act of the European Union (EU)
- Puts control of personal data into the user’s hands
- Data privacy of PII
  - Collection and retention
  - Use
  - Sharing

General Data Protection Regulation (GDPR)

Rules - organizations

- Within the EU that process personal data
- Outside of the EU processing EU citizen data

Rights - individuals

- Clear communication to people about personal data collection and use
- Correction of inaccurate personal data
- Access to personal data

General Data Protection Regulation (GDPR)

IS auditing and GDPR compliance

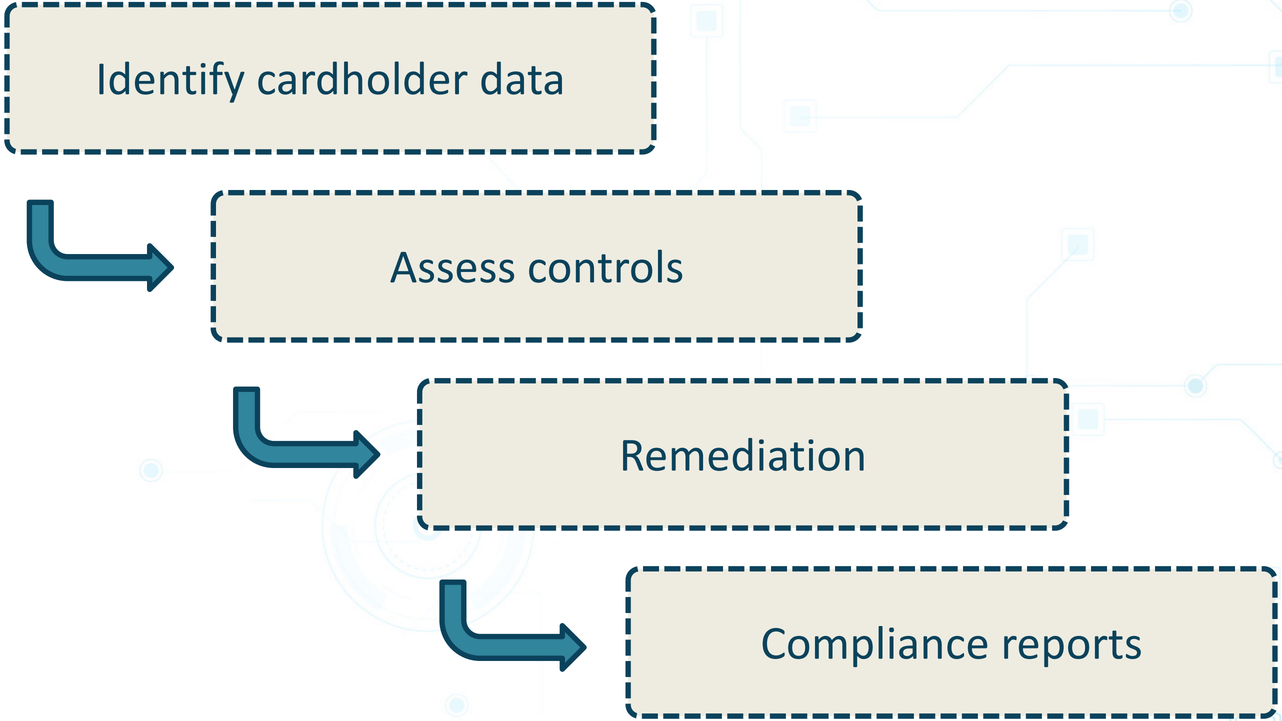
Data processing practices

Efficacy of GDPR-related controls

Payment Card Industry Data Security Standard (PCI DSS)

- International
- Merchant protection of cardholder data
- Strives to harden payment card-processing environments
- Each card type has its own specific compliance details
    - Visa, MasterCard, and American Express

Payment Card Industry Data Security Standard (PCI DSS)



Identify cardholder data

Assess controls

Remediation

Compliance reports

Payment Card Industry Data Security Standard (PCI DSS)

Goal	Control
Build and maintain a secure network	- Firewalls - Change system defaults

Payment Card Industry Data Security Standard (PCI DSS)

Goal	Control
Build and maintain a secure network	• Firewalls • Change system defaults
Protect cardholder data	• Storage data protection • Network encryption over open, public networks

Payment Card Industry Data Security Standard (PCI DSS)

Goal	Control
Build and maintain a secure network	• Firewalls • Change system defaults
Protect cardholder data	• Storage data protection • Network encryption over open, public networks
Maintain a vulnerability management program	• Anti-virus solution including updates • Apply security to all SDLC phases

Payment Card Industry Data Security Standard (PCI DSS)

Goal	Control
Build and maintain a secure network	• Firewalls • Change system defaults
Protect cardholder data	• Storage data protection • Network encryption over open, public networks
Maintain a vulnerability management program	• Anti-virus solution including updates • Apply security to all SDLC phases
Implement strong access control	• "Need to know basis" access to cardholder data • Unique user accounts • Physical security controls

Payment Card Industry Data Security Standard (PCI DSS)

Goal	Control
Regularly monitor and test networks	• Network, host, and app monitoring • Periodic security testing

Payment Card Industry Data Security Standard (PCI DSS)

Goal	Control
Regularly monitor and test networks	• Network, host, and app monitoring • Periodic security testing
Maintain an information security policy	• Organizational security policies

Payment Card Industry Data Security Standard (PCI DSS)

Compliance

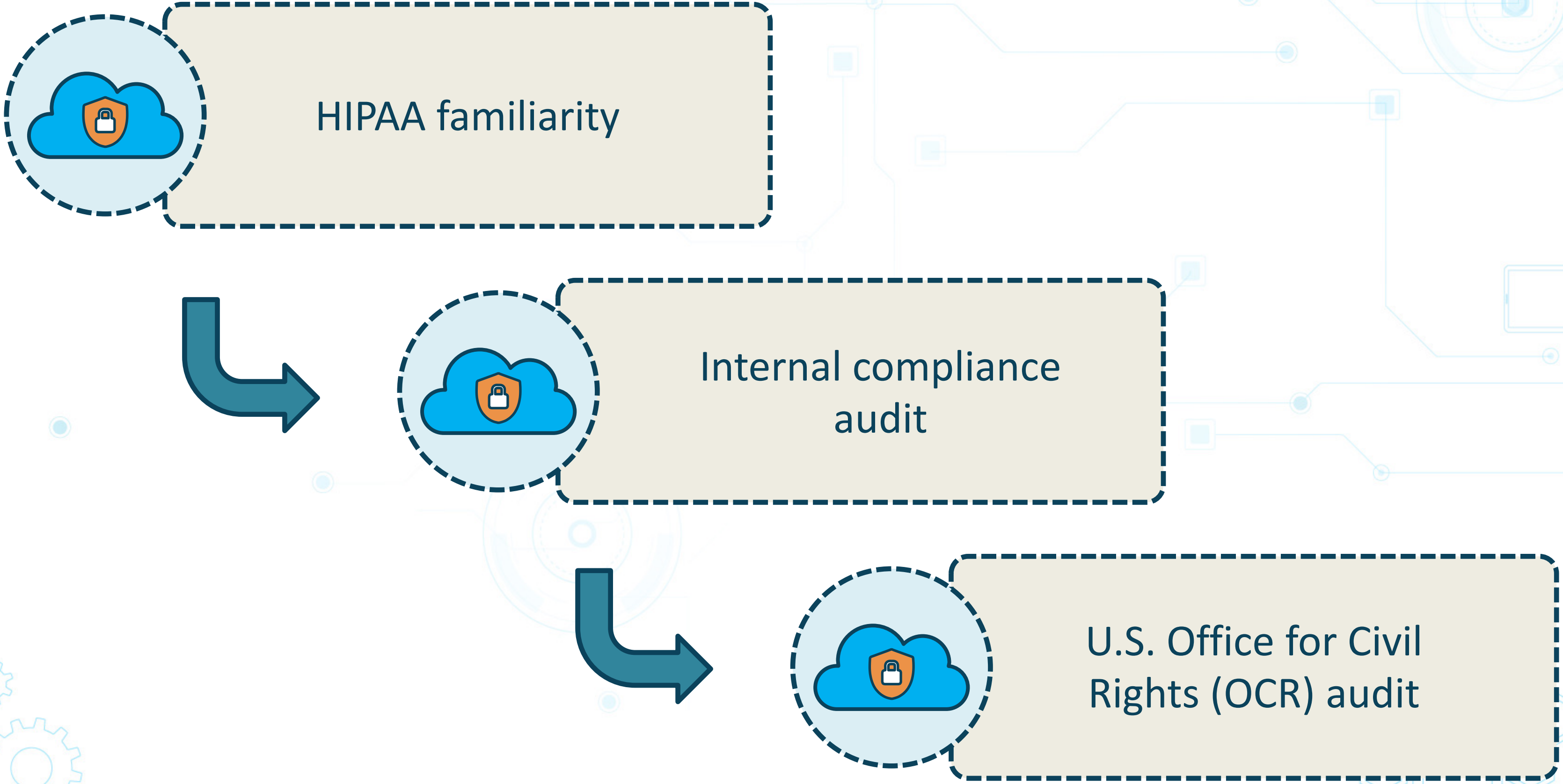
Self-assessment questionnaire

Report on Compliance (RoC)

Health Insurance Portability and Accountability Act (HIPAA)

- Limited disclosure of protected health information (PHI) in the United States
- Applies to HIPAA-related entities
  - Health care providers
  - Health plans

HIPAA Compliance



HIPAA familiarity

Internal compliance audit

U.S. Office for Civil Rights (OCR) audit

Health Insurance Portability and Accountability Act (HIPAA)

- User authentication
- Device authentication
- Encryption and data integrity
- Monitor for breaches

Federal Risk and Authorization Management Program (FedRAMP)

Cloud computing security standards

U.S. Govt federal agencies cloud usage

Federal Risk and Authorization Management Program (FedRAMP)

- Security control responsibility
  - Cloud service provider
  - Specific government agency
- Data location
  - Does not have to reside in the United States
- FedRAMP certified infrastructure
  - Layered IT services are *not* automatically certified

FedRAMP Requirements

- FIPS 140-2 cryptographic modules must be used
  - Encryption (AES 256)
  - Hashing and digital signatures (SHA 256)
  - Authentication

FedRAMP Requirements

- Transport Layer Security (TLS) v1.1 or higher
- Unique user accounts
- Principle of least privilege
- Malware updates, monitoring, and alerting

FedRAMP Certified Cloud Providers

- Microsoft Azure
- Amazon Web Services
- Google Cloud

Assets and Risks

- Identify assets, values, and custodians
- Identify risks
- Identify controls

IT Asset Lifecycle

- Planning and procurement
- Deployment
- Operation and support including updates
- Decommissioning

Asset Risk Calculations

- Exposure Factor (EF)
  - Percentage of asset affected by a single negative incident
- Single Loss Expectancy (SLE)
  - Cost associated with a single negative incident
- Annual Rate of Occurrence (ARO)
  - Negative incidents per year
- Annualized Loss Expectancy (ALE)
  - ARO x SLE

Asset Risk Calculation Example

Database, value of data: $500,000

Exposure Factor (EF) is .05

Database security breach: 5% of data value loss

SLE=AV x EF
500,000 x .05

$25,000

A breach is expected once every 2 years

ARO=.5

ALE=ARO x SLE
.5 x $25,000

$12,500

In this exercise, you will

- Describe the CIA security triad
- Provide examples of PII
- Provide examples of PHI
- Explain how the annual loss expectancy (ALE) is calculated.

CIA Security Triad

- Confidentiality
- Integrity
- Availability

PII

- Personally identifiable information
- Name
- Street address
- Bank account numbers

PHI

- Protected health information
- Blood type
- Lab test results
- Medical insurance details

Calculate ALE

- ARO = annual rate of occurrence
- SLE = single loss expectancy
- ARO x SLE