Et bilde som inneholder tekst, sirkel, Font, skjermbilde

KI-generert innhold kan være feil.

*Information gathered from the google cybersecurity course*

Innhold

[Security and Risk Management 2](#_Toc192672665)

[Asset Security 2](#_Toc192672666)

[Security Architecture and Engineering 2](#_Toc192672667)

[Communications and Network Security 3](#_Toc192672668)

[Identity and Access Management 3](#_Toc192672669)

[Security Assessment and Testing 3](#_Toc192672670)

[Security Operations 4](#_Toc192672671)

[Software Development Security 4](#_Toc192672672)

## Security and Risk Management

* Defining security goals and objectives
* Risk Mitigation

- Procedures and rules available

* Compliance

- Security policies, regulatory requirements and independent standards

* Business continuity

- Establishing disaster recovery plans

* Legal regulations

- Following laws, rules and ethical behavior to reduce negligence, abuse

and fraud

## Asset Security

* PII = Personally Identifiable Information
* SPII = Sensitive Identifiable Information
* Securing digital and physical assets
* Storage, maintenance, retention and destruction of data

## Security Architecture and Engineering

* Threat modeling
* Least privilege
* Defense in depth
* Fail securely
* Separation of duties
* Keeping it simple
* Zero Trust
* Trust but verify
* Optimizing data security

- Effective tools

- Systems

- Processes

* Shared responsibility

## Communications and Network Security

* Managing and securing physical networks and communications

- For example, managing devices availability to connect to certain networks

or Bluetooth devices

* Securing on premises networks with port evaluation and other security factors

## Identity and Access Management

* “IAM” – Identity and Access Management
* Identification (e.g, username, access card or biometric data)
* Authentication to prove someones identity
* Authorization
* Principle of least privileged
* Access
* Limited and strict access to reduce risk
* Established policies to control and manage assets
* Accountability - easier to distinguish what users did what (example logs)

## Security Assessment and Testing

* Security control testing

- Identify new and better ways to mitigate threats, risks and vulnerabilities

- Examining goals and objectives

-Evaluating if controls help achieve goals and objectives

* Collecting and analyzing data
* Security audits to monitor risks, threats and vulnerabilities

## Security Operations

* Training and awareness
* Reporting and documentation
* Intrusion detection (system) (IDS) and prevention
* SIEM tools
* Incident management
* Playbooks
* Post-breach forensics
* Reflecting on lessons learned
* Conducting investigations

- Collecting evidence

- Logs

- When?

- Where?

- What?

- Who?

- Why?

* Implementing preventative measures

## Software Development Security

* Securing coding practices

- Each phase goes under a security review for minimizing risk

- Secure design review during design phase

- Secure code reviews during the development and testing phases

- Penetration testing during the deployment and implementation phases