Table of Contents

Information security

Information security, sometimes shortened to infosec, is the practice of protecting information by mitigating information risks.

*Snippet from Wikipedia: **Information security***

> **Information security**, sometimes shortened to **infosec**, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized or inappropriate access to data or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g., electronic or physical, tangible (e.g., paperwork), or intangible (e.g., knowledge). Information security's primary focus is the balanced protection of data confidentiality, integrity, and availability (also known as the "CIA" triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. This is largely achieved through a structured risk management process that involves:
>
> - Identifying information and related assets, plus potential threats, vulnerabilities, and impacts;
> - Evaluating the risks
> - Deciding how to address or treat the risks, i.e., to avoid, mitigate, share, or accept them
> - Where risk mitigation is required, selecting or designing appropriate security controls and implementing them
> - Monitoring the activities and making adjustments as necessary to address any issues, changes, or improvement opportunities
>
> To standardize this discipline, academics and professionals collaborate to offer guidance, policies, and industry standards on passwords, antivirus software, firewalls, encryption software, legal liability, security awareness and training, and so forth. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, transferred, and destroyed. However, the implementation of any standards and guidance within an entity may have limited effect if a culture of continual improvement is not adopted.

method, requirements, architecture, programming, maintenance, change, devopsplan, devopscreate, devopsverify, release

Todo:

- BDD-Security
- Black Duck
- Charles Proxy
- Checkmarx AppSec Accelerator
- Checkmarx SAST (Static Application Security Testing)

- CyberArk Conjur
- Fortify SCA
- Fortify WebInspect
- HashiCorp Vault
- IriusRisk
- Kiuwan
- Klocwork
- LogRhythm SIEM
- OSSEC
- OWASP Zed Attack Proxy (ZAP)
- Qualys Cloud Platform
- SD Elements
- SecureAssist
- Signal Sciences
- Snort
- SonarQube
- Sqreen
- Tripwire
- Twistlock
- Venafi Trust Protection Platform
- Veracode
- WhiteHat