ISO/IEC 27000:2018(en)

Information technology — Security techniques — Information security management systems

Overview and vocabulary

The standard ISO/IEC 27000:2018 provides a collection of terms and definitions for information security management. It is part of the ISO/IEC 27000 set of standards, which give recommendations and basic concepts for beginning, implementing, maintaining, and enhancing an organization's information security management.

Some of the most important terminology and meanings in ISO/IEC 27000:2018 are:

Assets include data, hardware, software, people, and a company's reputation.

Confidentiality is the quality of preventing the disclosure of information to unauthorized individuals, entities, or procedures.

Integrity is the quality of preventing information from being corrupted or altered in an unintended or illegal manner.

Availability is the property that ensures information is accessible and usable when required by authorized users.

Information that is protected from unauthorized access, use, disclosure, disruption, alteration, or deletion.

Risk is the potential for harm to an organization or its assets as a result of vulnerabilities being exploited.

A weakness in an asset or system that can be exploited by an adversary.

Threat: Any condition or occurrence that has the potential to inflict harm to an organization or its assets.

A security event is an occurrence that has caused or could have caused a security breach.

Controls for preventing threats to the confidentiality, integrity, and availability of data.

ISMS: A collection of rules, procedures, and controls that protect the confidentiality, integrity, and availability of information.

Certification: The process of validating independently that an organization's ISMS complies with a specific standard.

Overall, ISO/IEC 27000:2018 provides a framework for managing information security in an organization and assists companies in protecting their assets and ensuring the confidentiality, availability, and integrity of their information.

References

Chapple, M., Stewart, J. M., & Gibson, D. (2021). (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide. Sybex.

ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary, Available at https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en