# ISO 27001 (ISMS)

## Summary

**Regulation**: Information Security Management System (ISMS)

**Abbreviation**: ISO 27001 (ISMS)

**Governs these parties**: all organizations that store or manage data, IT-based, Health, Government, and public companies

**Enforced by**: the majority of global companies require their partners and vendors to meet these standards

## Details

Through the adoption of an Information Security Management System (ISMS), ISO 27001 provides a framework that can help organizations protect their information in a systematic and cost-effective manner in terms of confidentiality, integrity, and availability. The process involves identifying the potential problems that could occur with the information (risk assessment), and then determining how these problems can be prevented (risk mitigation or risk treatment).

The rest of this document is designed to help our community understand ISO 27001 (ISMS) better by outlining the following information.



### How it Relates to Cybersecurity

ISO 27001 (ISMS) requires businesses to:

- ensure their IT systems, including operating systems and software, are secure and protected against data loss with events records and generating evidence, periodic verification of vulnerabilities, and taking precautions to prevent audit activities from affecting operations
- secure communications by protecting the network infrastructure and services, as well as the information that travels through them
- have a security incident policy in place in order to handle security events and incidents with proper communication so that they can be resolved in a timely manner
- ensure the continuity of information security management during disruptions and the availability of information systems