What is Information Security

Information security is often reduced to hacking and technical vulnerabilities. While those threats matter, they represent only a fraction of the discipline.

At its core, information security is about protecting information—regardless of format or medium—from unauthorized access, misuse, disruption, modification, or destruction. Its primary objective is to preserve **confidentiality, integrity, and availability**, while enabling organizations to operate productively and responsibly.

The meaning of information security often depends on perspective:

- A finance leader sees risk reduction.
- A legal officer sees compliance.
- A business executive sees resilience and maturity.
- A board member sees trust.

These viewpoints are not conflicting—they are complementary.

Information security is a **coordinated set of strategies, processes, and controls** designed to prevent, detect, and respond to threats across digital and non-digital assets alike. It is inherently multidisciplinary, combining technical, organizational, human, and legal dimensions.

In other words, information security is not just about defending systems—it's about safeguarding the information that organizations rely on to function, decide, and compete.

This topic is explored further in Section 1.2, *What is Information Security*, in Chapter 1 of Volume 1 (*Information Security Fundamentals*) of the *Mastering Information Security* series.