

**“IT  
decisions  
made only  
by IT teams”**

**“IT  
decisions governed  
by top  
management  
(ISO/IEC 38500)”**

**Content:**

- 01: Main Page Index Content**
- 02: What is ISO/IEC 38500?**
- 03: Why organisations use ISO/IEC 38500?**
- 04: Key characteristics of ISO/IEC 38500 .**
- 05: The core principles.**

**“Good governance ensures that technology serves the organisation, not the other way around.”**

## 02: What is ISO/IEC 38500?

### Definition:

ISO/IEC 38500 is an international standard for the governance of information technology. It provides guidance for boards and senior management on how to direct and control the use of IT within an organisation.

### Main focus areas:

Strategic alignment of IT with business goals  
Accountability and responsibility for IT decisions  
Oversight of risk, performance, and compliance

### Goal:

To ensure that IT supports the organisation's objectives, delivers value, and is used responsibly and effectively.

**Provide information**  
and guidance to  
managers that control  
the use of IS/IT in your  
organization/Company.

**Ensure that**, if the rule is  
followed properly, the  
stakeholders (managers,  
Consultants, etc.) can rely  
on the corporate  
governance of IT.

**Provide a basis for**  
objective evaluation  
by top management  
of IT management.

**"IT governance is about making IT work for organisation and stakeholders".**

## WHO ?

Was primarily developed by Standards Australia based on their AS 8015:2005 standard

Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2008.

## WHY ?

Organizations use ISO/IEC 38500 to ensure their IT investments deliver maximum value while minimizing risks and ensuring legal compliance.

It shifts the view of IT from a technical department responsibility to a strategic corporate asset that is governed at the board level.

### Primary Reasons for Adoption:

- Ensures IT strategies and activities directly support overall business goals
- Provides a framework to identify and manage IT-related risks
- Helps boards make informed, data-driven decisions on IT investments to ensure they contribute positively
- Establishes clear accountability for meeting legal and regulatory requirements



“Better decisions create better outcomes.”

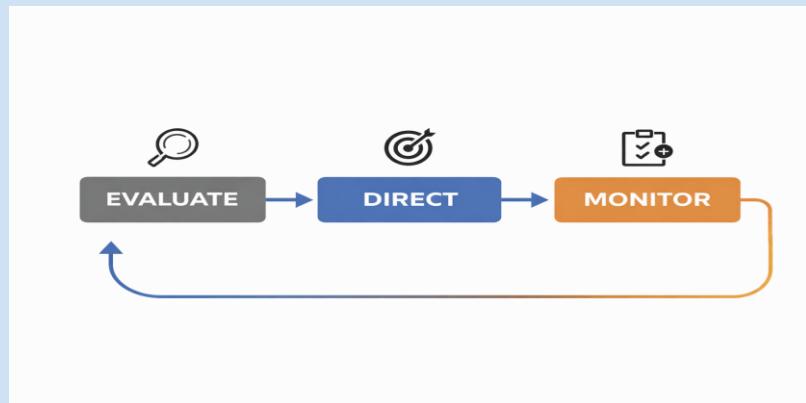
## Nature and scope of the standard ?

ISO/IEC 38500 is a high-level governance standard. It applies at the board and executive level and does not address operational IT management. The standard is technology-independent and applicable to all types of organizations.

## Principle-based approach ?

The standard follows a principle-based approach rather than a procedural one. It does not provide detailed methods or technical solutions. Organizations remain free to design their own governance mechanisms within a common framework.

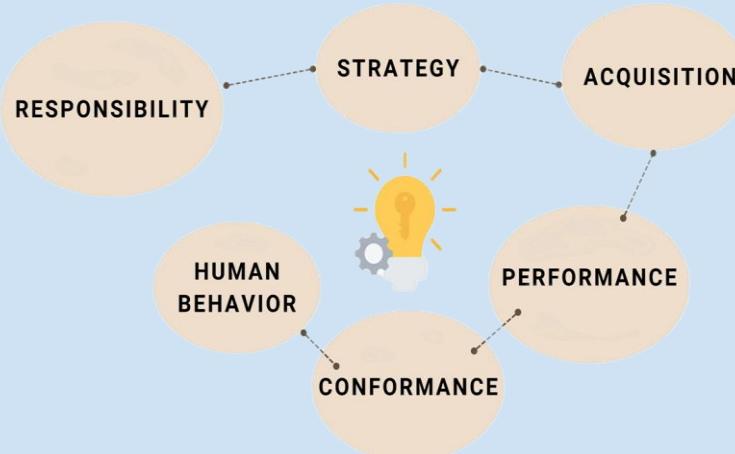
## Governance model and structurer:



ISO/IEC 38500 is structured around the Evaluate – Direct – Monitor (EDM) governance model. This structure enables continuous oversight of IT-related decisions and ensures clear accountability at the leadership level.

**“Governing IT is no longer optional, it is strategic.”**

## 05: The core principles



**Responsibility** – Clear accountability for IT decisions

**Strategy** – IT supports organisational objectives

**Acquisition** – IT investments deliver value

**Performance** – IT is fit for purpose

**Conformance** – Compliance with laws and policies

**Human Behaviour** – People are considered in IT decisions

**"IT delivers value only when decisions are governed."**