SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M10 Most common Certifications available on the market

Contents

M10.1 Most common Certifications available on the market

- Competence and Governance. Introduction and context.
- ISACA - COBIT 5 Framework and ISO/IEC 38500:2015
- Certification for people related to Governance and Management of Enterprise IT. ISACA – COBIT

Context

COMPETENCE AND GOVERNANCE. RELATED CERTIFICATION

We have seen that *standards* and *frameworks* are a valid tool to guide organizations and companies in continuous improvement. Since companies are also made up of *people*, taking into account the *human resources* available and not, **governance** and **competence** can be very close issues.

There are specific **certifications** in this field to demonstrate the knowledge, the skills and ability of people who need to master how IT companies must be organized by adopting best practices and more.

Context

COMPETENCE AND GOVERNANCE. RELATED CERTIFICATION

The organization of a company, starting from the definition of its **objectives**, is a fundamental skill for many professional figures (including those profiles who do not have to establish the strategic address or manage parts of the organization).

The objectives of IT companies are **specific** to this type of activity and they must be *integrated* within the overall objectives.

Context

INFORMATION AS A COMMON RESOURCE

Information is a key resource for all enterprises, and from the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in enterprises and in *social*, *public* and *business* environments.

[Source: COBIT 5 framework - isaca.org]

Context

COBIT 5 PURPOSES

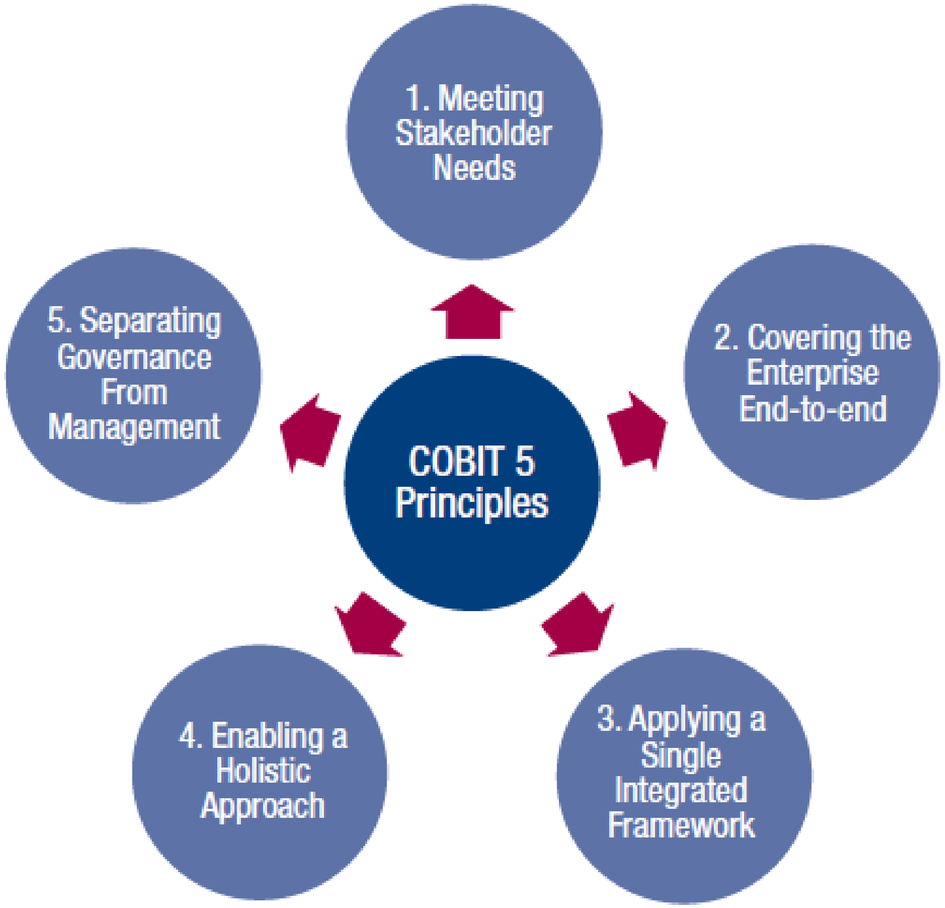
COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it can help enterprises create optimal value from IT by maintaining a balance between *realising benefits* and *optimising risk levels* and *resource use*.

This Framework enables IT to be governed and managed in a **holistic manner** for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of *internal* and *external* stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT



[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Principle 1, **Meeting Stakeholder Needs.** It introduces the COBIT 5 *goals cascade*. The enterprise goals for IT are used to formalise and structure the stakeholder **needs**. Enterprise goals can be linked to *IT-related goals*, and these IT-related goals can be achieved through the *optimal use* and *execution* of all enablers, including processes. This set of connecting goals is called **the COBIT 5 goals cascade**. The chapter also provides examples of typical *governance* and *management* questions that stakeholders may have about enterprise IT.

[Source: COBIT 5 framework - isaca.org]

Cobit 5

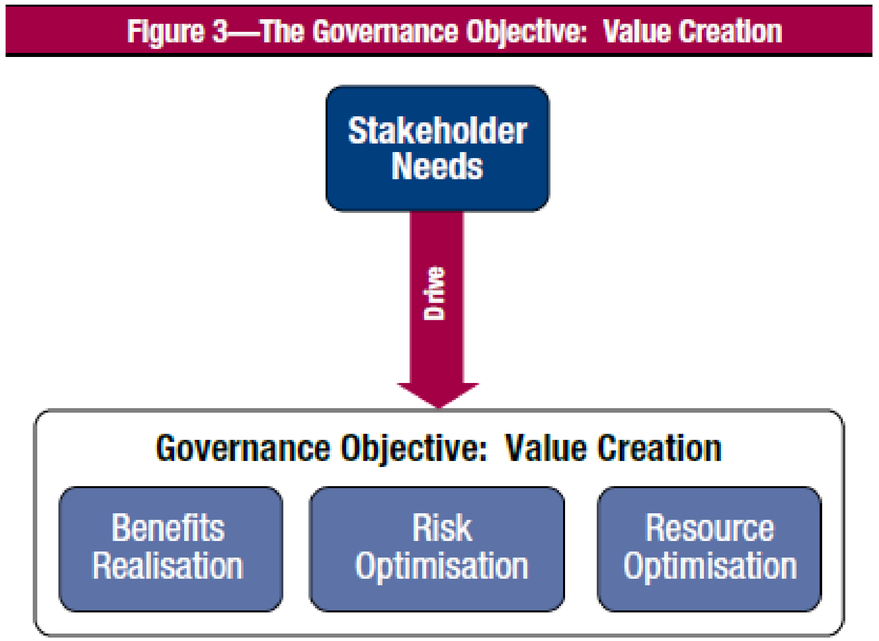
A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Step 1. *Stakeholder Drivers Influence Stakeholder* ***Needs***
Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and new technologies.

Step 2. *Stakeholder Needs Cascade to* ***Enterprise*** *Goals*

Step 3. **Enterprise** Goals Cascade to IT-related Goals

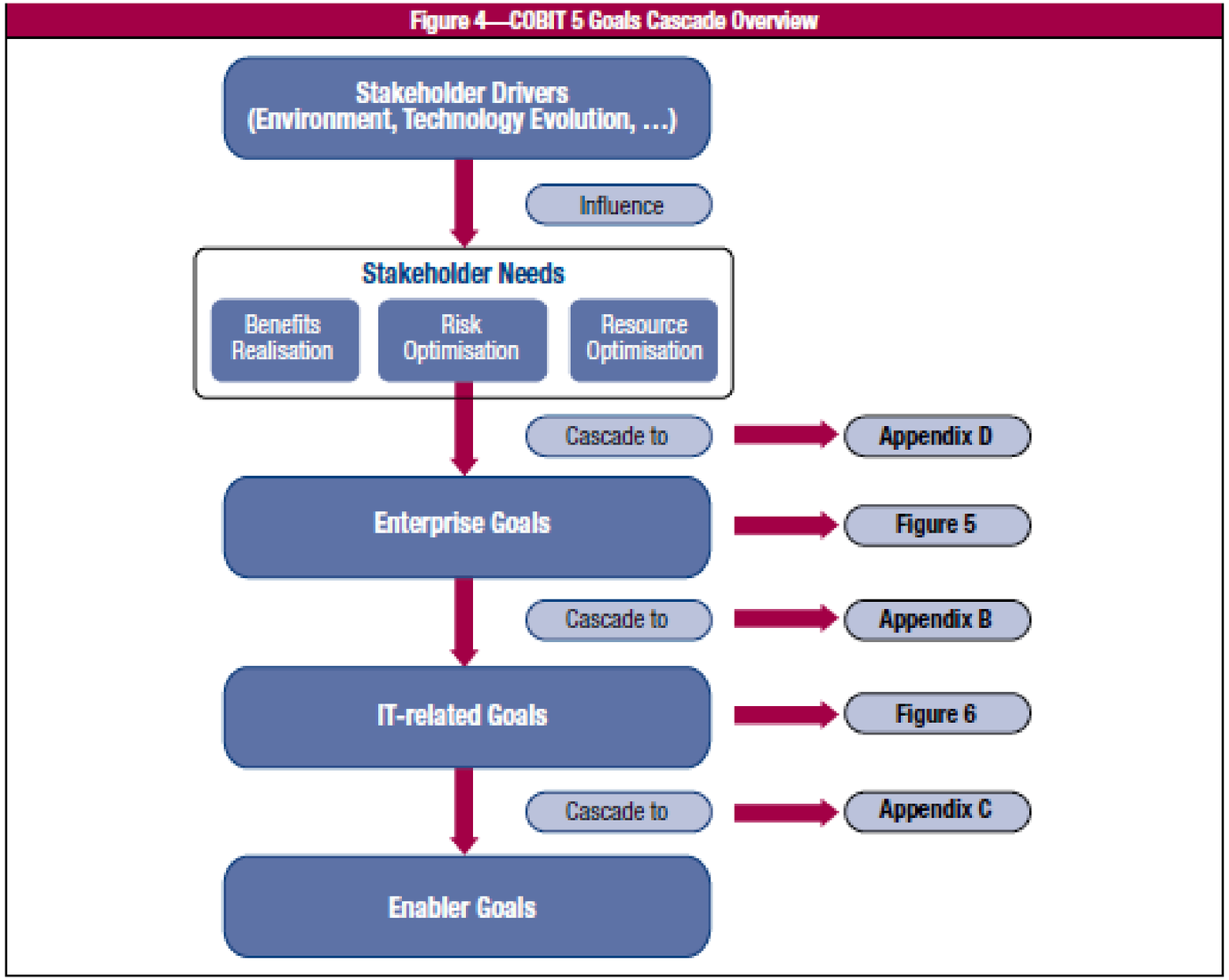
Step 4. IT-related Goals Cascade to **Enabler** Goals



[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

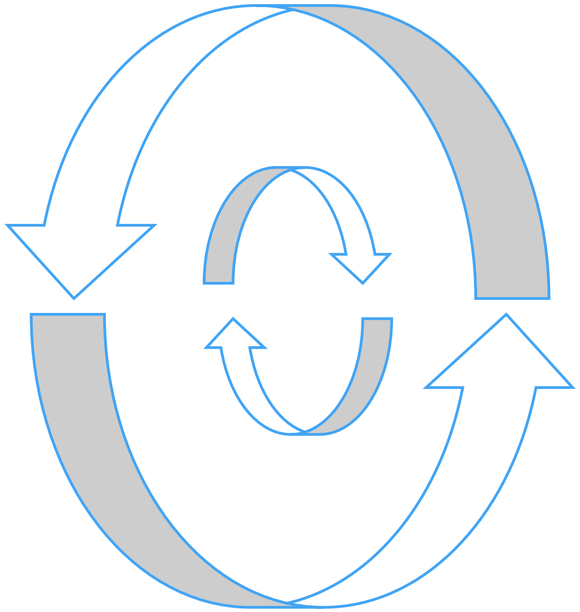


[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Principle 2, **Covering the Enterprise End-to-end**. It explains how COBIT 5 integrates *governance of enterprise IT* into *enterprise governance* by covering all functions and processes within the enterprise.

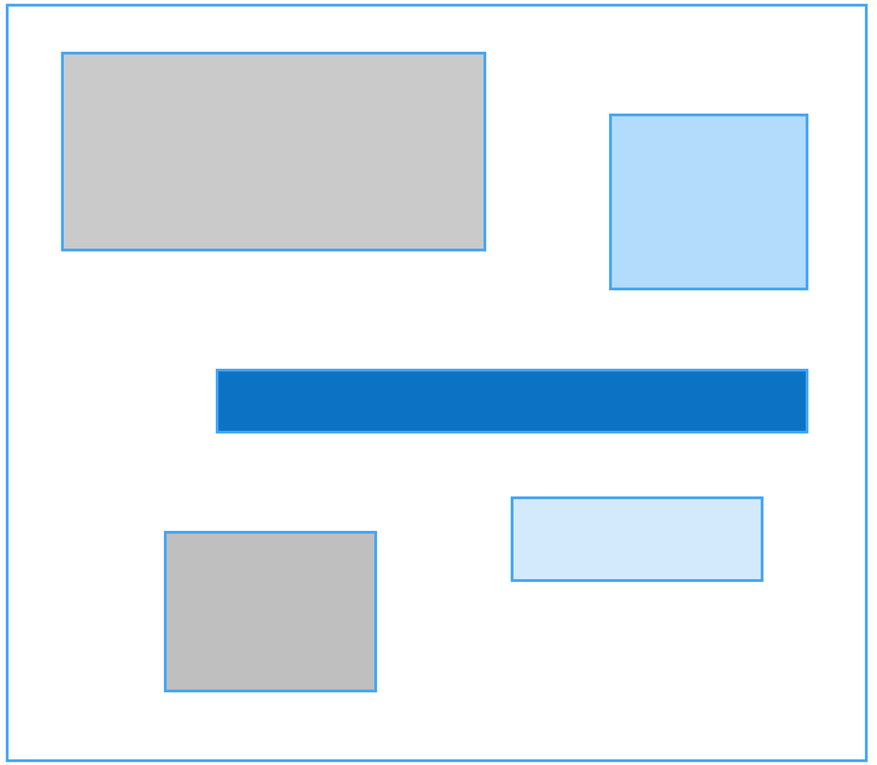


[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Principle 3, **Applying a Single Integrated Framework**, describes briefly the COBIT 5 architecture that achieves the integration.

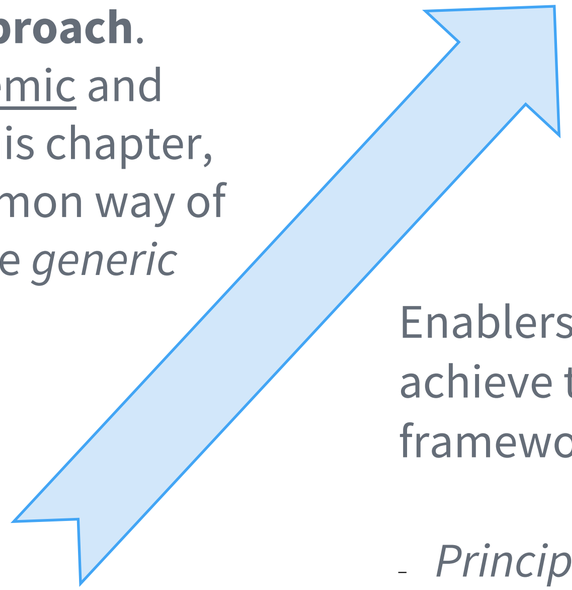


[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Principle 4, **Enabling a Holistic Approach**. Governance of enterprise IT is systemic and supported by a *set of enablers*. In this chapter, enablers are introduced and a common way of looking at enablers is presented: the *generic enabler* model.



Enablers are broadly defined as anything that can help to achieve the **objectives** of the enterprise. The COBIT 5 framework defines seven categories of enablers:

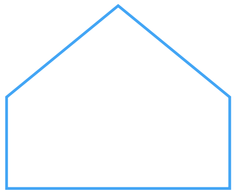
- *Principles*, *Policies* and *Frameworks*
- *Processes*
- Organisational *Structures*
- *Culture*, *Ethics* and *Behaviour*
- *Information*
- *Services*, *Infrastructure* and *Applications*
- *People*, *Skills* and *Competencies*

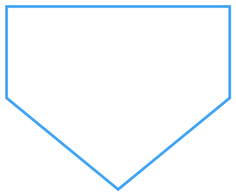
[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Principle 5, **Separating Governance From Management**, and discusses the difference between management and governance, and how they interrelate. The high-level COBIT 5 process reference model is included as an *example*.





[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Principle 5, **Separating Governance** From **Management**

- Governance

Governance ensures that stakeholder needs, conditions and options are evaluated to determine **balanced**, **agreed-on** *enterprise objectives to be achieved*; setting direction through *prioritisation* and *decision making*; and *monitoring* performance and *compliance* against agreed-on direction and objectives.

In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.

[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Principle 5, **Separating Governance** From **Management**

- Management

  Management plans, builds, runs and monitors activities *in alignment with the direction set by the governance body* to achieve the enterprise objectives.

  In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

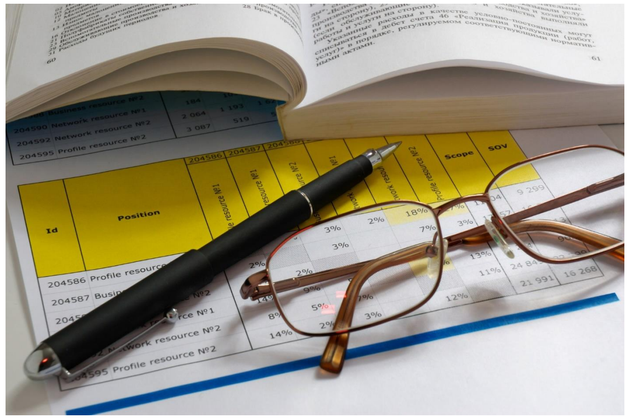
[Source: COBIT 5 framework - isaca.org]

Cobit 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

Implementation Guidance describes how the appropriate environment can be created, the enablers required, typical pain points and trigger events for implementation, and the implementation and continual improvement life cycle.

The COBIT 5 Process Capability Model in the COBIT Assessment Programme approach (*www.isaca.org/cobit-assessment-programme*)



[Source: COBIT 5 framework - isaca.org]

ISO/IEC 38500

PRINCIPLES

ISO/IEC 38500:2015 provides *guiding principles* for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or *similar*) on the **effective**, **efficient**, and **acceptable** use of information technology (IT) within their organizations.

[Source: iso.org]

ISO/IEC 38500

PRINCIPLES

It also provides guidance to those *advising*, *informing*, or *assisting* governing bodies. They include the following:

- *executive* managers;
- members of groups monitoring the resources within the organization;
- *external* business or technical specialists, such as **legal** or **accounting** specialists, *retail* or *industrial* associations, or professional bodies;
- internal and external service providers (including consultants);
- **auditors**.

[Source: iso.org]

ISO/IEC 38500

PRINCIPLES

ISO/IEC 38500:2015 applies to the governance of the organization's **current** and **future** use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organization, *external* service providers, or business units *within* the organization.

[Source: iso.org]

ISO/IEC 38500

PRINCIPLES

ISO/IEC 38500:2015 defines the governance of IT as a subset or domain of *organizational governance*, or in the case of a corporation, corporate governance.

ISO/IEC 38500:2015 is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. ISO/IEC 38500:2015 is applicable to organizations of all sizes from the smallest to the largest, *regardless* of the extent of their use of IT.

[Source: iso.org]

ISO/IEC 38500

PRINCIPLES

The purpose of ISO/IEC 38500:20015 is to promote **effective**, **efficient**, and **acceptable** use of IT in all organizations by:

- assuring stakeholders that, if the principles and practices proposed by the standard are followed, they can have *confidence* in the organization's governance of IT,

- informing and guiding governing bodies in governing the use of IT in their organization, and

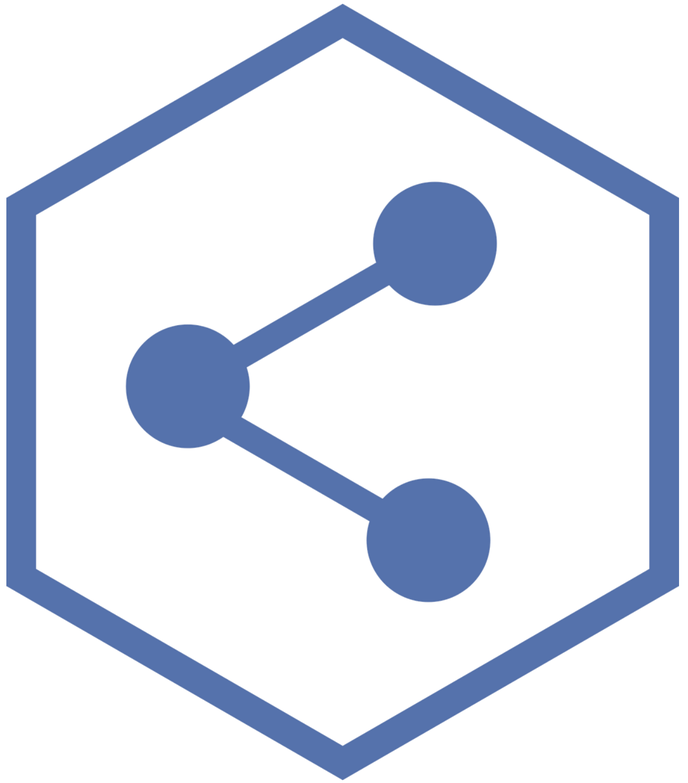
- establishing a vocabulary for the governance of IT.

[Source: iso.org]

ISO/IEC 38500

PRINCIPLES

Many of the principles addressed in ISO / IEC 38500: 2015 are **covered** by Cobit 5 Framework.



ISO/IEC 38500:2015

PRINCIPLES

ISO/IEC 38500:2015 is structured in 6 principles:

Chapter 5.2 - Principle 1: *Responsibility*

Chapter 5.3 - Principle 2: *Strategy*

Chapter 5.4 - Principle 3: *Acquisition*

Chapter 5.5 - Principle 4: *Performance*

Chapter 5.6 - Principle 5: *Conformance*

Chapter 5.7 - Principle 6: *Human Behaviour*

[Source: iso.org]

ISO/IEC 38500:2015

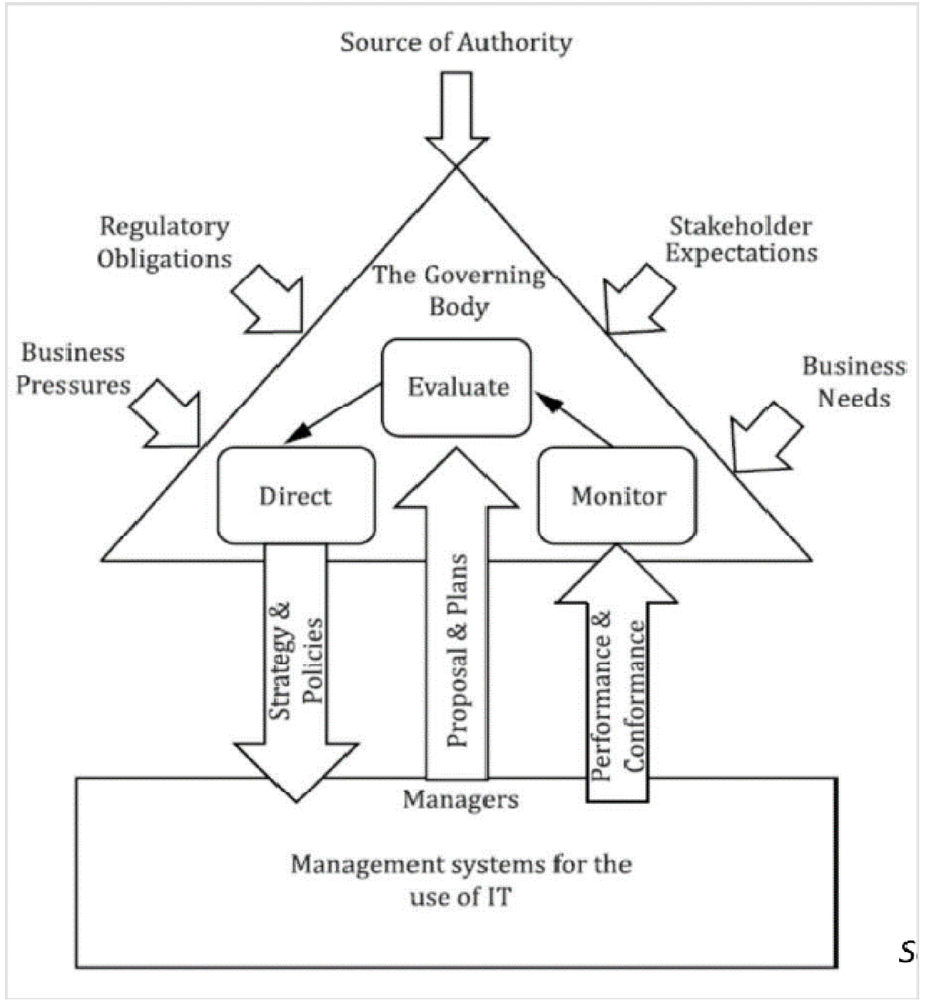
INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

ISO/IEC 38500 Principles

Principle 1—Responsibility

The business (*customer*) and IT (*provider*) should work together in a *partnership model* utilising effective communications based on a positive and trusted *relationship* and demonstrating clarity regarding **responsibility** and **accountability**. For larger enterprises, an IT executive committee (also referred to as the IT strategy committee) acting on behalf of the board and chaired by a board member is a very effective mechanism for evaluating, directing and monitoring the use of IT in the enterprise and for advising the board on critical IT issues.

[Source: COBIT 5 framework - isaca.org]



[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

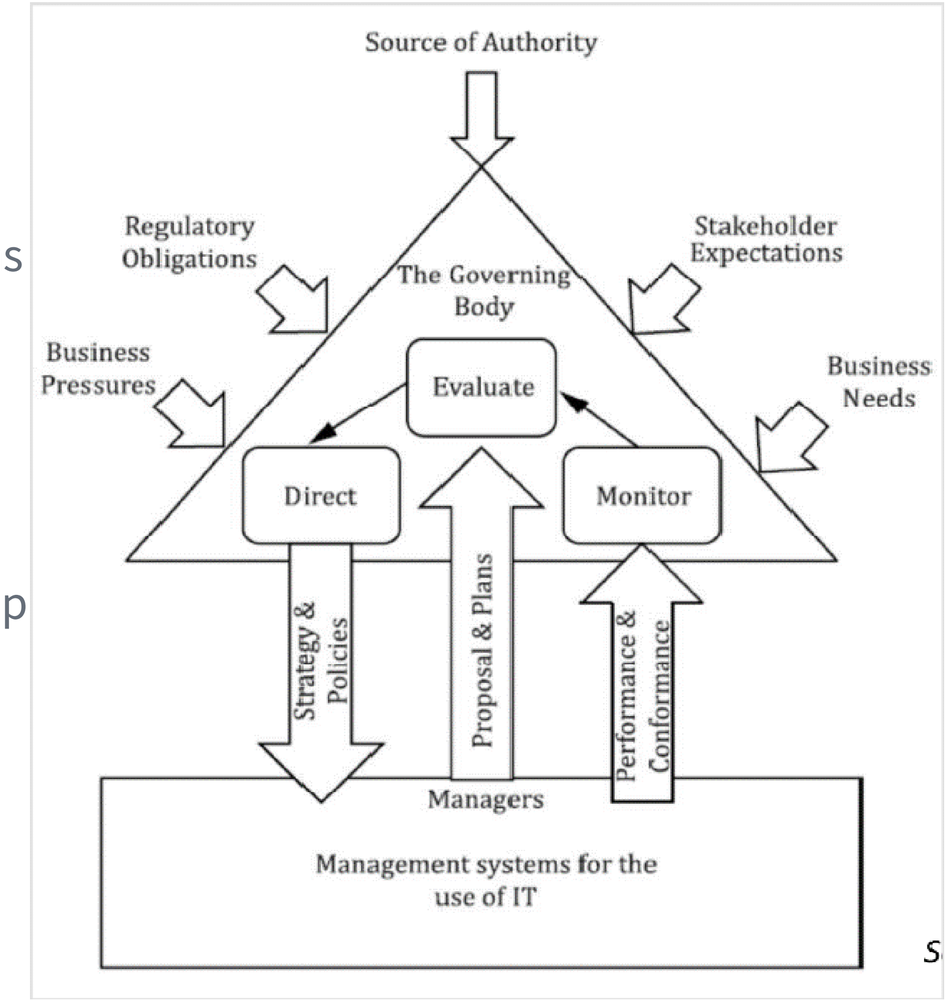
INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

Principle 1—Responsibility

Directors of small and medium-sized enterprises with a simpler command structure and shorter communication paths need to take *a more direct approach* when overseeing IT activities.

In all cases, appropriate governance organisational **structures**, **roles** and **responsibilities** are required to be mandated from the governing body, providing clear ownership and accountability for important decisions and tasks. This should include relationships with key third-party IT service providers.

[Source: COBIT 5 framework - isaca.org]



[Source: ISO/IEC 38500:2015]

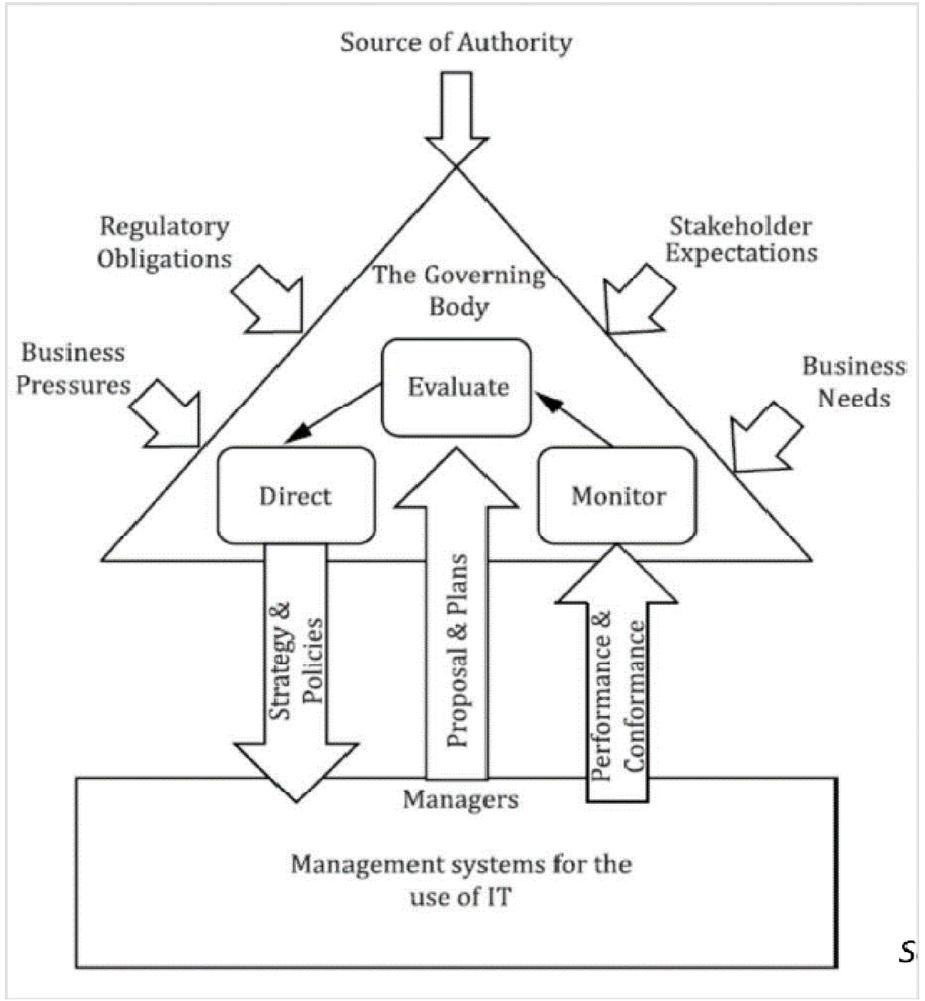
ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

PRINCIPLE 2—STRATEGY

IT strategic planning is a *complex* and critical undertaking requiring close co-ordination amongst enterprisewide business unit and IT strategic plans. It is also vital to prioritise the plans most likely to achieve the desired benefits and to allocate resources *effectively*. High-level goals need to be translated into achievable tactical plans, ensuring *minimal failures and surprises*.
The goal is to deliver **value** in support of *strategic objectives* while considering the *associated risk* in relation to the board's risk appetite.

[Source: COBIT 5 framework - isaca.org]



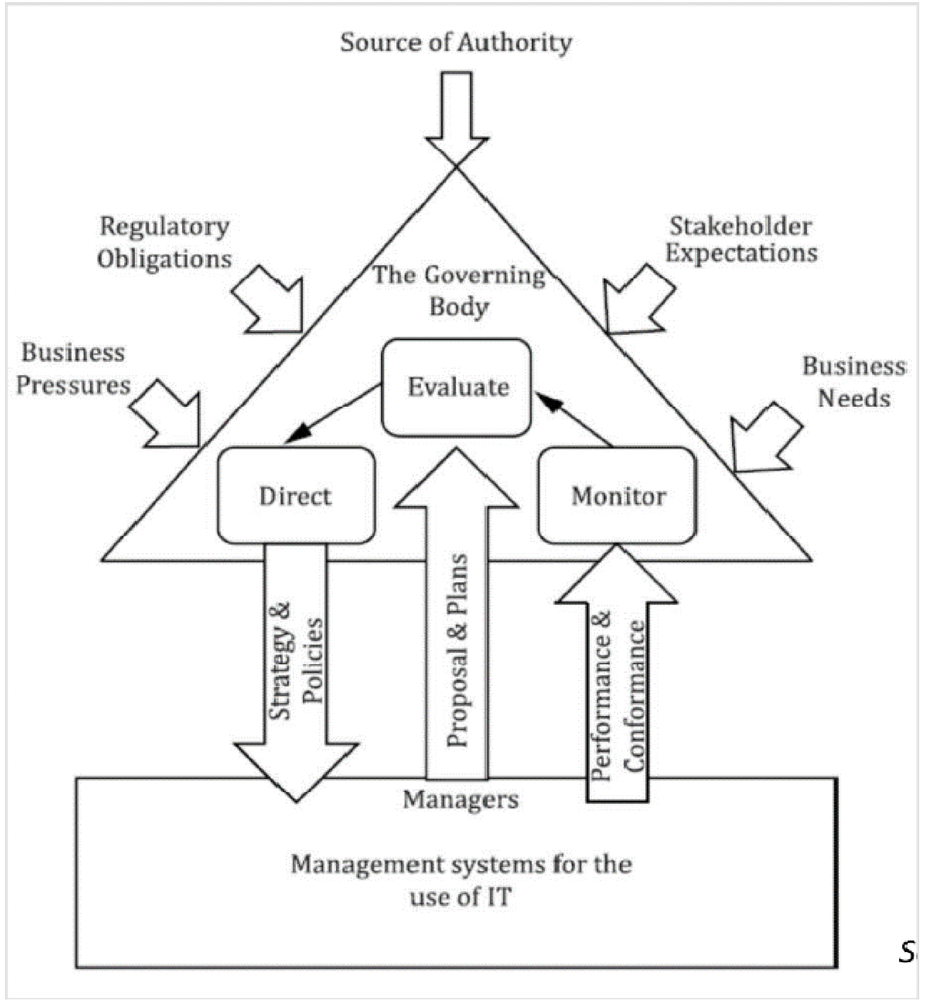
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

While it is important to cascade plans in a top-down fashion, the plans must also be **flexible** and adaptable to meet rapidly changing business requirements and IT opportunities. Furthermore, the presence or absence of IT capabilities can either enable or hinder business strategies; therefore, IT strategic planning should include transparent and appropriate planning of IT capabilities.

[Source: COBIT 5 framework - isaca.org]



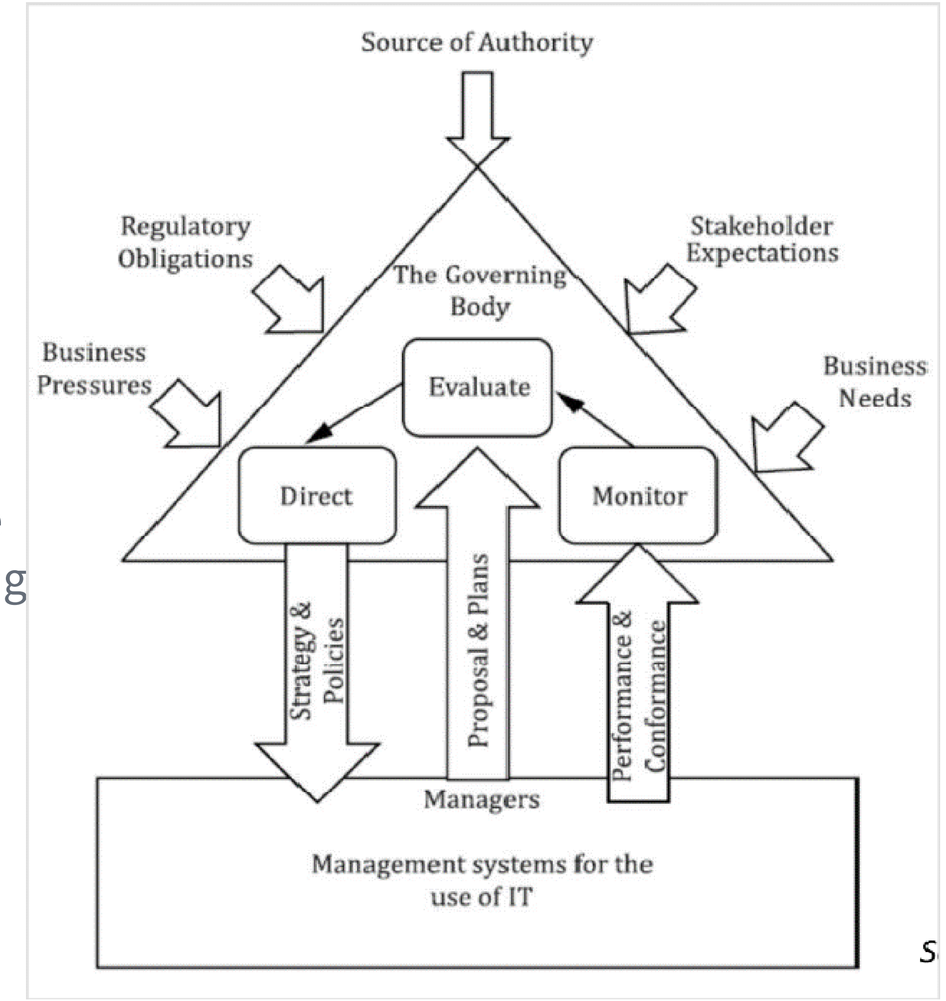
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

This should include assessment of the ability of the current IT infrastructure and human resources to support **future business requirements** and consideration of future technological developments that might *enable* competitive advantage and/or optimise **costs**. IT resources include relationships with many external product vendors and service providers, some of whom likely play a *critical role* in supporting the business. Governance of strategic sourcing is thus a very significant strategic planning activity requiring *executive-level* direction and oversight.

[Source: COBIT 5 framework - isaca.org]



[Source: ISO/IEC 38500:2015]

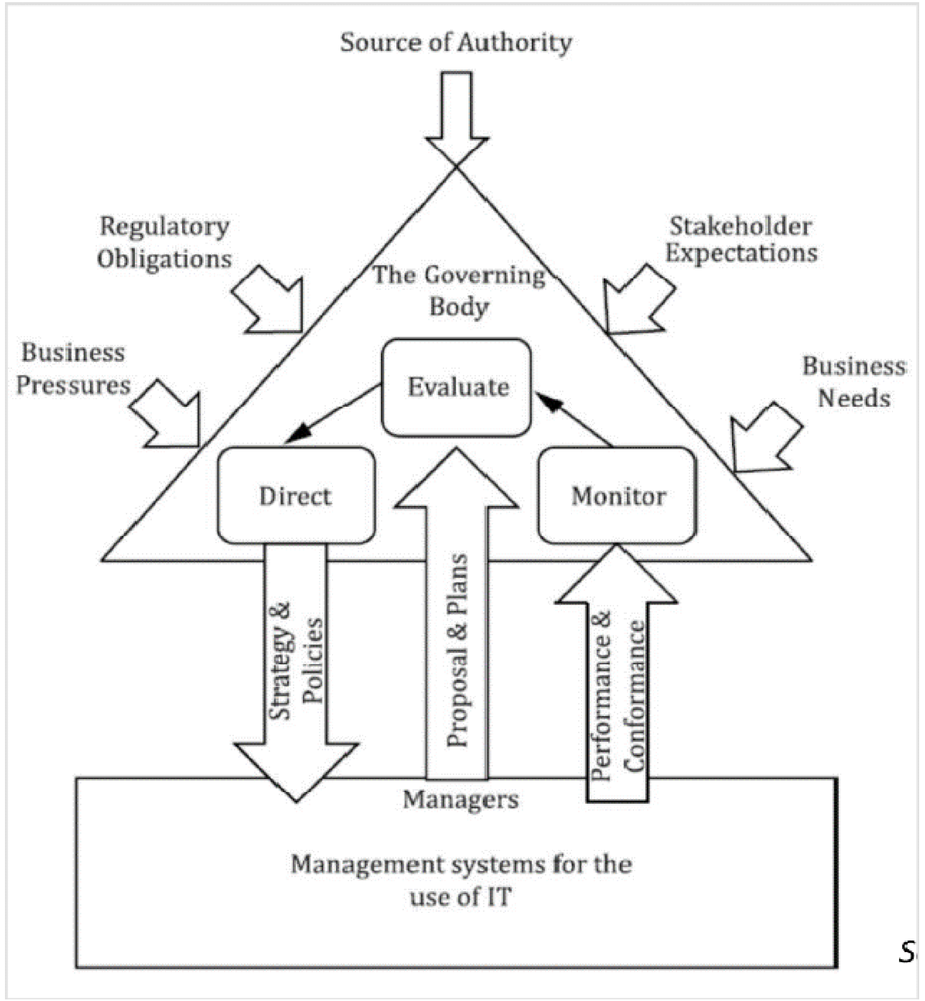
ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

PRINCIPLE 3—ACQUISITION

IT solutions exist to support business processes and therefore care must be taken to not consider IT solutions in isolation or as just a '*technology*' project or service. On the other hand, an inappropriate choice of technology architecture, a failure to maintain a current and appropriate technical infrastructure, or an absence of skilled human resources can result in project *failure*, an *inability* to sustain business operations or a *reduction* in value to the business.

[Source: COBIT 5 framework - isaca.org]



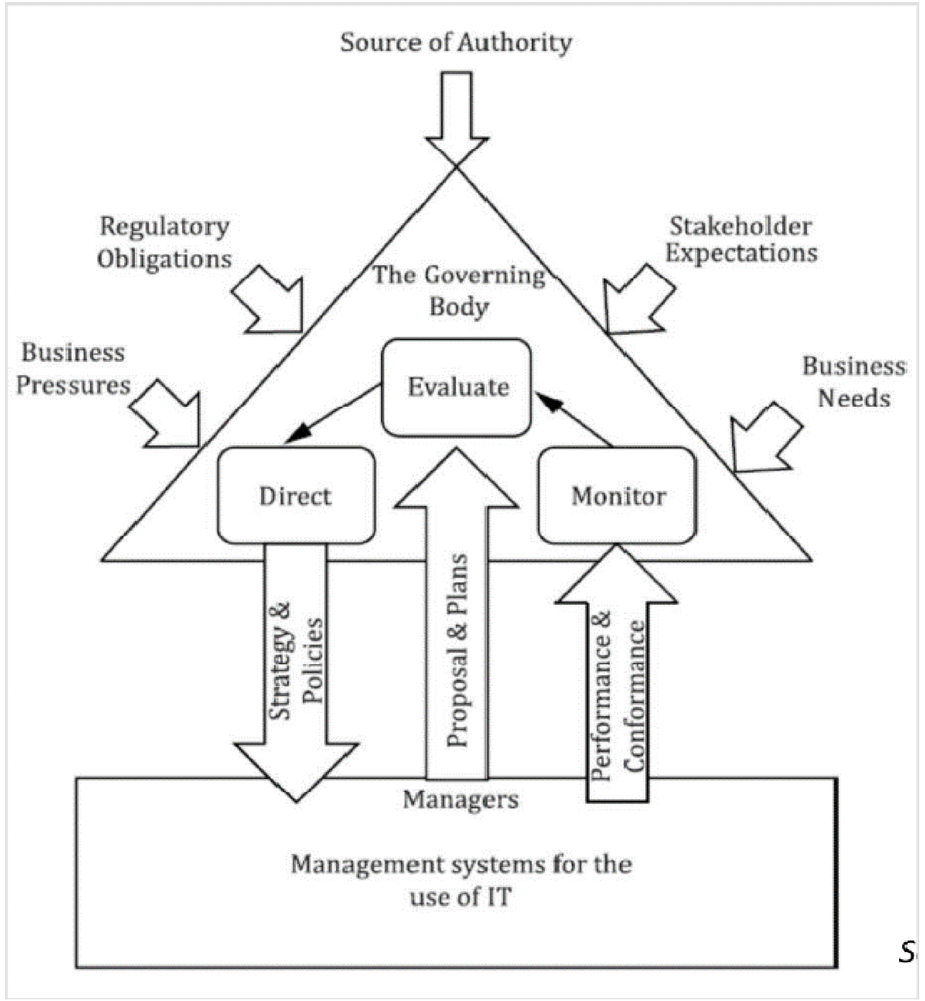
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

Acquisitions of IT resources should be considered as a **part** of wider IT-enabled business change. The acquired technology must also support and operate with existing and planned business processes and IT infrastructures. Implementation is also not just a technology issue, but rather a combination of organisational *change*, *revised* business processes, *training* and *enabling* the change. Therefore, IT projects should be undertaken as part of wider enterprisewide change programmes that include other projects satisfying the full range of activities required to help ensure a successful outcome.

[Source: COBIT 5 framework - isaca.org]



[Source: ISO/IEC 38500:2015]

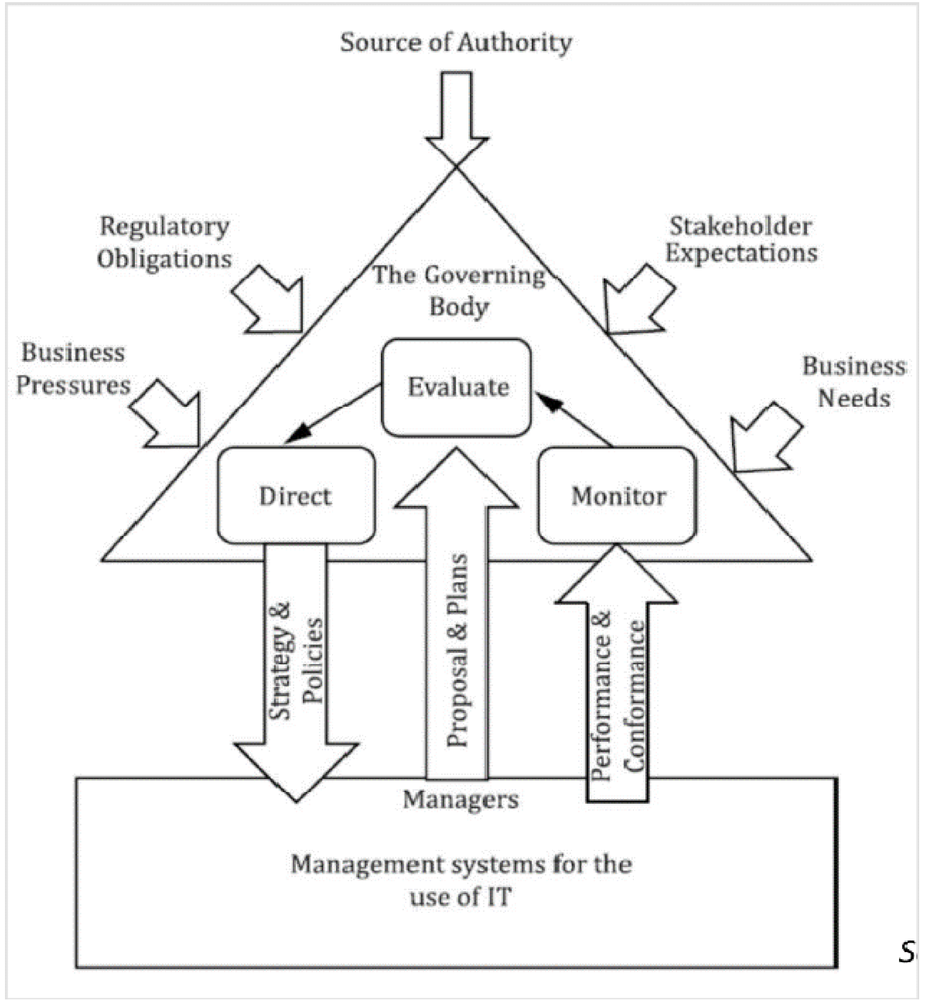
ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

PRINCIPLE 4—PERFORMANCE

Effective performance measurement depends on two key aspects being addressed: the clear definition of **performance goals** and the establishment of effective **metrics** to monitor achievement of goals. A performance measurement process is also required to help ensure that performance is monitored consistently and reliably.

[Source: COBIT 5 framework - isaca.org]



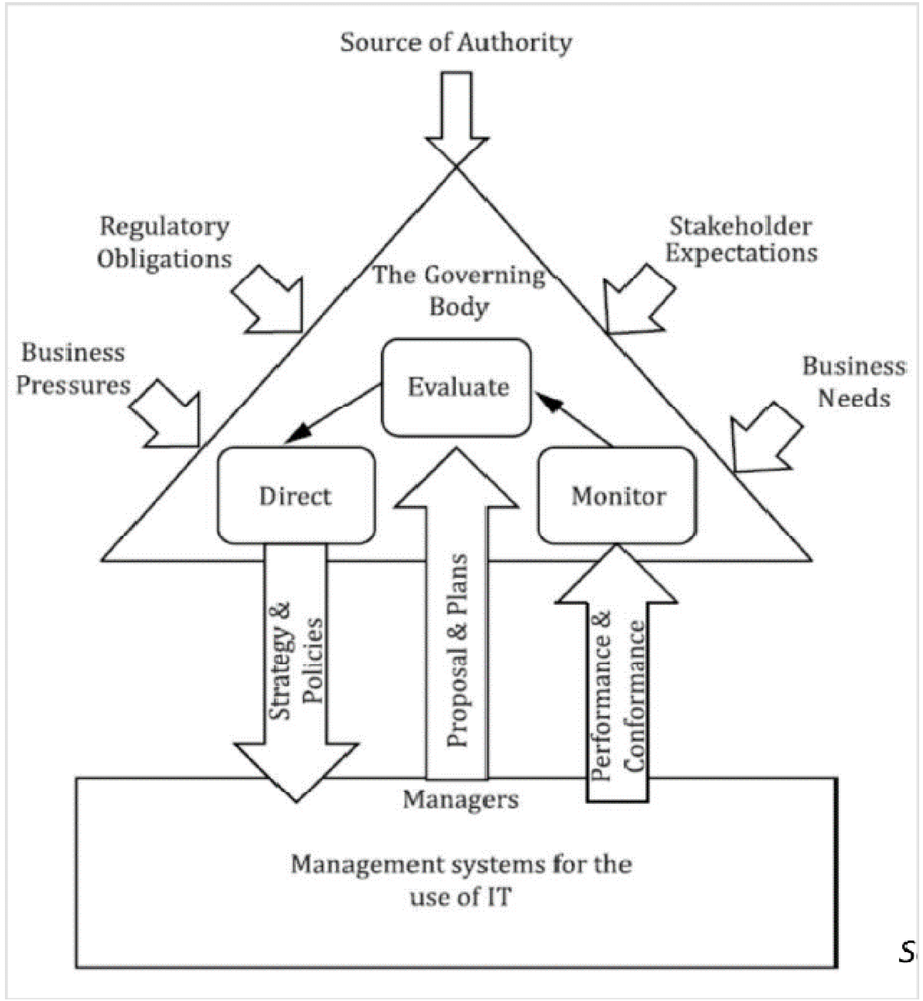
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

Effective governance is achieved when goals are set from the **top down** and aligned with high-level, approved business goals, and metrics are established from the bottom up and aligned in a way that enables the achievement of goals at all levels to be monitored by each layer of management. Two critical governance success factors are the **approval of goals** by *stakeholders*, and the *acceptance* of accountability for achievement of goals by directors and managers. IT is a complex and technical topic; therefore, it is important to achieve transparency by expressing goals, metrics and performance reports **in language meaningful to the stakeholders** so that appropriate actions can be taken.

[Source: COBIT 5 framework - isaca.org]



[Source: ISO/IEC 38500:2015]

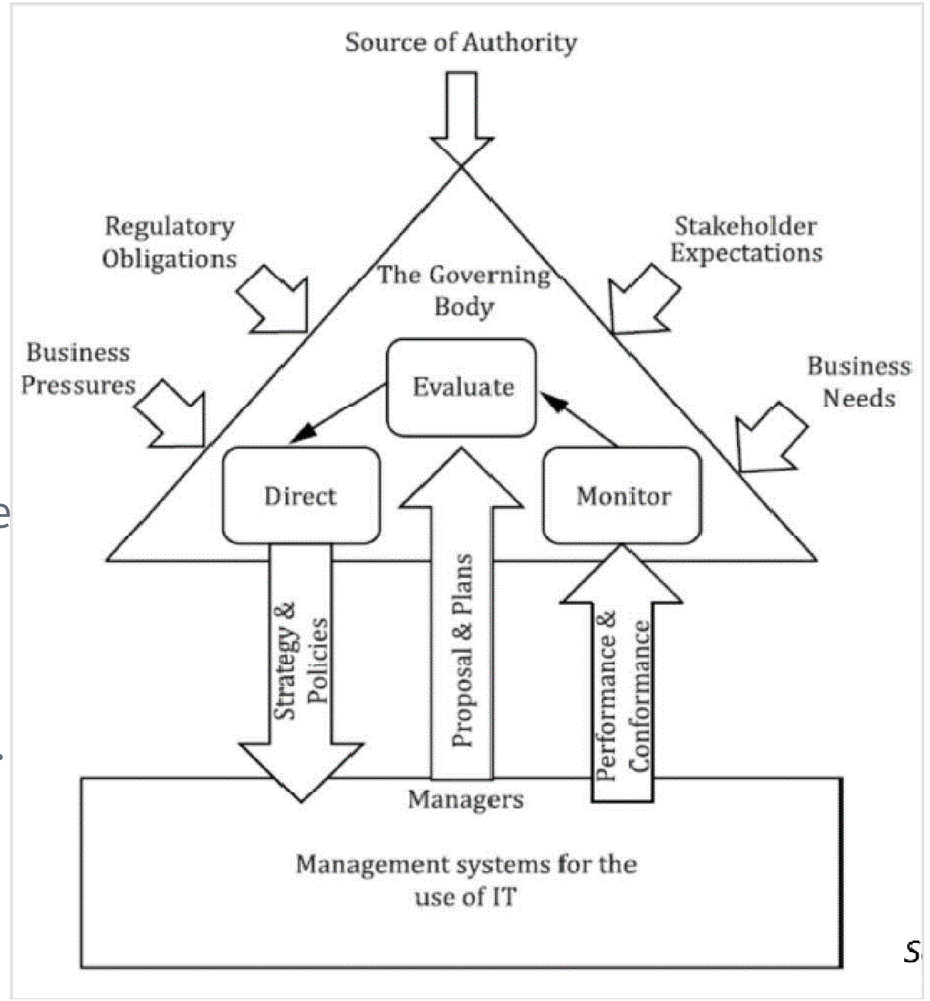
ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

PRINCIPLE 5—CONFORMANCE

In today's global marketplace, enabled by the Internet and advanced technologies, enterprises need to comply with a growing number of legal and regulatory requirements. Because of corporate scandals and financial failures in recent years, there is a heightened awareness in the boardroom of the existence and implications of tougher laws and regulations. Stakeholders require increased assurance that enterprises are complying with laws and regulations and conforming to good corporate governance practice in their operating environment.

[Source: COBIT 5 framework - isaca.org]



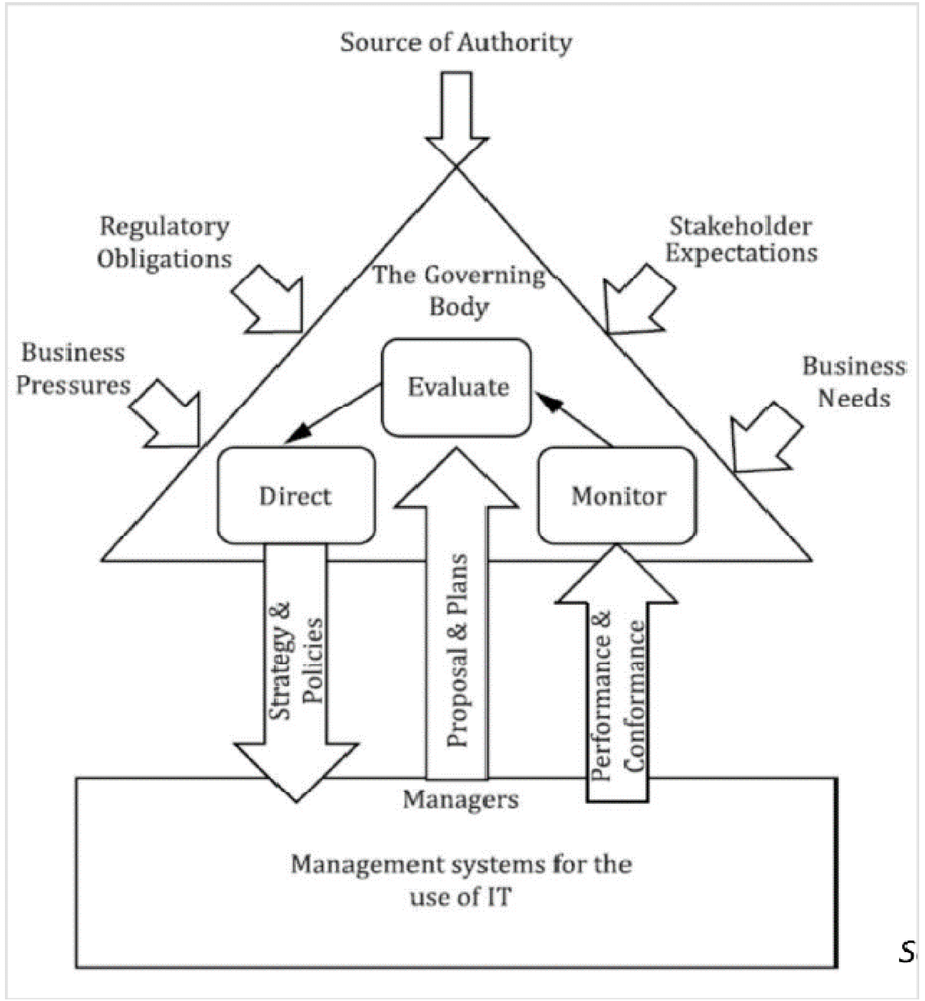
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

In addition, because IT has enabled seamless business processes between enterprises, there is also a growing need to help ensure that contracts include important IT-related requirements in areas such as privacy, confidentiality, intellectual property and security.
Directors need to ensure that compliance with external requirements is dealt with as a part of strategic planning rather than as a costly afterthought.

[Source: COBIT 5 framework - isaca.org]



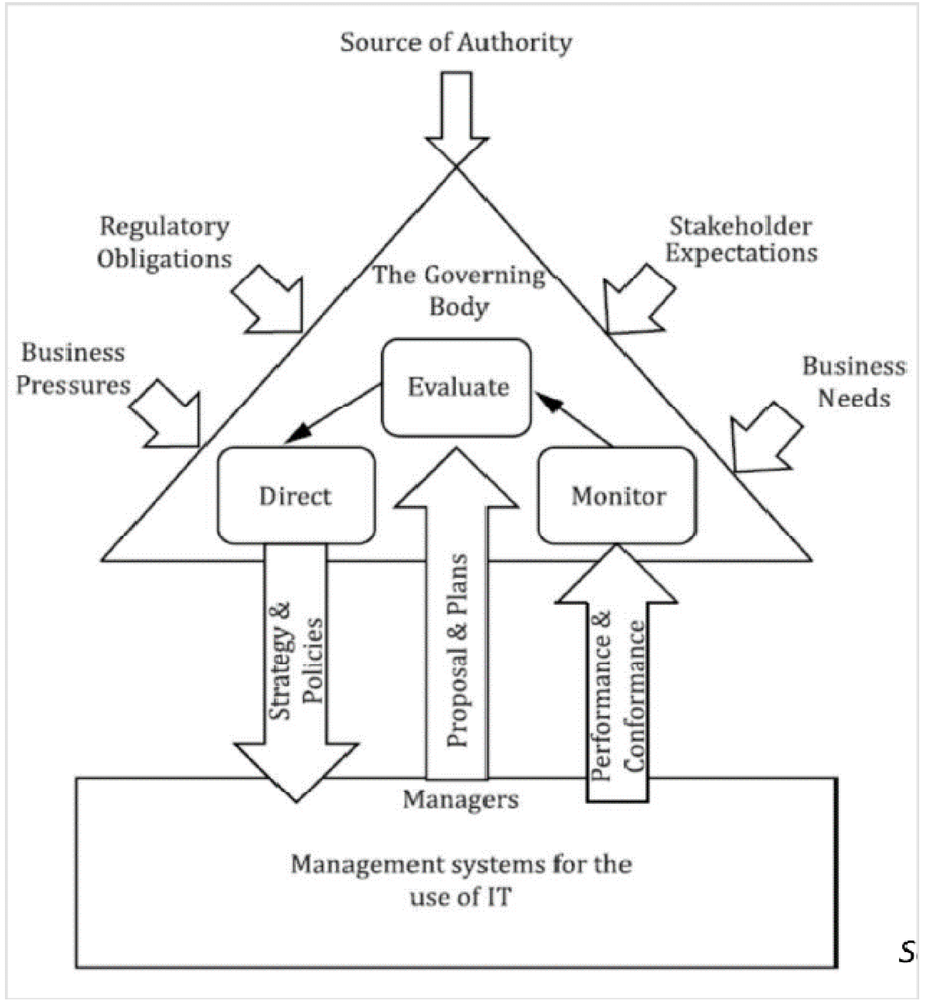
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

They also need to set the tone at the top and establish policies and procedures for their management and staff to follow, to ensure that the goals of the enterprise are realised, risk is *minimised* and compliance is **achieved**. Top management must strike an appropriate *balance* between performance and conformance, ensuring that performance goals do not jeopardise compliance and, conversely, that the conformance regime is appropriate and does not overly restrict the operation of the business.

[Source: COBIT 5 framework - isaca.org]



[Source: ISO/IEC 38500:2015]

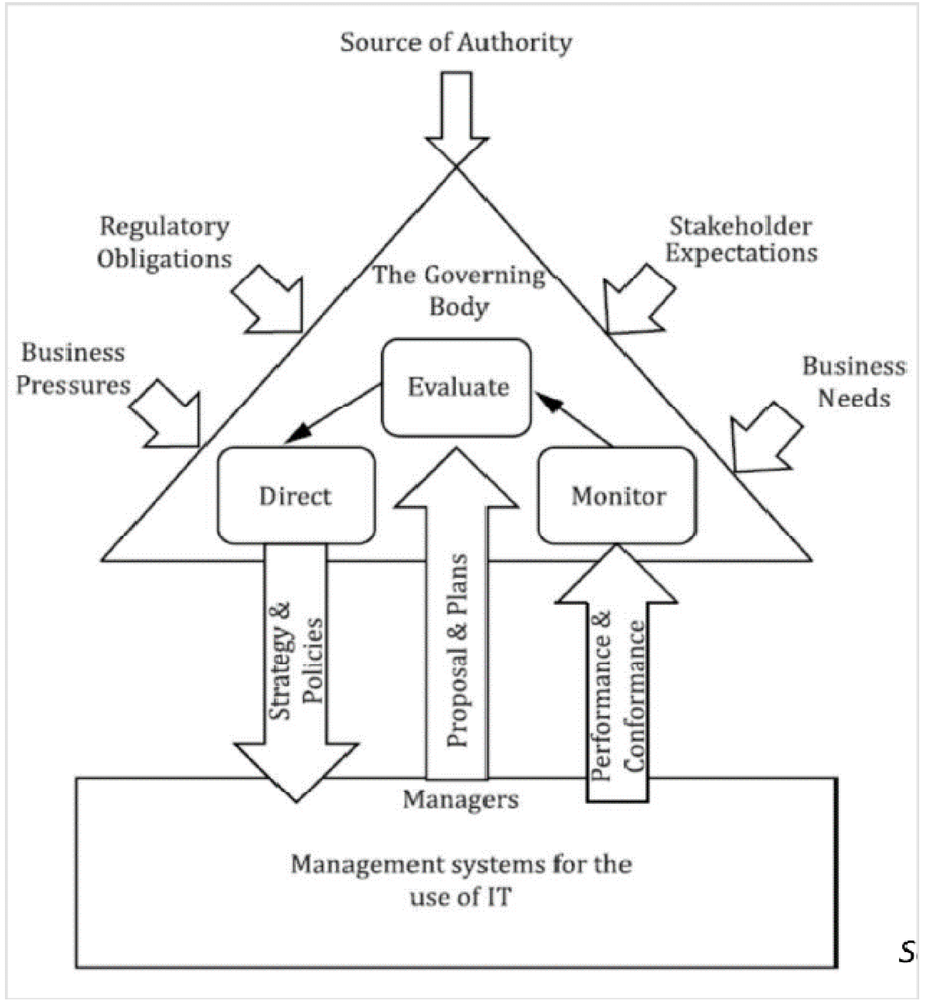
ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

PRINCIPLE 6—HUMAN BEHAVIOUR

The implementation of any IT-enabled change, including IT governance itself, usually requires significant cultural and behavioural change within enterprises as well as with customers and business partners.

[Source: COBIT 5 framework - isaca.org]



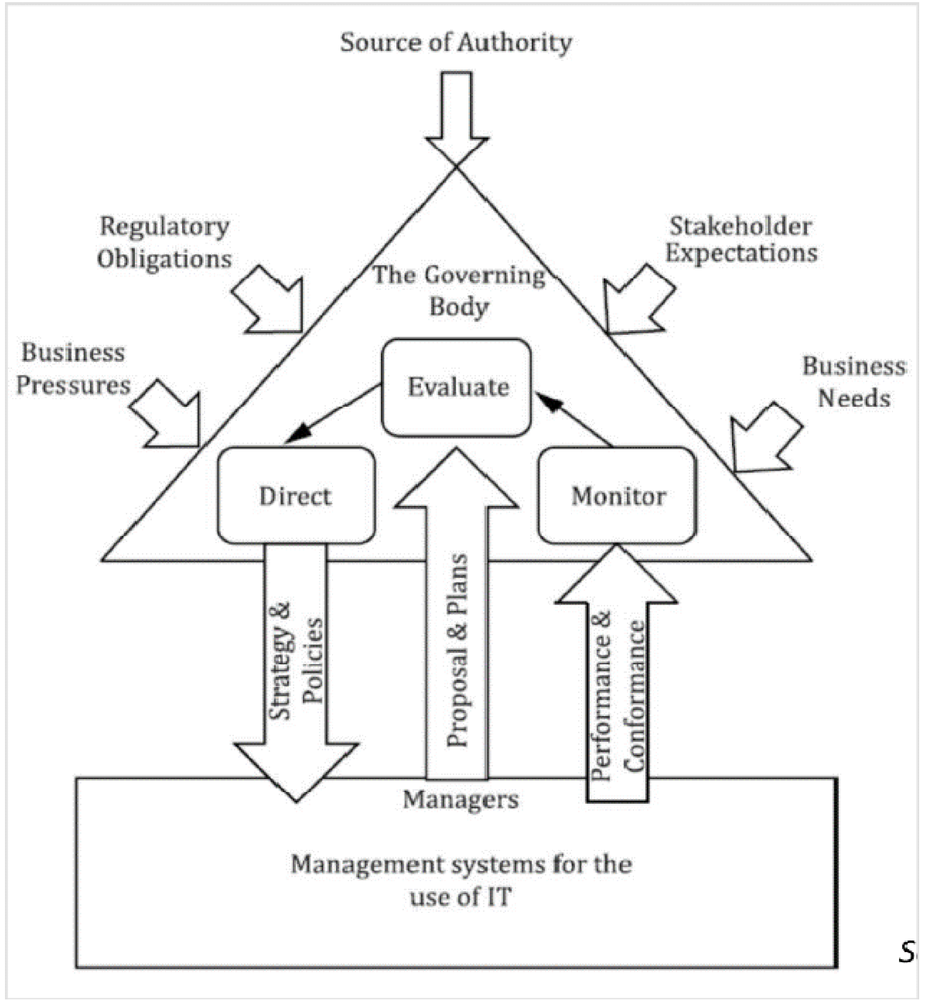
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

People are affected by IT **at all level**s in an enterprise, as stakeholders, managers and users, or as specialists providing IT-related services and solutions to the business. Beyond the enterprise, IT affects customers and business partners and increasingly enables self-service and automated intercompany transactions within countries and *across borders*.

[Source: COBIT 5 framework - isaca.org]



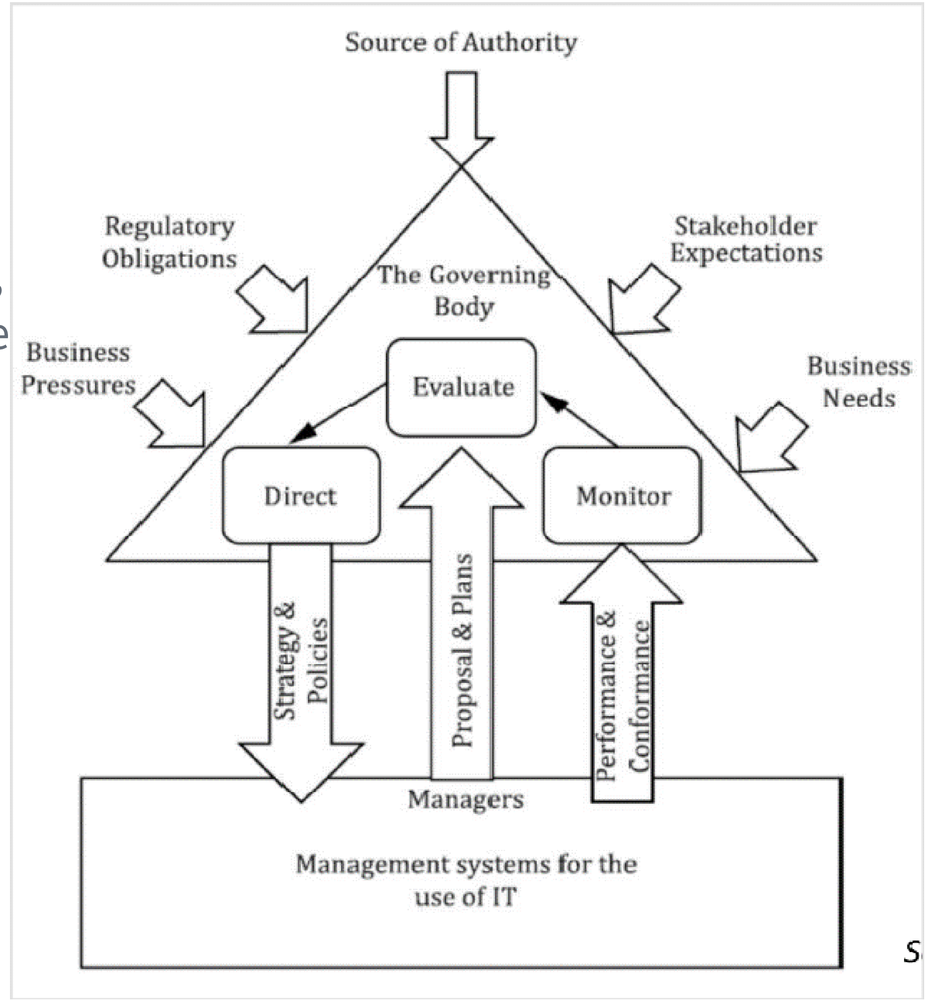
[Source: ISO/IEC 38500:2015]

ISO/IEC 38500:2015

INFORMATION TECHNOLOGY — GOVERNANCE OF IT FOR THE ORGANIZATION

While IT-enabled business processes bring new benefits and opportunities, they also carry increasing types of **risk**. Issues such as *privacy* and *fraud* are growing concerns for individuals, and these and other types of risk need to be managed if people are to trust the IT systems they use. Information systems can also *dramatically affect* working practices by automating manual procedures.

[Source: COBIT 5 framework - isaca.org]



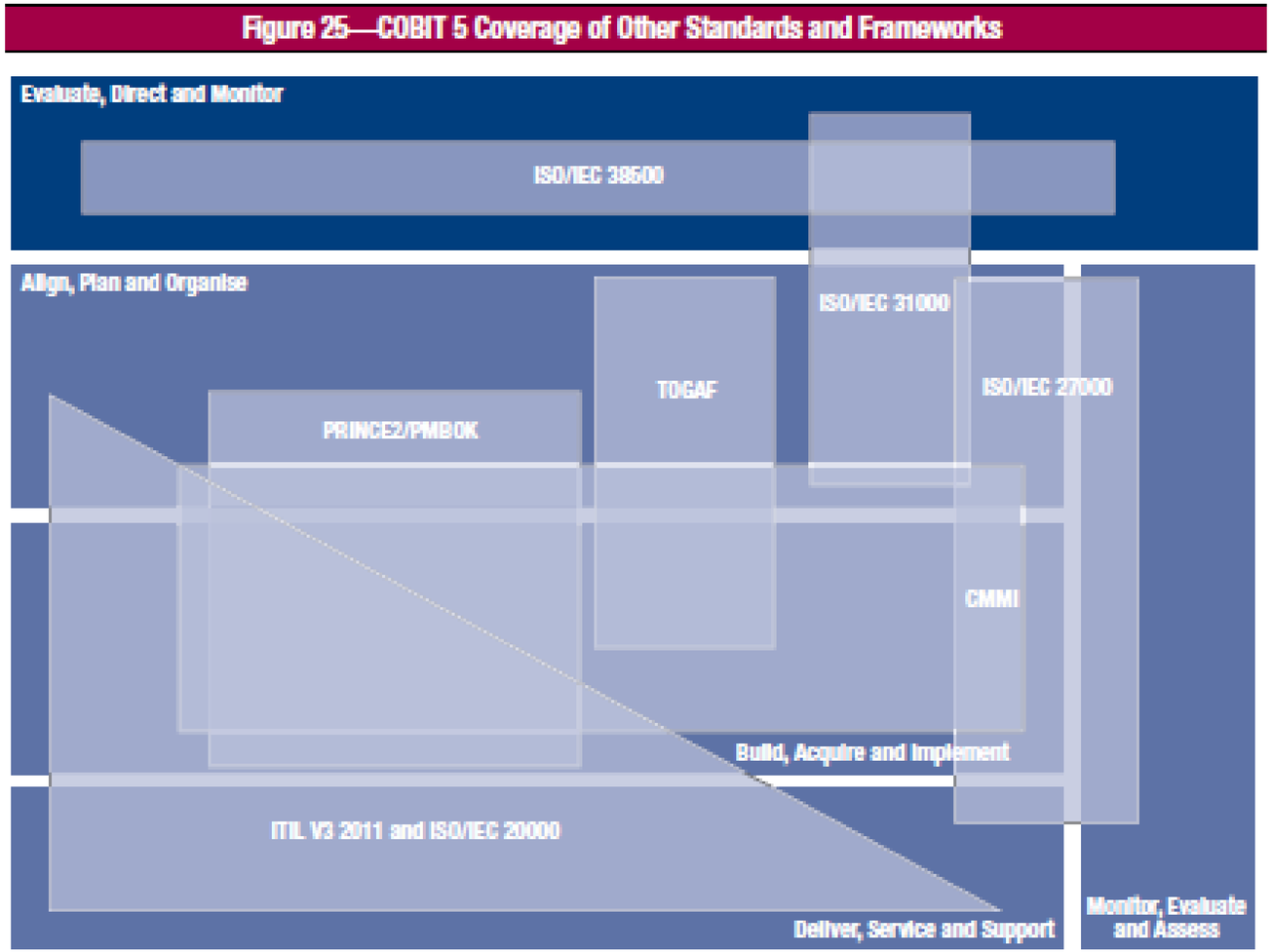
[Source: ISO/IEC 38500:2015]

Cobit 5 coverage of other Standards and Frameworks

COBIT 5 was developed taking into account a number of other standards and frameworks.

- TOGAF for modeling the overall structure of the system and its components;
- ITIL for IT Service Management;
- **ISO27000 family for information security;**
- **ISO31000 for risk management;**
- PMBOK for project management and control.

[Source: COBIT 5 framework - isaca.org]



IT Governance and Management certifications (ISACA - COBIT)

COBIT 5 Assessor
Demonstrates *mastery* in understanding and performing a formal Process Capability Assessment. Holders ensure stronger, more reliable control over internal processes and provide stakeholders a clear line of sight into process capabilities, allowing IT leaders to redirect or liberate resources—from service delivery to designing and implementing technology-enabled, information-rich and transformed business process – to increase innovation and value for the enterprise.

[Source: isaca.org]

IT Governance and Management certifications (ISACA - COBIT)

COBIT 5 Foundation
Affirms holders' understanding of COBIT principles and concepts. Holders understand the IT management issues organizations face today and know how to use COBIT to respond to these challenges. These professionals have used the elements of COBIT, in practice, and are prepared to recommended applications of COBIT for enterprise-wide projects.

[Source: isaca.org]

IT Governance and Management certifications (ISACA - COBIT)

The COBIT Foundation Certificate Exam ensures that you understand:

- How to align IT goals with strategic business objectives using tools designed to give governance a *wider* perspective, and practitioners more flexibility.

- The value derived from IT, necessary resources, and potential risks in the process of building a *mature* relationship between the business and IT.

- The *different* types of IT governance frameworks such as ITIL, NIST etc., including the benefits of each and how they work

[Source: isaca.org]

IT Governance and Management certifications (ISACA - COBIT)

COBIT 5 Implementation
Confirms holders' ability to understand and apply the elements of COBIT 5 across an enterprise. These professionals have mastered the approach to implementing the "Governance of Enterprise Information Technology or (GEIT)" based on a continual improvement life cycle. These professionals have demonstrated the understanding of how COBIT 5 should be tailored to suit an enterprise's specific needs.

[Source: isaca.org]

IT Governance and Management certifications (ISACA - COBIT)

IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK USING COBIT 5

Showcases the holder's understanding of the goals and content of the **Cybersecurity Framework** (CSF) and *how to apply the seven Cybersecurity Framework implementation steps using COBIT*. In order to obtain this credential, professionals must be able to show that they have successfully completed the COBIT 5 *Foundation* Exam.

[Source: isaca.org]

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M10 Most common Certifications available on the market