**CIS 4402: IT Governance**

Definitions

- Governance -gov·er·nance noun (ˈgə-vər-nən(t)s) the way that a city, company, etc., is controlled by the people who run it

- Corporate governance: The structure and the relationships which determine corporate direction and performance.

* The board of directors is typically central to corporate governance – accountable to shareholders
* Participants include: management, employees, customers, suppliers, and creditors
* Depends on the legal, regulatory, and culture of the community

Information technology governance (ITG):

“The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.” © 2010 Gartner, Inc.

“A decision-making framework for IT investments that is designed to maximize the return of benefits while managing risk to acceptable levels.” © 2010 Forrester Research, Inc.

“The system by which the current and future use of IT is directed and controlled. Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization.” © International Organizations for Standardization (ISO).

“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.” © ISACA (COBIT5®).

IT Governance Institute – more definitions

*1998 Definition*: The responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extends the organization’s strategies and objectives. © IT Governance Institute.

*Today’s Definition*: A governance system enables multiple stakeholders in an enterprise to have an organized say in evaluating conditions and options, setting direction and monitoring performance against enterprise objectives. Setting and maintaining the appropriate governance approach is the responsibility of the board of directors or equivalent body. © IT Governance Institute.

**IT Governance & IT Management Issues**

IT governance and corporate governance are interrelated; IT governance is an integral part of corporate governance. For this reason, many issues and concepts discussed in corporate governance are also involved in IT governance. These include

* IT risk management.
* The establishment of a governance framework.
* A sense of teamwork and of enterprise.
* Value delivery through IT.
* A more activist information security department and board of directors.
* Cloud computing.
* Continuous auditing and assurance.

1. *IT Risk management*

Successful organizations that manage to derive business value out of IT investments also understand the importance of IT control environment and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on IT. This in particular means that they manage the risks associated with growing IT opportunities. The risks associated with business processes conducted through IT support are not only anymore marginal or ‘technical’ problems and become more and more a key ‘business problem’.

IT risks are risks associated with intensive use of IT to support and improve business processes and business as a whole. They are related to threats and dangers that the intensive use of IT may cause undesired or unexpected damages, misuses and losses in whole business model and its environment. Conscience about the systematic IT risk management should be present at all managerial level in organizations whose business is in any way related to the functioning of modern information systems (IS), no matter if they are used only for the purpose of business automation, or some vital business process are performed electronically. Since the efficiency, effectiveness and in a great deal the successfulness of all business activities depend on the functioning of the IT and IS, a sound risk management process should not only include technical or operational issues but also executive management’ frameworks such as IT Governance and IT Audit.

IT Risks represent the likelihood that in certain circumstances a given threat-source can exercise a particular potential vulnerability and negatively impacts the IT assets (data, software, hardware), IT services, key business processes or the whole organization.

*IT Risks = F (asset, threat, vulnerability)*

Quantitative risk assessment draws upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, business processes, recovery costs, etc., impact, and therefore risk, can be measured in terms of direct and indirect costs. Mathematically, quantitative risk can be expressed as Annualized Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realized over a one-year period

ALE = SLE \* ARO

where:

SLE (Single Loss Expectancy) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss. ARO (Annualized Rate of Occurrence) is how often the loss occurs. This is the likelihood or the number of occurrences of the undesired event.

1. *IT Governance framework*

All organizations need to make a decision on the IT governance framework to adopt. These include:

* CobiT (Control Objectives of Information and related Technology),
* ISO 38500:2015
* ITIL (IT Infrastructure Library)

The main objective of all frameworks is to align IT to the organization, create value and control.

1. *Sense of teamwork and of enterprise*

* an organization with a cultural focus on results and teamwork tends to implement simple structures of IT governance and simple decision-making processes, uses more efficiently their IT resources and integrates better its organizational knowledge
* In organizations that value individual work, there is less teamwork, the structures are more complex and the decision-making will be more difficult, slow and bureaucratic. This type of culture causes less participation of business executives in the IT governance model, less interaction between areas and different resources and therefore less optimized IT resource management
* worker participation, supervision, feedback, rewards, formalization and work rules have an impact on IT governance resource planning
* three dimensions of organizational culture called strategy, coordination and leadership, have a strong relationship with governance in the business IT alignment maturity. Likewise, aspects of organizational culture like innovation, risk taking, team orientation, and change readiness have a significant impact on the strategic alignment components

1. *Value delivery*

Growing need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as key elements of enterprise governance. Value, risk and control constitute the core of IT governance.

1. *Information security department and board of directors*

From IT Governance, IT Audit and IT Security perspective, IT risk management is the process of understanding and responding to factors that may lead to a failure in the authenticity, non-repudiation, confidentiality, integrity or availability of an information system. Attainment of security needs to be one of the targets set by the board of directors. It can be attained by implementation of ISO 27000:2013

1. *Cloud computing.*
2. *Continuous auditing and assurance*

Periodic internal or external IT audits are needed to detect the level of compliance with standards and regulatory frameworks. Performing IT audits are necessary in order to detect the priority risk areas, to identify specific IT controls needed, to constantly measure the level of their efficiency and to calculate IT risk level on regular basis

**IT Governance Frameworks/Authorities**

IT Governance Frameworks/Authorities include

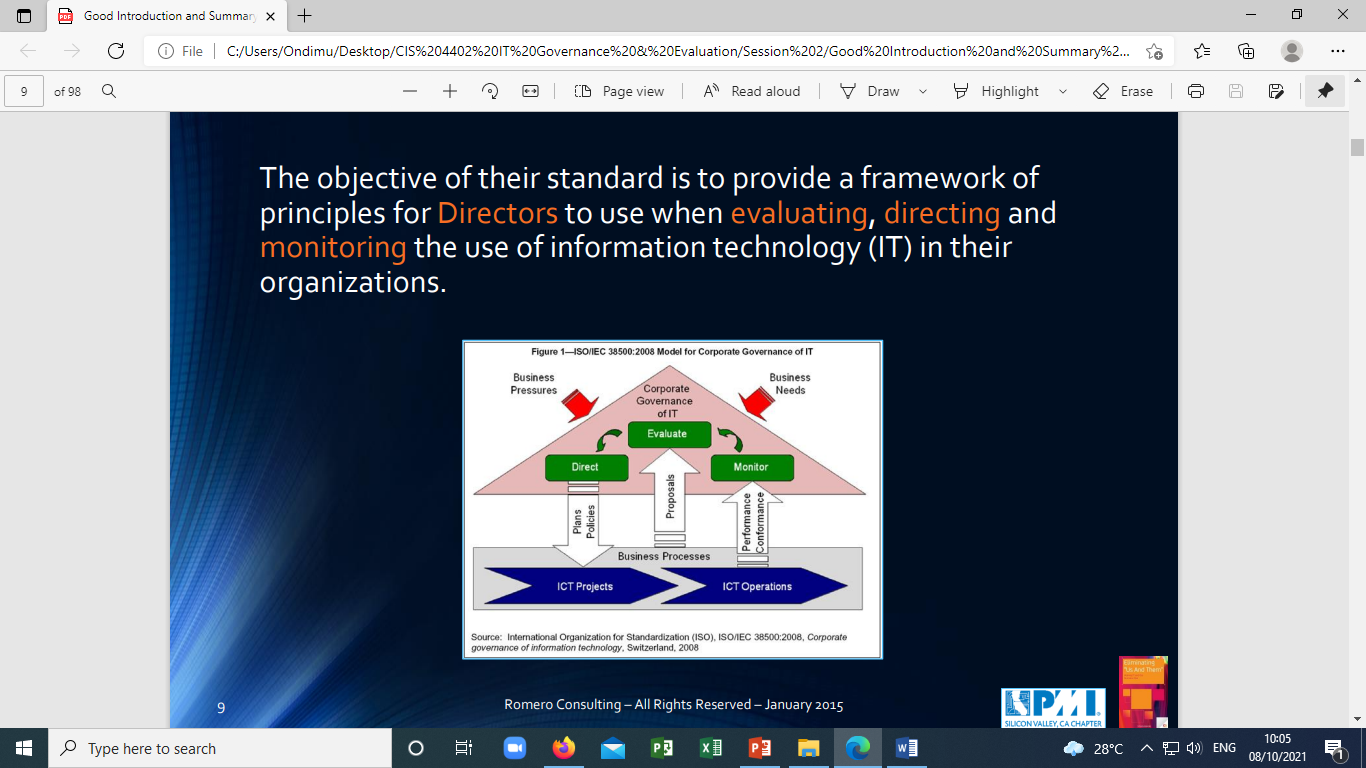
* International Standards Organization/ International Electrotechnical Commission (ISO/IEC)
* Information Systems Audit and Control Association (ISACA)

1. **The ISO/IEC IT Governance Standard**

ISO/IEC 38500 is a high level, principles based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of IT.

(ISO 38500 definition: - The system by which the current and future use of IT is directed and controlled. Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization.

The objective of their standard is to provide a framework of principles for Directors to use when evaluating, directing and monitoring the use of information technology (IT) in their organizations.



The ‘other’ objectives of ISO/IEC 38500

Proper corporate governance of IT may assist directors in assuring conformance with obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of IT.

Inadequate IT systems can expose the directors to the risk of not complying with legislation. For example, in some jurisdictions, directors could be held personally accountable if an inadequate accounting system results in tax not being paid.

ISO/IEC 38500A is a standard rooted in risk aversion. Processes dealing with IT incorporate specific risks must be appropriately addressed. For example, directors could be held accountable for breaches of:

* security standards
* privacy legislation
* spam legislation
* trade practices legislation
* intellectual property rights
* record keeping requirements
* environmental legislation and regulations
* health and safety legislation
* accessibility legislation
* social responsibility standards

ISO/IEC 38500 is based on meeting six principles

* *Responsibility* – Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
* *Strategy* –The organization’s business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization’s business strategy.
* *Acquisition* – IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
* *Performance* – IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.
* *Conformance* – IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
* *Human Behavior* – IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the ‘people in the process’.

*ISO/IEC 38500 Governance Model*

IT is governed through 3 main tasks

* Evaluate the current and future use of IT.
* Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.
* Monitor conformance to policies, and performance against the plans

“In ISO’s view, governance is distinct from management, and for the avoidance of confusion, the two concepts are clearly defined in their standard.”

1. **Control Objectives for Information and Related Technology (COBIT) Framework**

COBIT® 2012 – An ISACA framework

* COBIT®5 is a foundational enterprise IT Governance framework, providing a basis to effectively integrate other complimentary frameworks, standards, and practices.
* As a single overarching framework it serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic, common language.

Scope of COBIT®5

* COBIT®5 addresses the governance and management of information and related technology from an enterprise-wide, end-to-end perspective, including the activities and responsibilities of both the IT function and non-IT business functions.
* The end-to-end aspect is further supported by COBIT®5 coverage of all critical business elements, e.g. processes, organizational structures, principles & policies, culture, skills, information, service capabilities.

IT governance according to COBIT®

*Governance*

• Ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions, and options

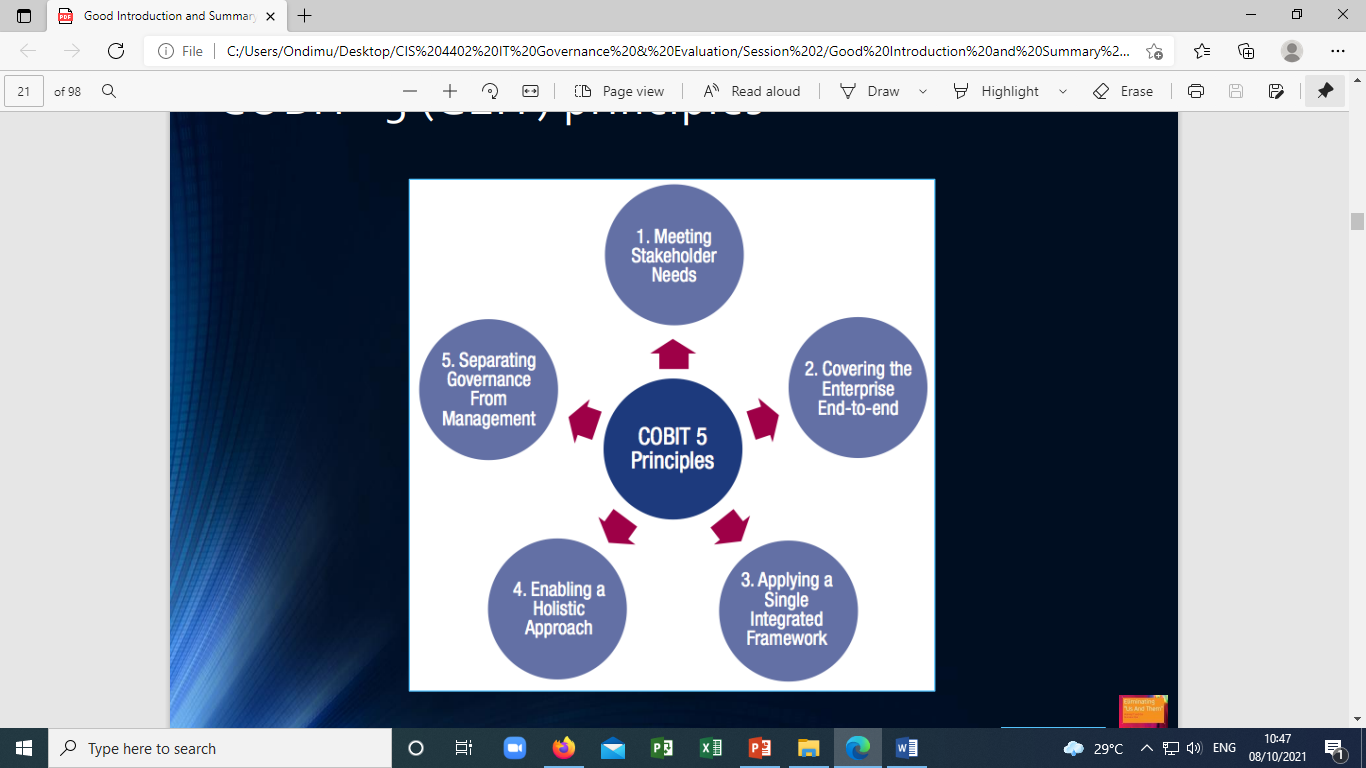
• Sets direction through prioritization and decision making

• Monitors performance, compliance, and progress against the agreed upon direction and objectives

*Management*

• Plans, builds, runs, & monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives

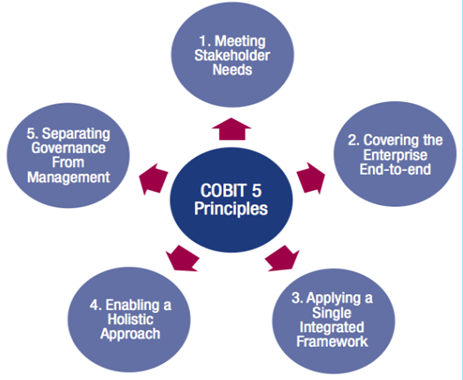
COBIT®5 (GEIT) principles COBIT



1. Meeting stakeholder needs
2. Covering the enterprise end-to-end
3. Applying a single integrated framework
4. Enabling a holistic approach
5. Separating governance from Management

COBIT and ISO/IEC standards have dissimilar IT governance principles

COBIT 5 ISO 38500



• Responsibility

• Strategy

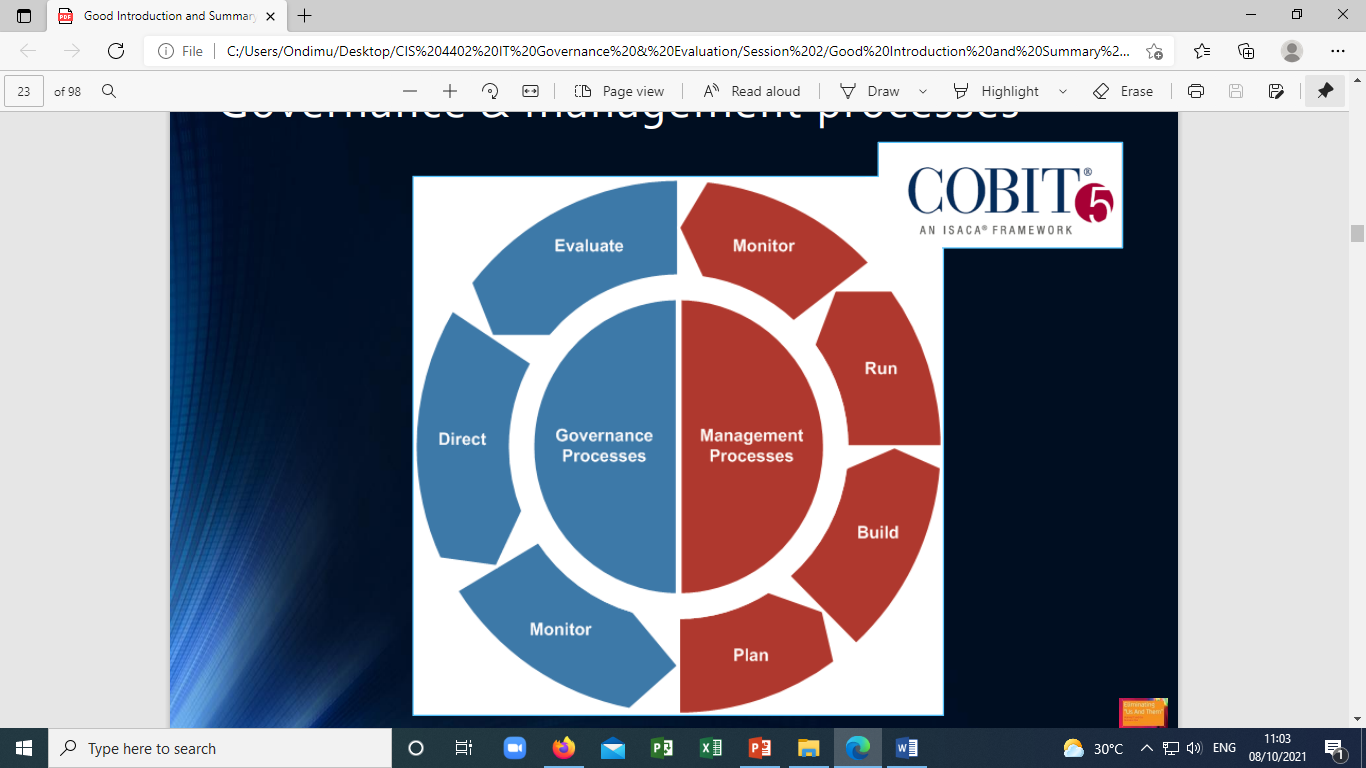
• Acquisition

• Performance

• Conformance

• Human Behavior

Governance & management processes



Principle 5: Separating governance & mgt.

Process reference model: Divides governance and management processes into two primary domains:

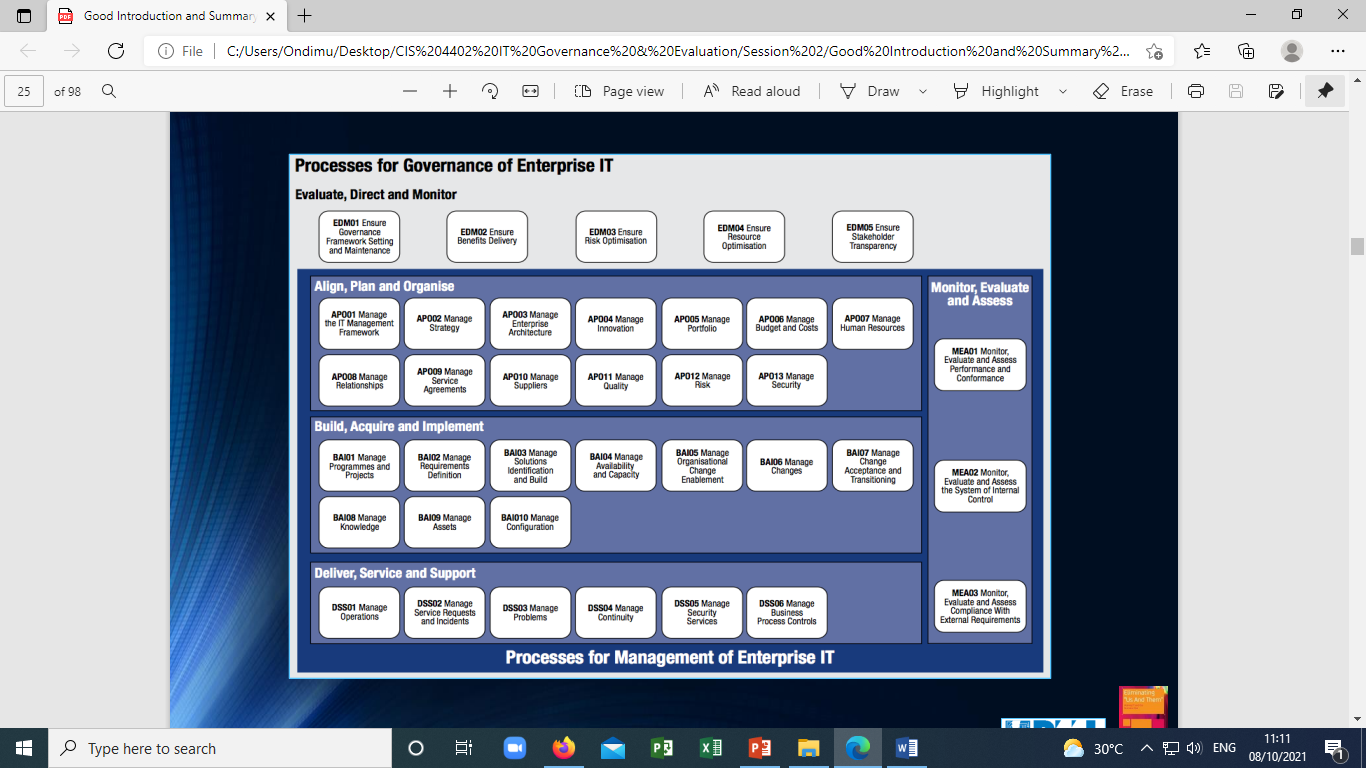
• Governance (1 Domain, 5 Processes)

* Within each process, evaluate, direct, and monitor practices are defined.

• Management (4 Domains, 32 Processes)

* In line with responsibility areas of plan, build, run, and monitor, provide an end‐to‐end coverage of IT Management. The processes cover the full spectrum of business and IT activities related to governance and management of enterprise IT thus making the process model truly enterprise wide

COBIT® Process reference model



COBIT Governance Processes

Governance Domain – evaluate, direct, and monitor

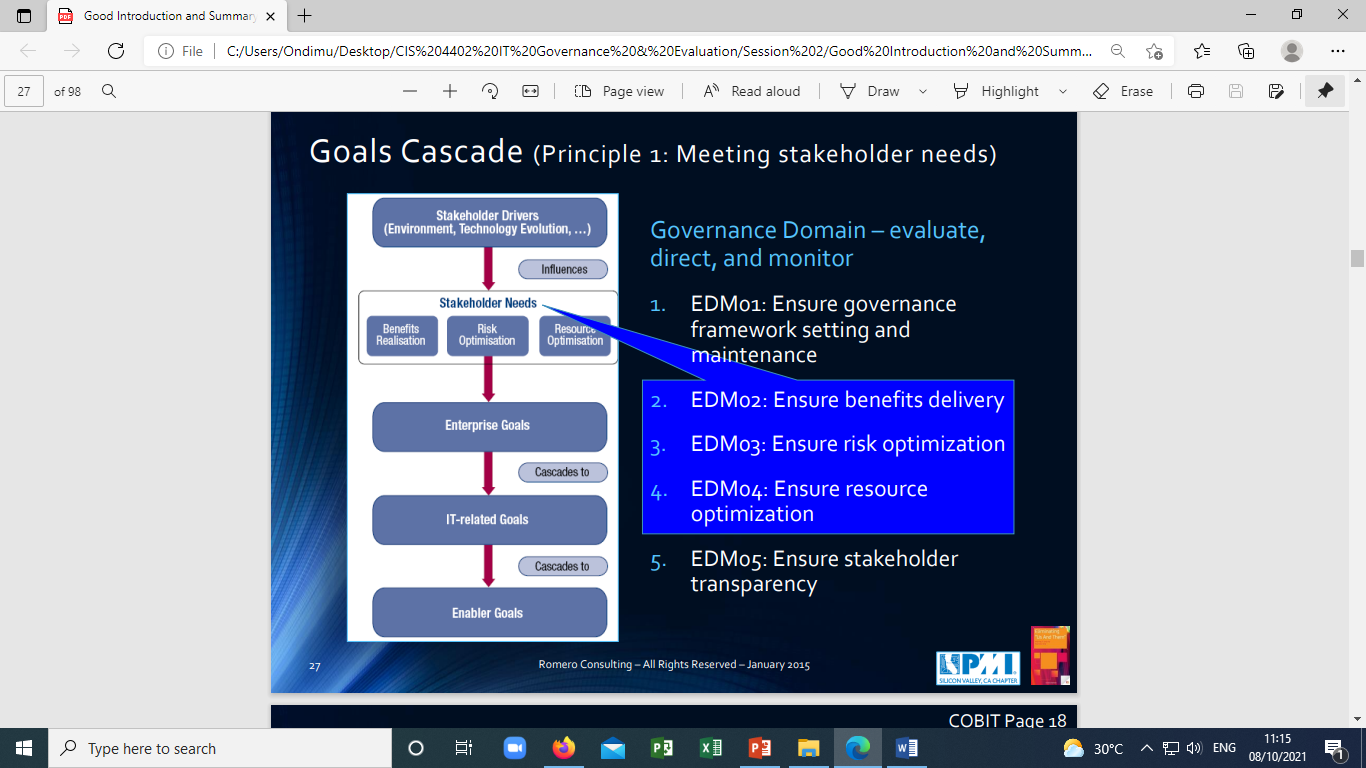
1. EDM01: Ensure governance framework setting and maintenance

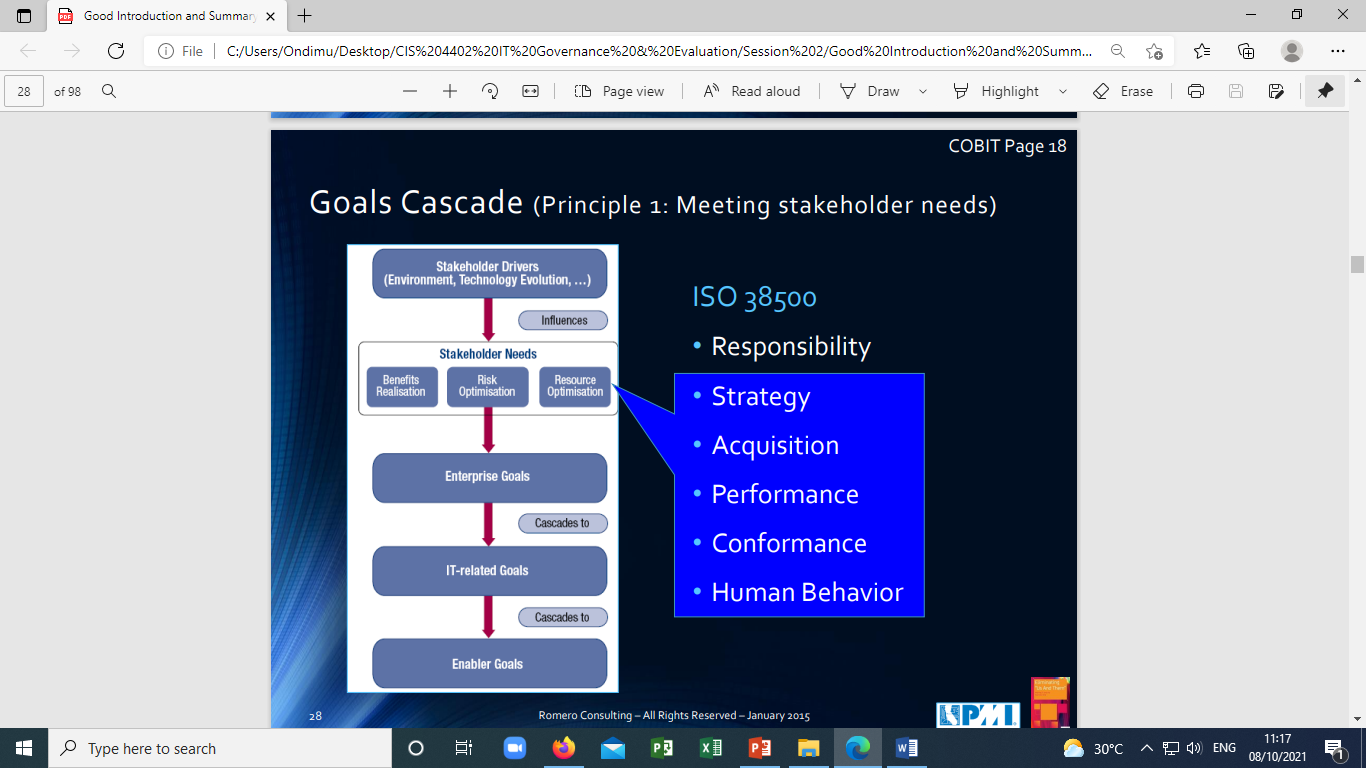
2. EDM02: Ensure benefits delivery

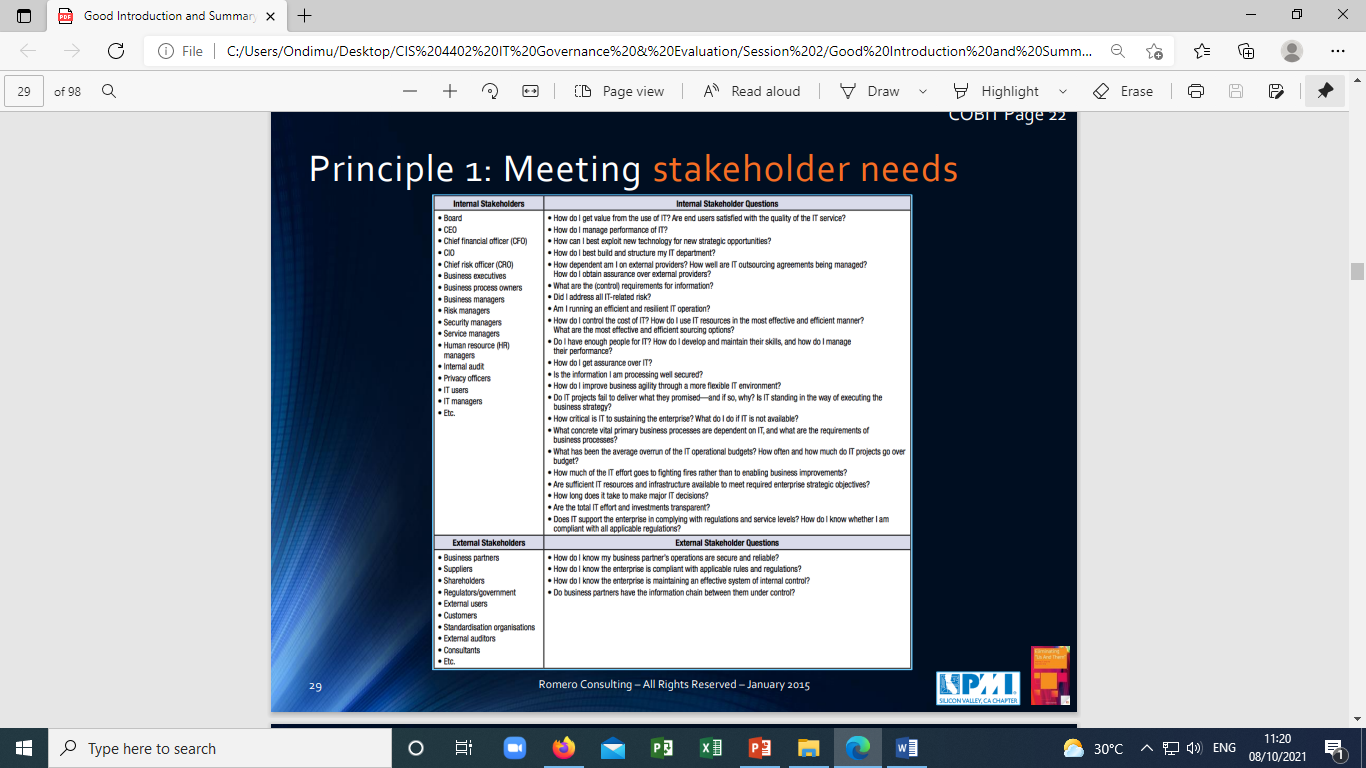
3. EDM03: Ensure risk optimization

4. EDM04: Ensure resource optimization

5. EDM05: Ensure stakeholder transparency COBIT Governance Processes







Principle 2: Covering enterprise end-to-end

• Governance Enablers (Principle 4)

• Frameworks, principles, structures, processes, practices

• Governance Scope - definable

• Enterprise, entity, or tangible asset

• Roles, activities and relationships

