www.andrewsai.com

IT Governance in COBIT Framework

Andrew Sai, CIMA Adv Dip MA, PhD candidate

Plan for Today

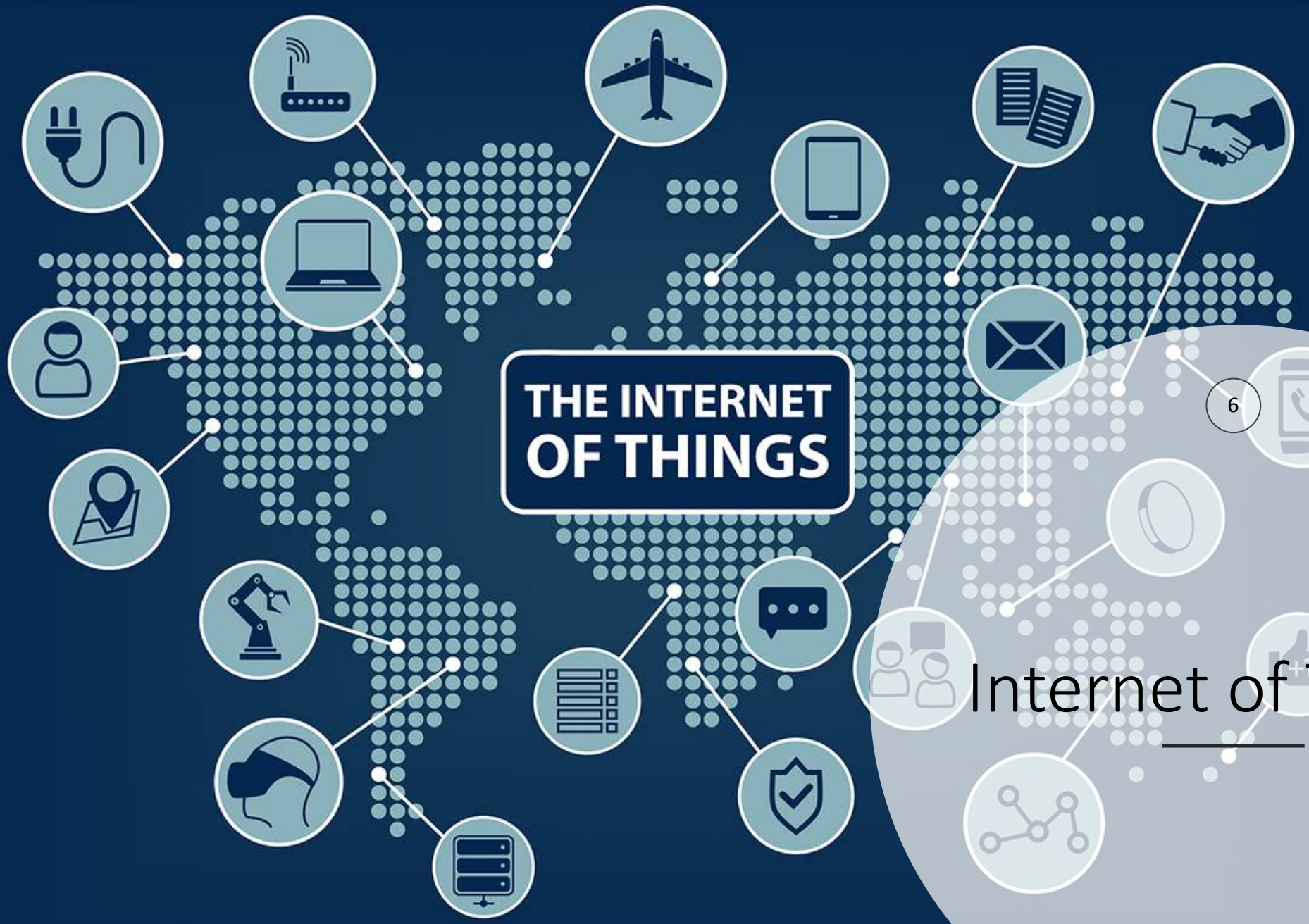
- ❑ IT Today
- ❑ Governance and Management
- ❑ IT Governance
- ❑ ISO38500: Corporate Governance of Information Technology
- ❑ Cobit 5 Framework
  - ❑ COBIT 5 Principles and Enablers
- ❑ Compliance in COBIT 5. Sarbanes–Oxley Act of 2002
- ❑ Risk Management and Governance in COBIT 5
- ❑ Governance, Risk Management, and Compliance (GRC)
- ❑ Instead of Summary
- ❑ Appendix

***Short Break* (10 mins)**

Knowledge check

1. IT Today


DIGITAL
TRANSFORMATION



Internet of Things


BIG DATA

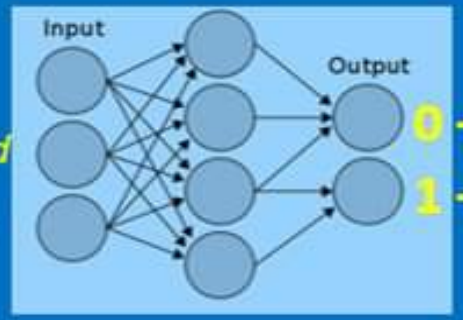
ARTIFICIAL INTELLIGENCE

MACHINE LEARNING

Date, time

Salary, m. spend

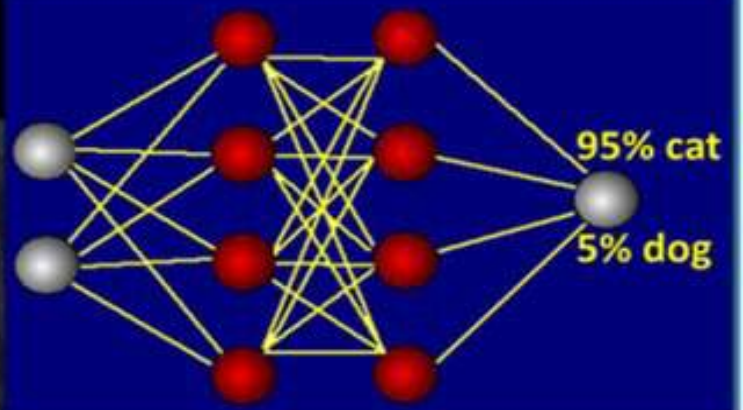
Loc. payment



0 – No Fraud

1 – Fraud

DEEP LEARNING



1950's | 1960's | 1970's | 1980's | 1990's | 2000's | 2010's


Cybersecurity

IT Potential Problems

IT systems evolve independently with no united direction or strategy

IT systems under/over-perform

IT managers don’t understand the operation

No sense of ownership on data, infrastructure and processes

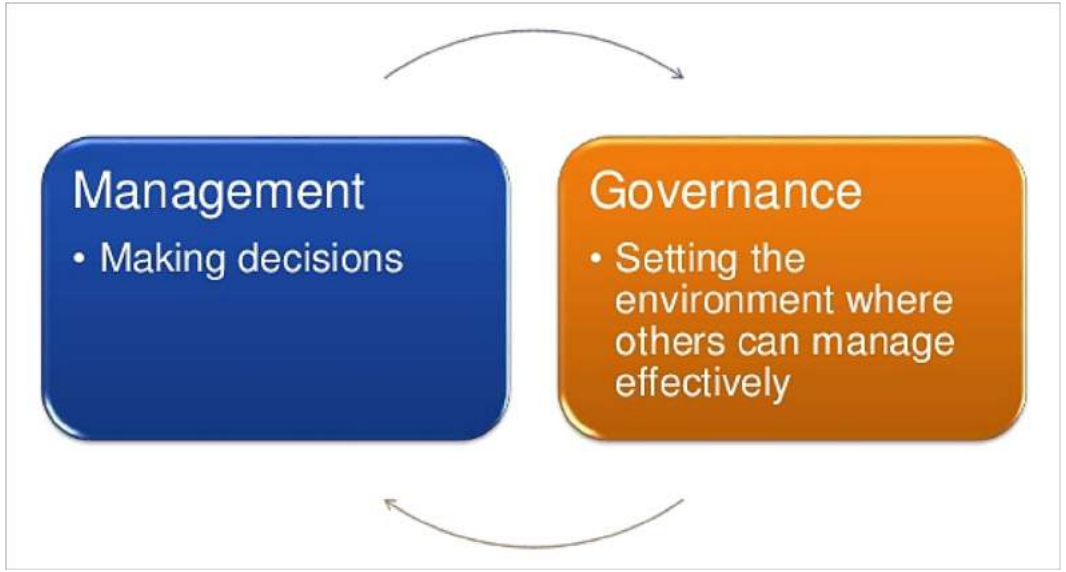
Users frustrated for, apparently, not having enough resources

IT is Critical to Most Businesses

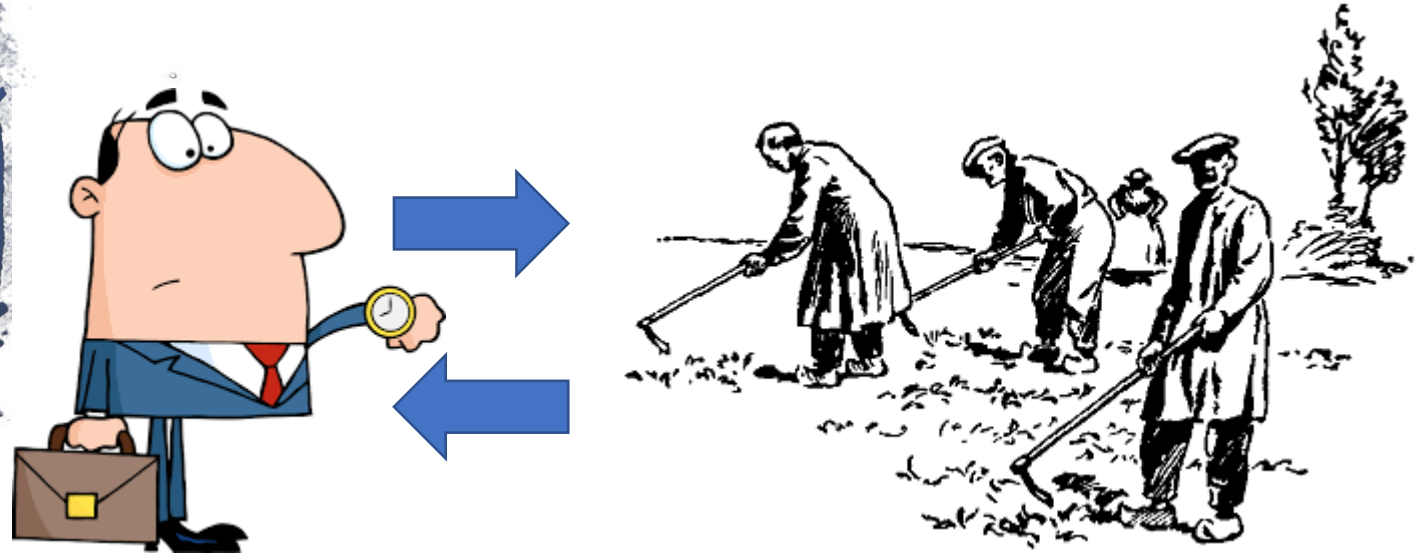
This criticality arises from:

- The increasing dependence on reliable, accurate and timely information and the systems and communications that deliver it
- The need for 24/7/365 availability to do business and to ensure customer trust
- IT failures and security breaches increasingly impacting reputation and enterprise value
- The potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs

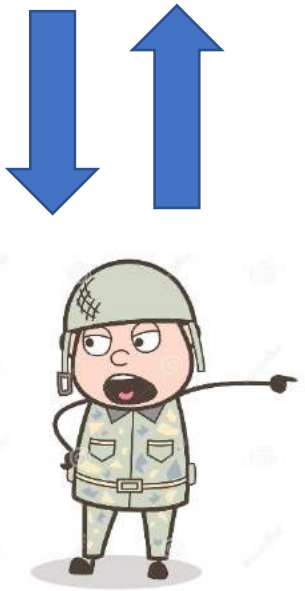
Governance and Management



Management

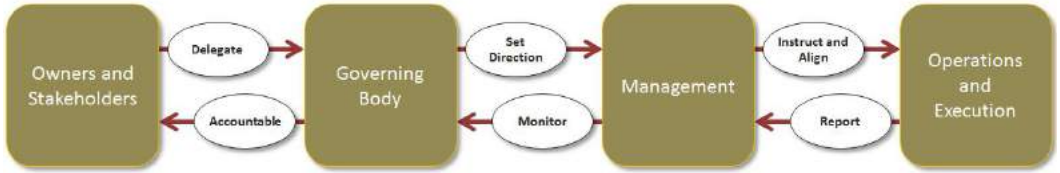


Governance & Management

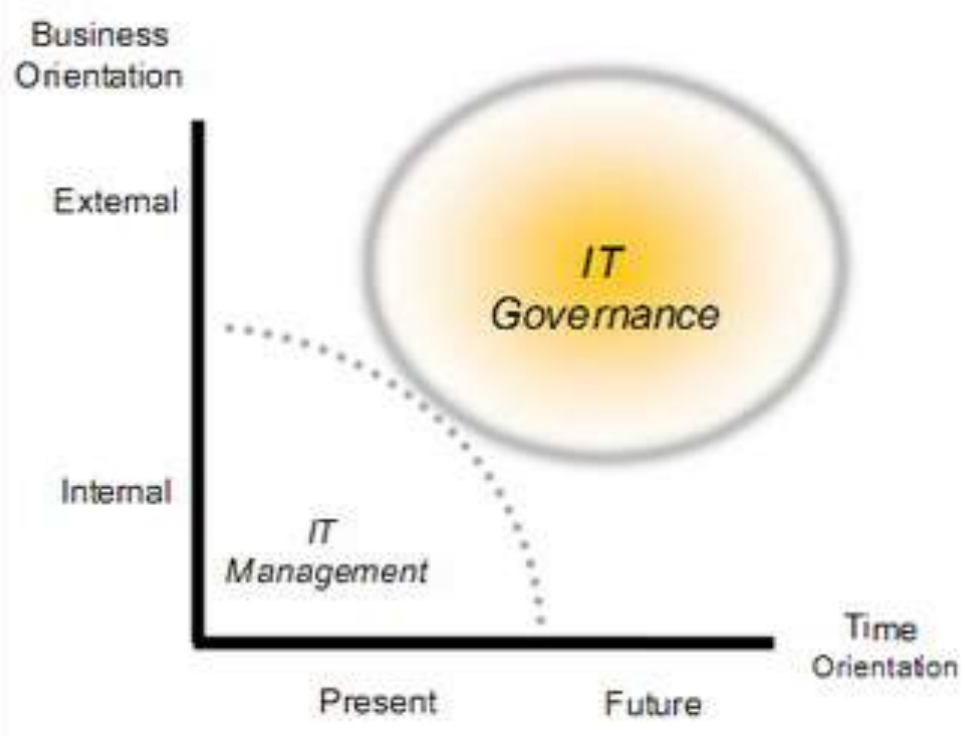


Manager

Governance and Management

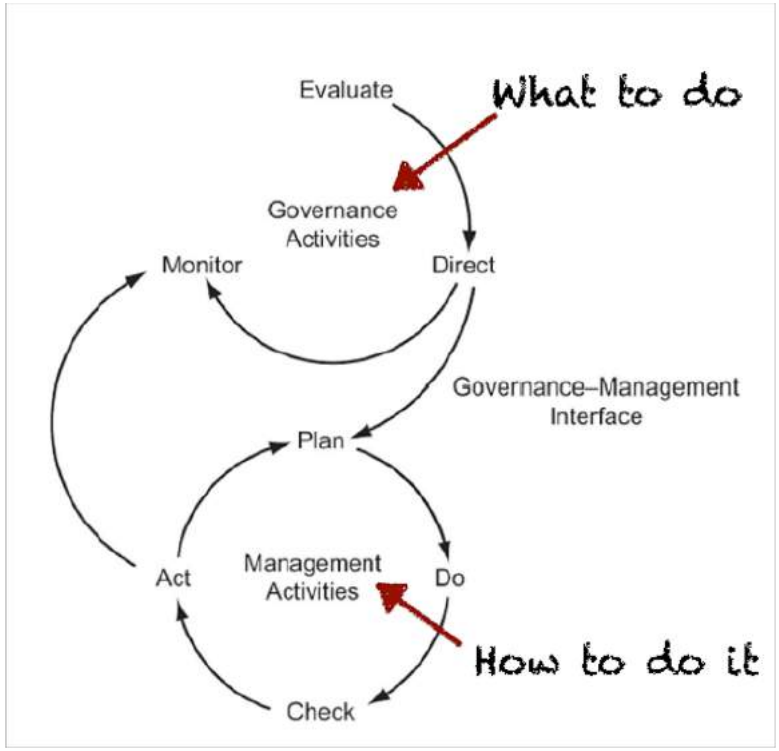


Governance and Management



Governance and Management

CORPORATE GOVERNANCE	CORPORATE MANAGEMENT
External Focus	Internal Focus
Governance assumes an open system	Management assumes a closed system
Strategy- oriented	Task-oriented
Concerned with where the company is going	Concerned with getting the company there



Governance and Management

- Governance ensures that enterprise objectives are achieved by **evaluating stakeholder needs**, conditions and options;
  setting direction through prioritisation and decision making; and **monitoring performance**, compliance and progress against agreed-on direction and objectives.
- Management **plans**, **builds**, **runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

Governance

Many definitions exist but with certain common elements, describing governance as the **policies, processes and structures used by an organisation**:

- To direct and control its activities
- To achieve its objectives
- To protect the interests of its stakeholders
- Consistent with appropriate ethical standards

The Responsibilities of the Board

The board's key functions should include:

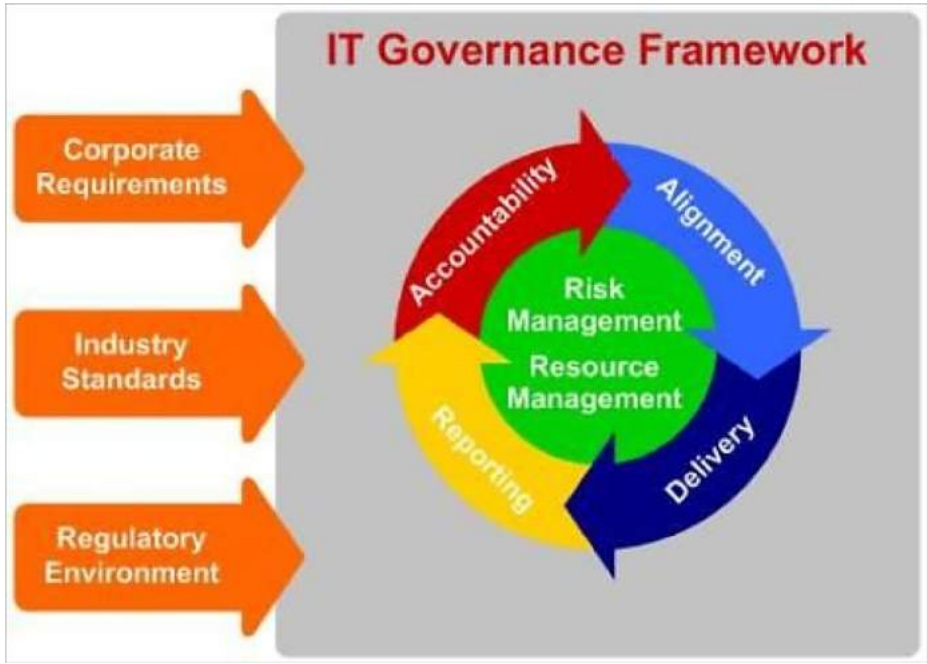
- **Reviewing** and **guiding** corporate strategy, annual budgets and business plans; setting performance objectives; monitoring corporate performance; and overseeing major capital expenditures, acquisitions and divestitures.
- **Monitoring** the effectiveness of the company's governance and risk management practices and making changes as needed.
- Selecting, compensating, monitoring and, when necessary, replacing key executives and overseeing succession planning.

Governance Elements

Governance does not exist as a set of distinct and separate processes and structures. There are relationships among governance, risk management, and internal controls:

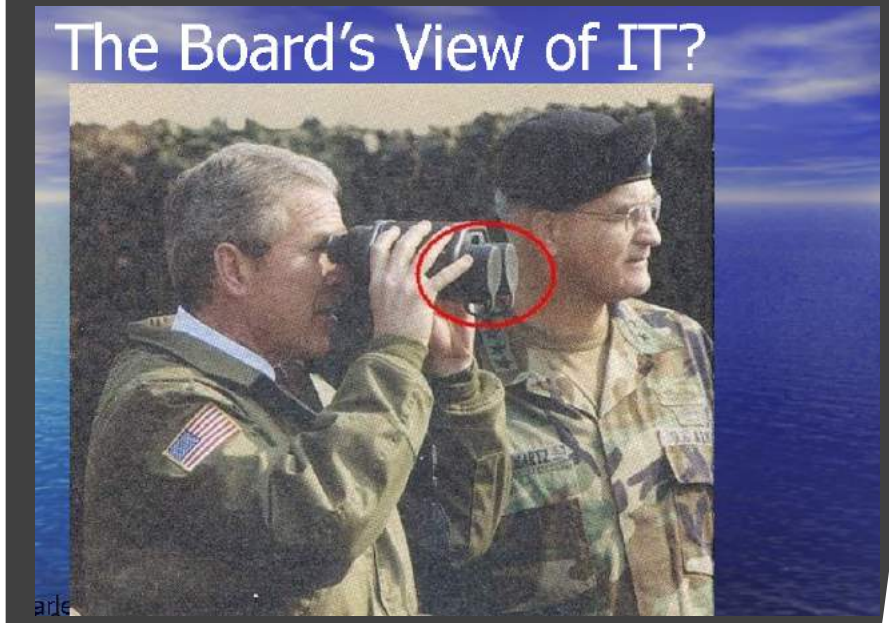
- Effective governance activities consider risk when setting strategy. Conversely, risk management relies on effective governance
- Effective governance relies on internal controls and communication to the board on the effectiveness of those controls.
- Control and risk also are related, as control is defined as “any action taken by management, the board and other parties to manage risk and increase the likelihood that established goals will be achieved.”

IT Governance




The IT aspects of corporate governance
are one of the things that chief executives
think they don't have to understand -
until it bites them!

IT Governance Problem Indicators include…….



IT NOT DIRECTLY REPRESENTED AT BOARD LEVEL

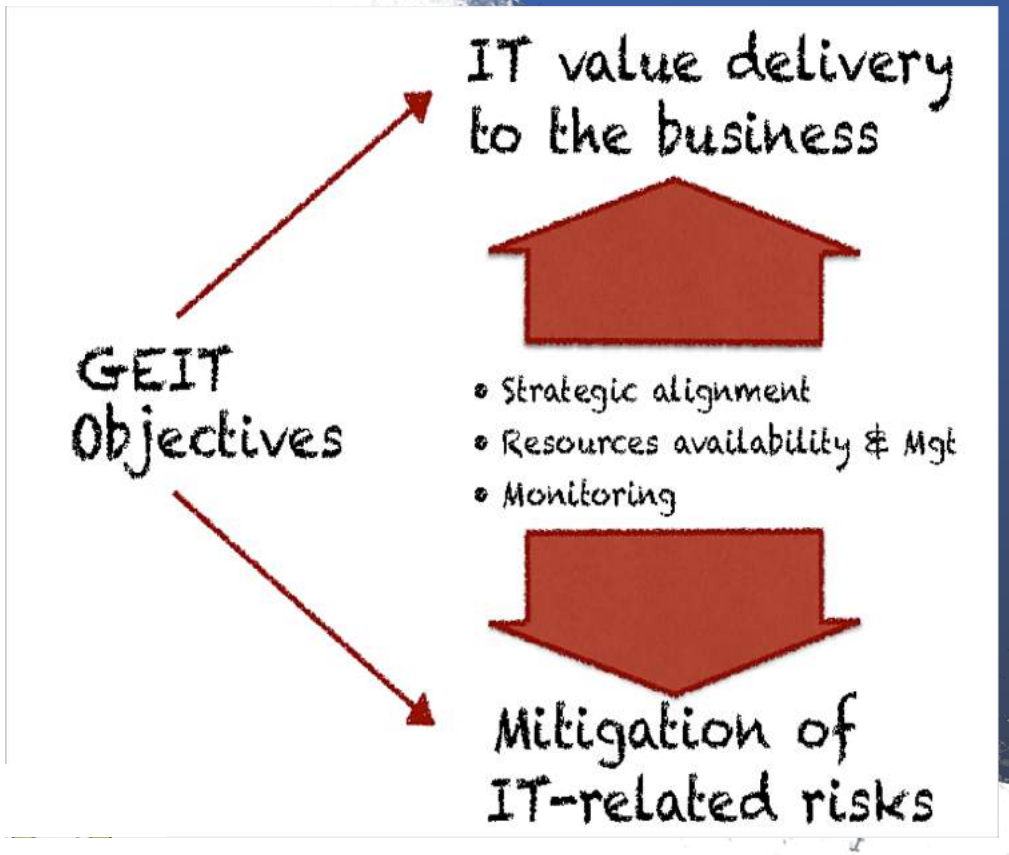
IT AND BUSINESS STRATEGY NOT CONCURRENTLY PREPARED AND ALIGNED

IT MANAGED BY TECHNOLOGY RATHER THAN BY BUSINESS FOCUS

IT SEEN AS A COST RATHER THAN AS A PROVIDER OF VALUE

INADEQUATE OR NON-EXISTENT IT RELATED METRICS

Why IT Governance?



GEIT is Governance of Enterprise IT

Why IT Governance?

IT Governance Institute (**ITGI**)

ITGI identifies **five focus areas** of GEIT:

- Strategic alignment
- Value delivery
- Risk management
- Resource management
- Performance measurement

IT Governance Definition

"Technology is a tool to accomplish business, not an end in itself"

IT Governance is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

IT governance is the responsibility of the board of directors and executive management.

by the IT Governance Institute®

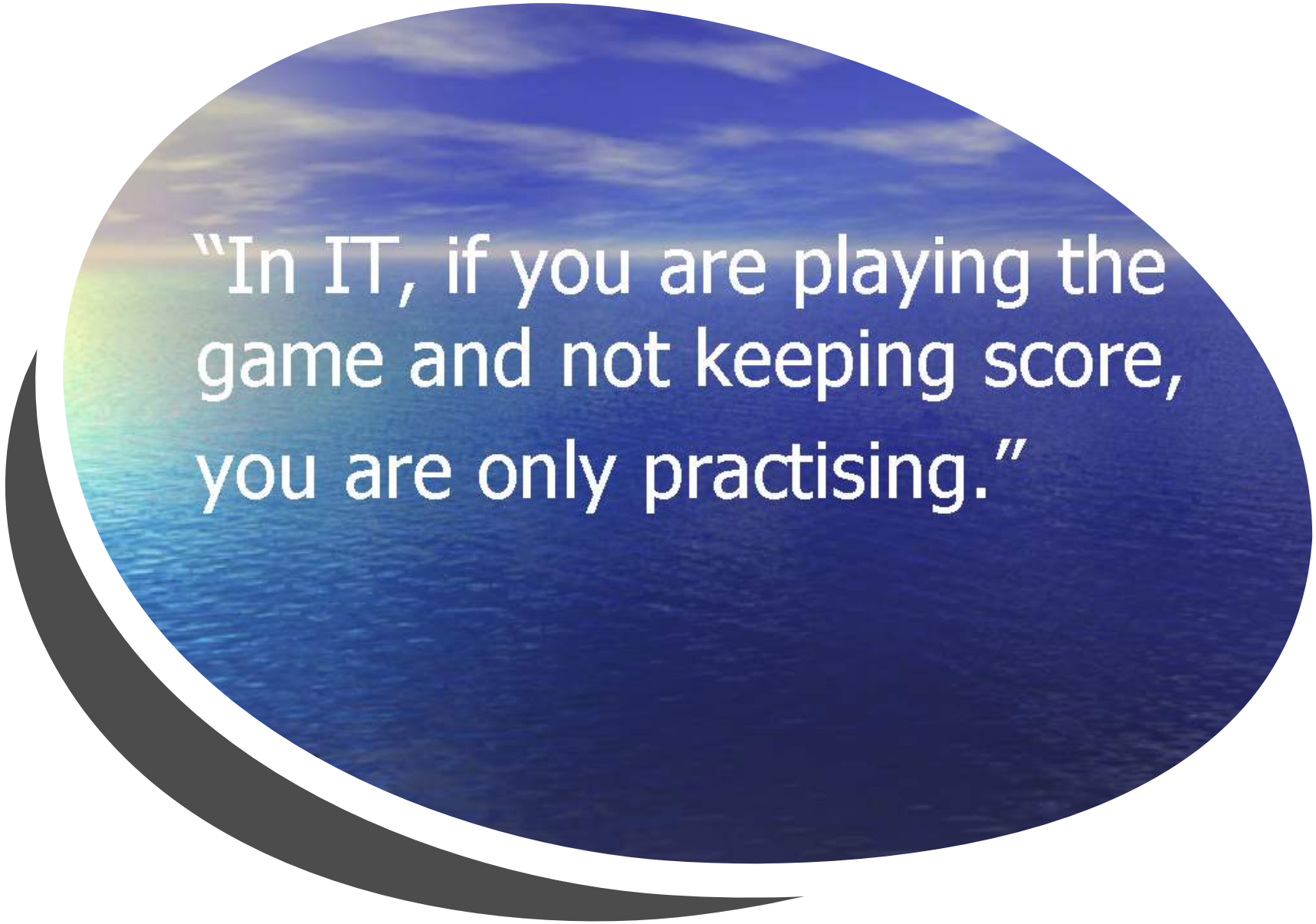
IT Governance

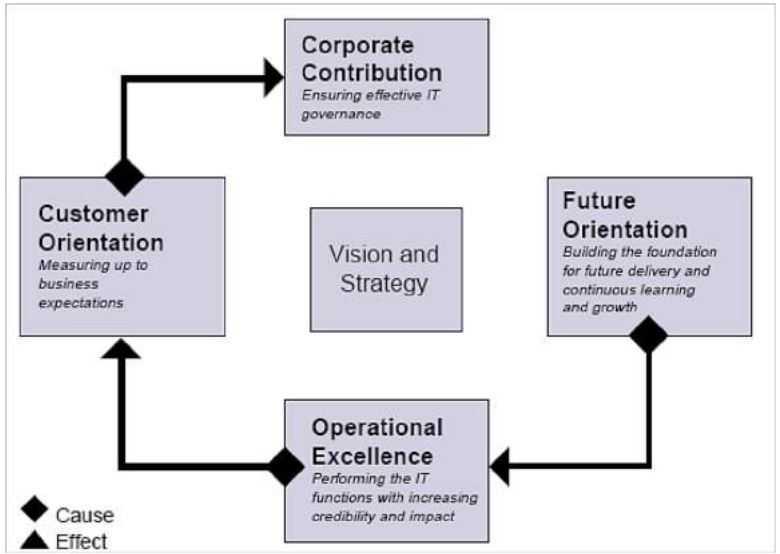
IT Governance or Corporate governance of information technology is a subset discipline of corporate governance, focused on information and technology (IT) and its performance and risk management.

The interest in IT governance is due to the ongoing need within organizations to focus value creation efforts on an organization's strategic objectives and to better manage the performance of those responsible for creating this value in the best interest of all stakeholders.

It is also very important to have an alignment of IT strategy with the business strategy.

An IT Governance framework is used to identify, establish and link the mechanisms to oversee the use of information and related technology to create value and manage the risks associated with using information and technology.


"In IT, if you are playing the
game and not keeping score,
you are only practising."



IT Balanced Scorecard

IT Governance requires a different perspective

- **Corporate contribution**—How do business executives view the IT department?
- **User orientation**—How do users view the IT department?
- **Operational excellence**—How effective and efficient are the IT processes?
- **Future orientation**—How well is IT positioned to meet future needs?

Enterprise Balanced Scorecard

P = Primary Relationship

S = Secondary Relationship

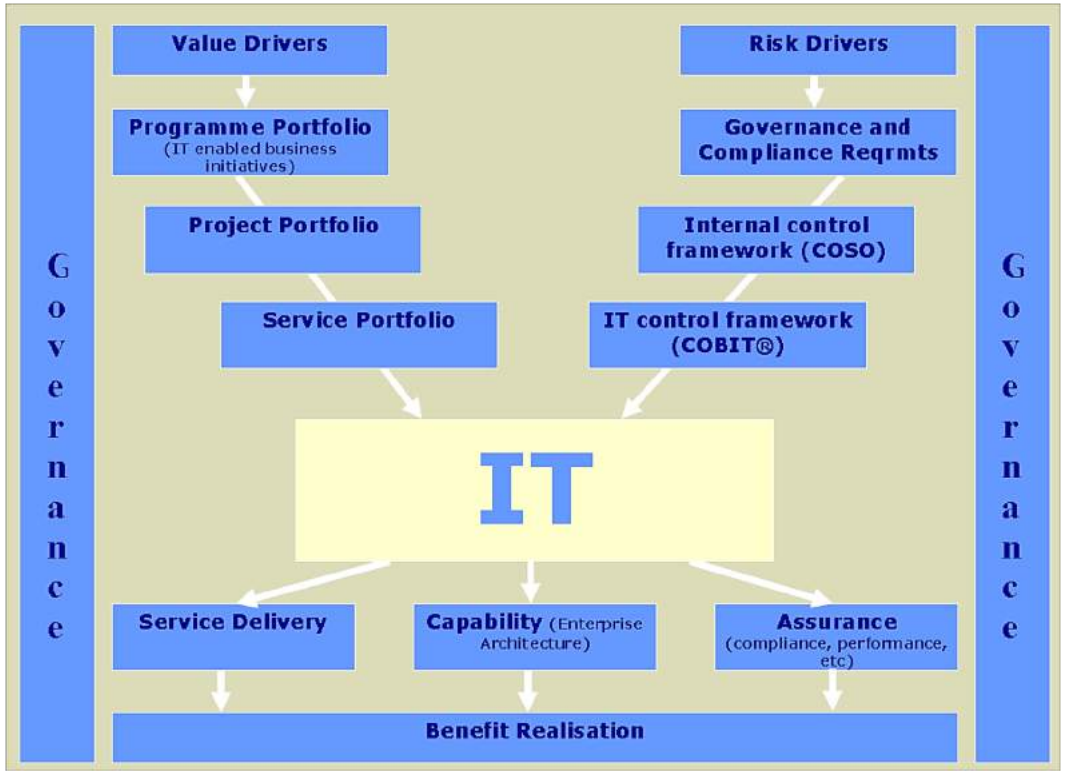
Figure 5—COBIT 5 Enterprise Goals

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

IT-Related Goals Balanced Scorecard

Figure 6—IT-related Goals		
IT BSC Dimension	**Information and Related Technology Goal**	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

IT Governance Map



Corporate Governance and ..

… IT Governance

IT service management (ITSM)

4. ISO38500: Corporate Governance of Information Technology

ISO38500: Corporate Governance of Information Technology

- Published June 2008, new version **ISO/IEC 38500:2015.**
- A '**high level principles based advisory standard**' for Directors when evaluating, directing and monitoring the use of IT in their organisations.
- The **objective of ISO 38500 is to provide a structure of principles for directors** (including owners, board members, directors, partners and senior executives) **to use when evaluating, directing and monitoring the use of IT in their organizations.**
- The scope of the standard is to provide guiding principles for directors of organizations on the effective, efficient and acceptable use of IT within their organizations. It is applicable for all organizations, from the smallest to the largest, regardless of purpose, design or ownership structure.

ISO38500: Corporate Governance of Information Technology

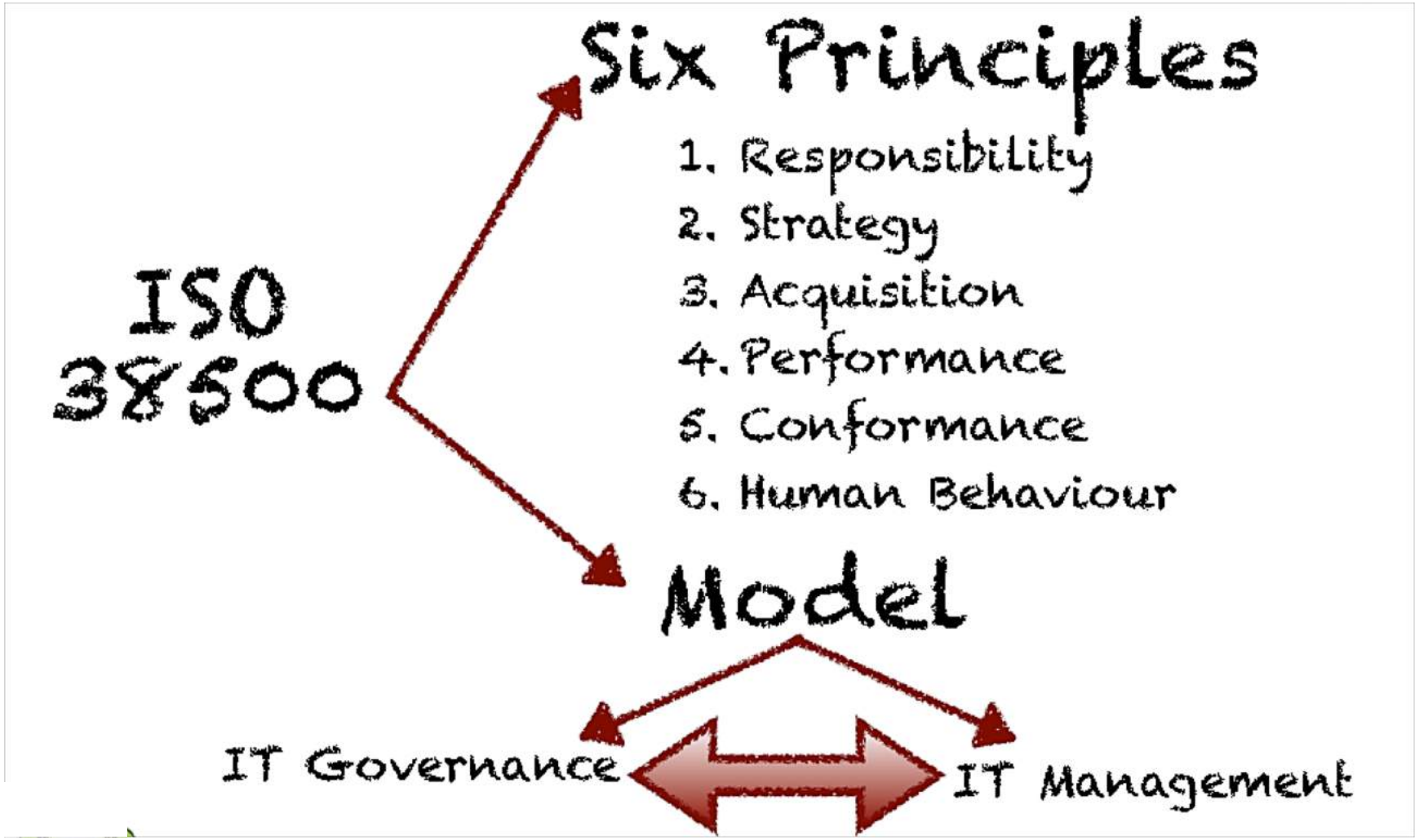
- ISO 38500 looks down from the top, much like a **roof** on a house.
- COBIT (the what) is the **walls**, and process frameworks such as ITIL and PMBOK (the how) are the **foundation**.
- Using the house analogy, if the board tried to implement the roof, ISO 38500, without the foundation or walls, it would collapse.
- ISO 38500 is not one size fits all.
- **It does not replace COBIT, ITIL, or other standards or frameworks**, but, rather, it complements them by providing a **demand-side**-of-IT-use focus.

ITIL - Information Technology Infrastructure Library

ISO38500: Objectives

- Provide a basis for the corporate governance of IT.
- Assuring stakeholders that if the standard is followed they can have confidence in the organisation's corporate governance of IT
- The global objective of ISO 38500 is to provide top managers with a **framework of principles** for **evaluatin**g, **directing** and **monitoring** the use of information technology in their organizations, thereby promoting IT performance and acceptance.
- The ISO 38500 standard delivers a model which helps executives structure the task of managing IT and equips them with a **standardized IT-terminology**.
  - This increased order in turn helps managers meet their IT related obligations (e.g. legal compliance, record keeping, IT-security etc.).
- Finally, a major benefit of the ISO 38500 lies in its ability to **integrate IT goals with overall business goals** thereby ensuring that IT works to the right end.

Framework


ISO
38500
Six Principles
1. Responsibility
2. Strategy
3. Acquisition
4. Performance
5. Conformance
6. Human Behaviour
Model
IT Governance
IT Management

The Guiding Principles of ISO 38500

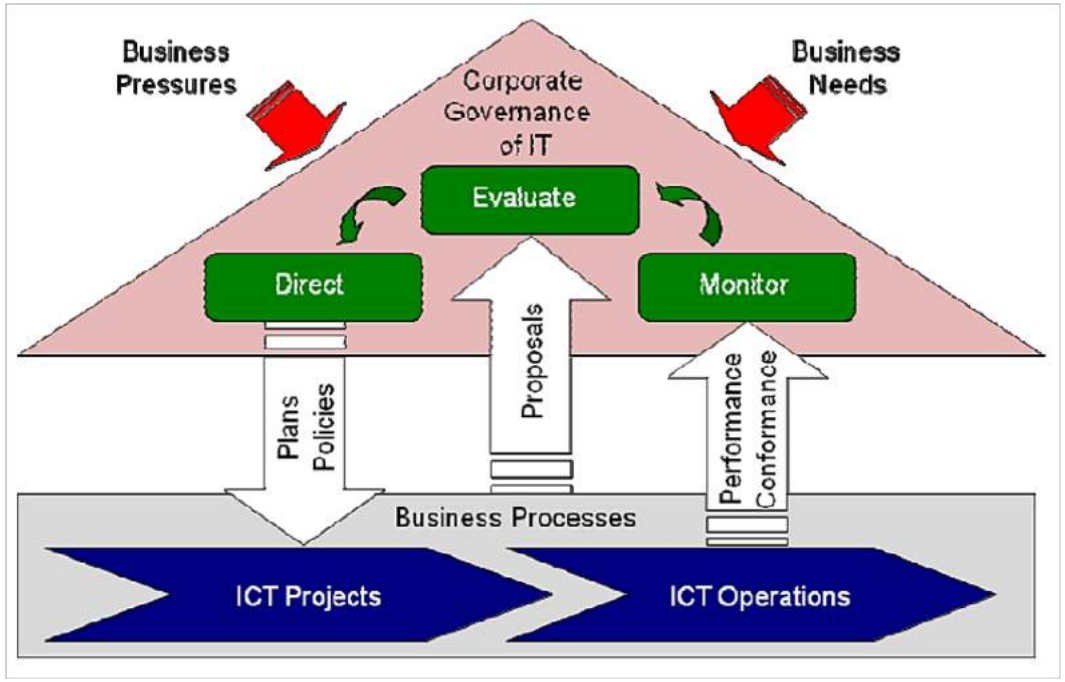
The ISO 38500 consists of **six guiding principles for good corporate governance of IT:**

- **Responsibility** – Employees know their responsibilities both in terms of demand and supply of IT and have the authority to meet them.
- **Strategy** – Business strategies take into account IT resources & capabilities and IT strategies are aligned with business strategies. Strategic plans for IT satisfy the current and ongoing needs of the organisation.
- **Acquisition** – IT acquisition decisions are taken in a reasonable and transparent way, short-term and long-term costs/risks and benefits are weighed.
- **Performance** – The purpose of IT is to serve business. It is ready to meet current and future needs.
- **Conformance** – IT complies with legislation and regulations. Policies and practices are clearly defined and implemented.
- **Human behavior –** IT policies, practices and decisions show respect for Human behavior and the needs of all the 'people in the process'.

Responsibility

- Everyone understands and accepts his or her responsibility
- This includes supply of and demand for IT
- Those with responsibility for actions also have the authority to perform those actions

ISO38500: the Model



ISO38500: the Model

Directors should govern IT through three main tasks:

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

ISO38500 Model: Evaluate

- Managers should continually **examine** and assess the current and future use of IT as well as strategies, proposals and sourcing issues.
- In doing so external and internal factors must be considered (SWOT).

ISO38500 Model: Direct

MANAGERS SHOULD ASSIGN RESPONSIBILITIES FOR AND DIRECT THE PREPARATION AND IMPLEMENTATION OF PLANS AND POLICIES.

WHILE PLANS SET THE DIRECTION FOR IT INVESTMENTS, POLICIES DEFINE THE WAY EMPLOYEES SHOULD BEHAVE IN THE USE OF IT.

IT REFRESH; INTERNET USAGE POLICIES

IN DIRECTING, MANAGERS MUST ENSURE THAT WHEN PROJECTS ARE BEING IMPLEMENTED THEIR IMPACT ON BUSINESS AND COMMON PRACTICE ARE TAKEN INTO ACCOUNT.

Implemention of ISO 38500

- Make ISO 38500 a board and executive management priority, if it is to succeed. IT governance must be directed from the top.
- Make IT governance part of the IT strategy, which is, in turn, part of the business strategy.
- Look for tangible benefits as opposed to “compliance for compliance’s sake.”
- Acknowledge the people factor, and incorporate it into key performance indicators (KPIs).
- Prioritize IT governance activities with clear milestones.

ISO38500 Model: Monitor

In order to measure actual IT performance against planed performance, especially in regard to business objectives, **appropriate measurement systems must be in place**.

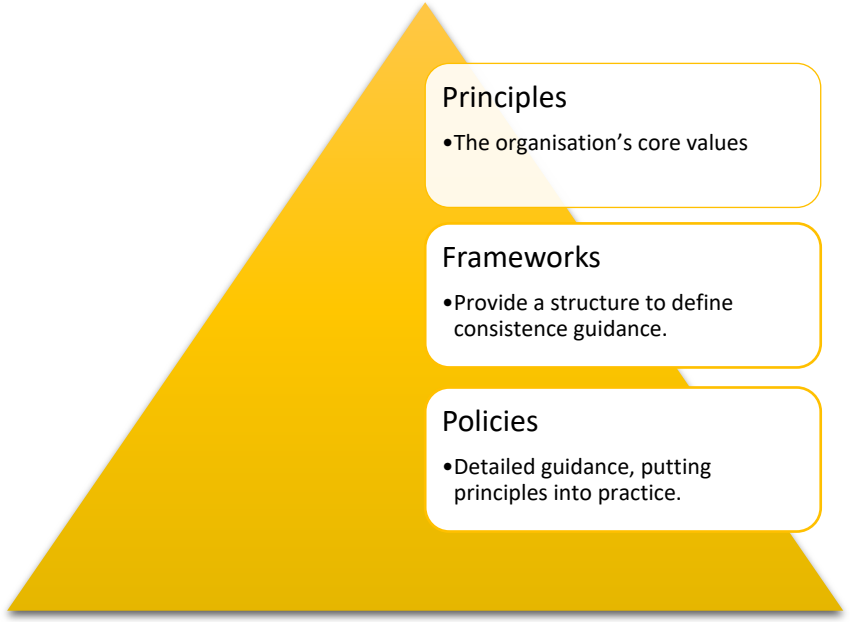
Managers must make sure that **IT conforms with external regulations and internal policies.**

The combination of the six guiding principles with these three simple activities constitutes the ISO 38500 framework.

The focus of ISO 38500 on linking IT performance to overall business performance makes the ISO 38500 an effective instrument for IT top management.

COBIT 5 Framework

Principles, Policies And Frameworks



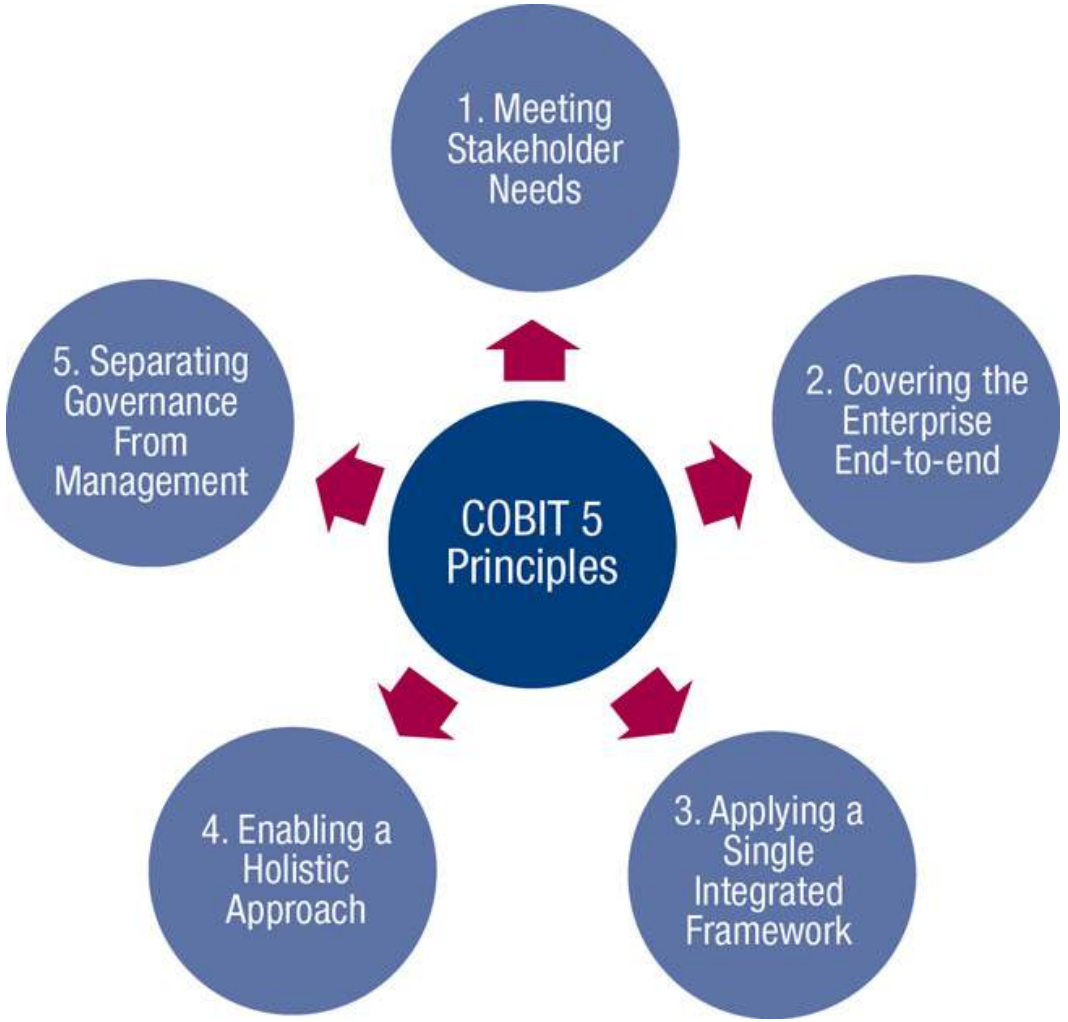
Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.

The COBIT 5 Framework

- **The COBIT 5 principles and enablers are generic** and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

COBIT 5 Principles and Enablers

COBIT 5 Principles

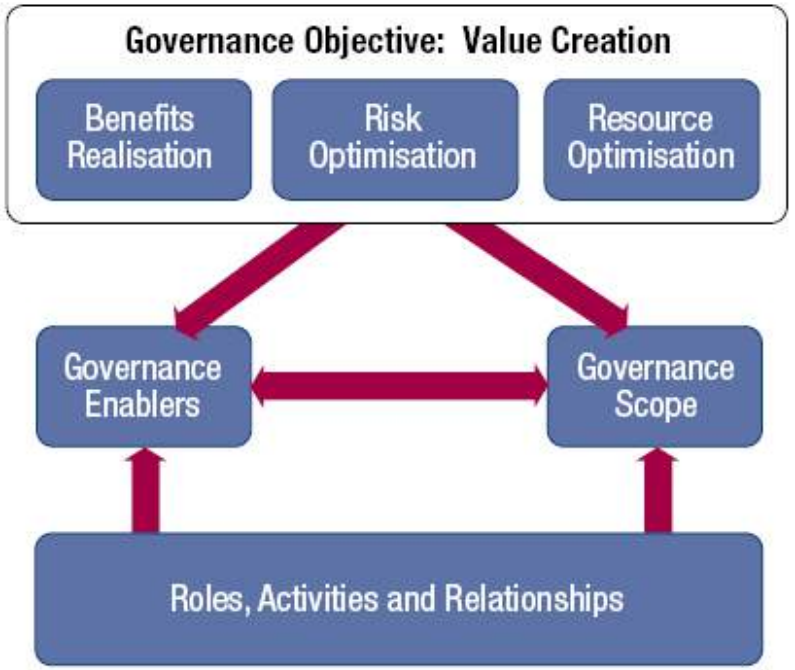


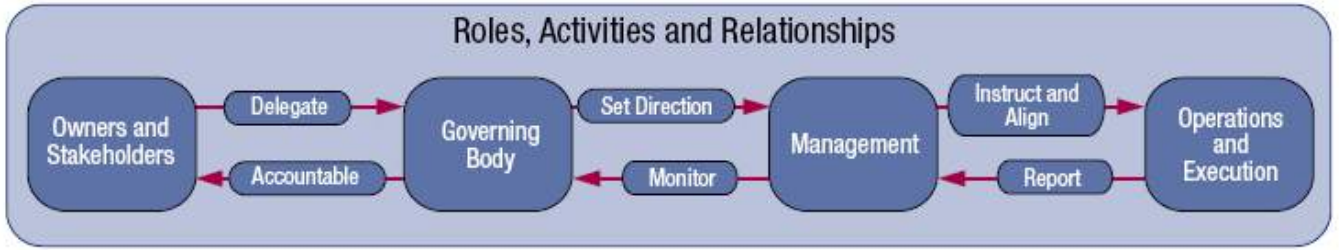
Principle 1:
Meeting Stakeholder Needs

Enterprises exist to **create value** for their stakeholders.

Principle 2: Covering the Enterprise End-to-End

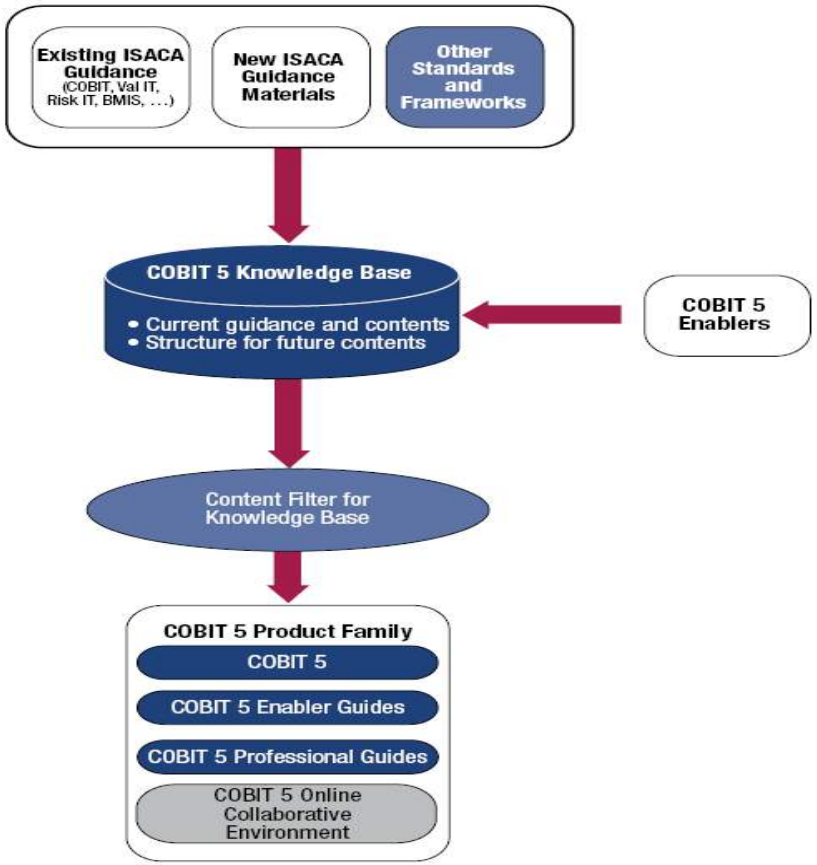
- Enterprisewide, end-to-end perspective
- Information and related technology **wherever** that information is being processed
- **NOT** just the IT function





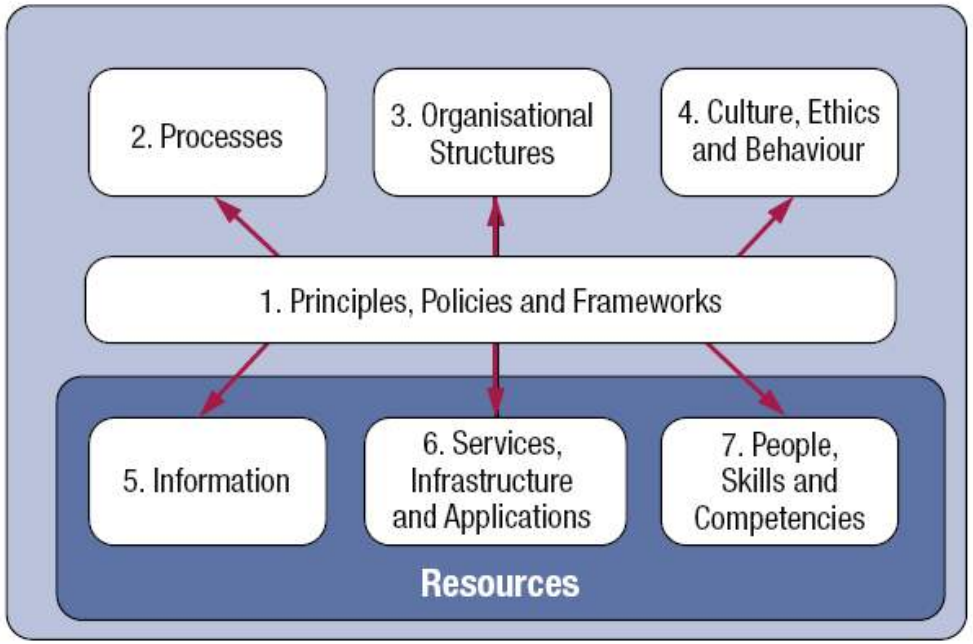
Principle 3: Applying a single Integrated Framework

- Aligns with other standards and frameworks
- Complete in enterprise coverage
- Simple architecture for:
  - structuring guidance materials
  - producing a consistent product set
- Integrates all knowledge previously dispersed over different ISACA/ITGI frameworks



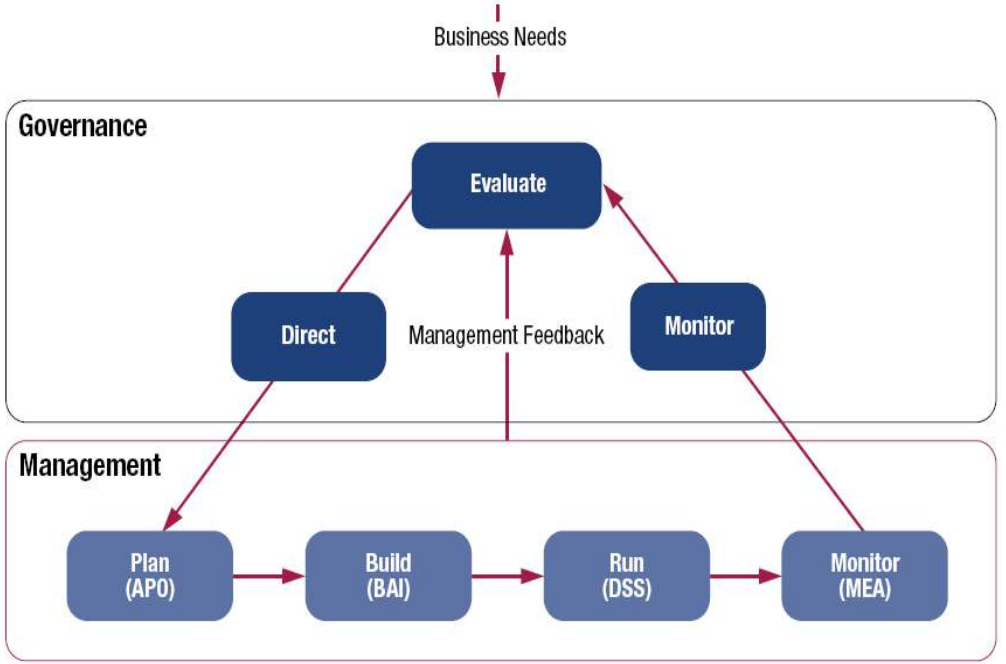
Principle 4: Enabling a holistic approach

- Driven by the goals cascade – goals define what enablers should achieve
- To achieve enterprise objectives consider an interconnected set of enablers
- **Some enablers are the enterprise resources**

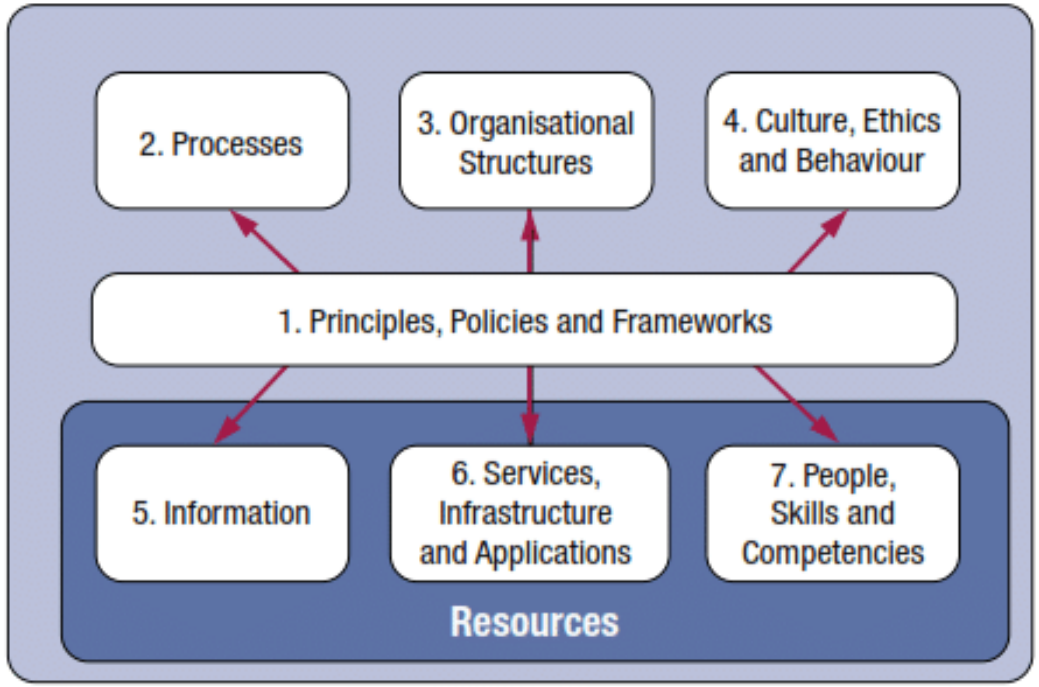


Principle 5: Separating Management from Governance

- Different activities and different responsibilities
- Interactions between them are facilitated through the Enablers



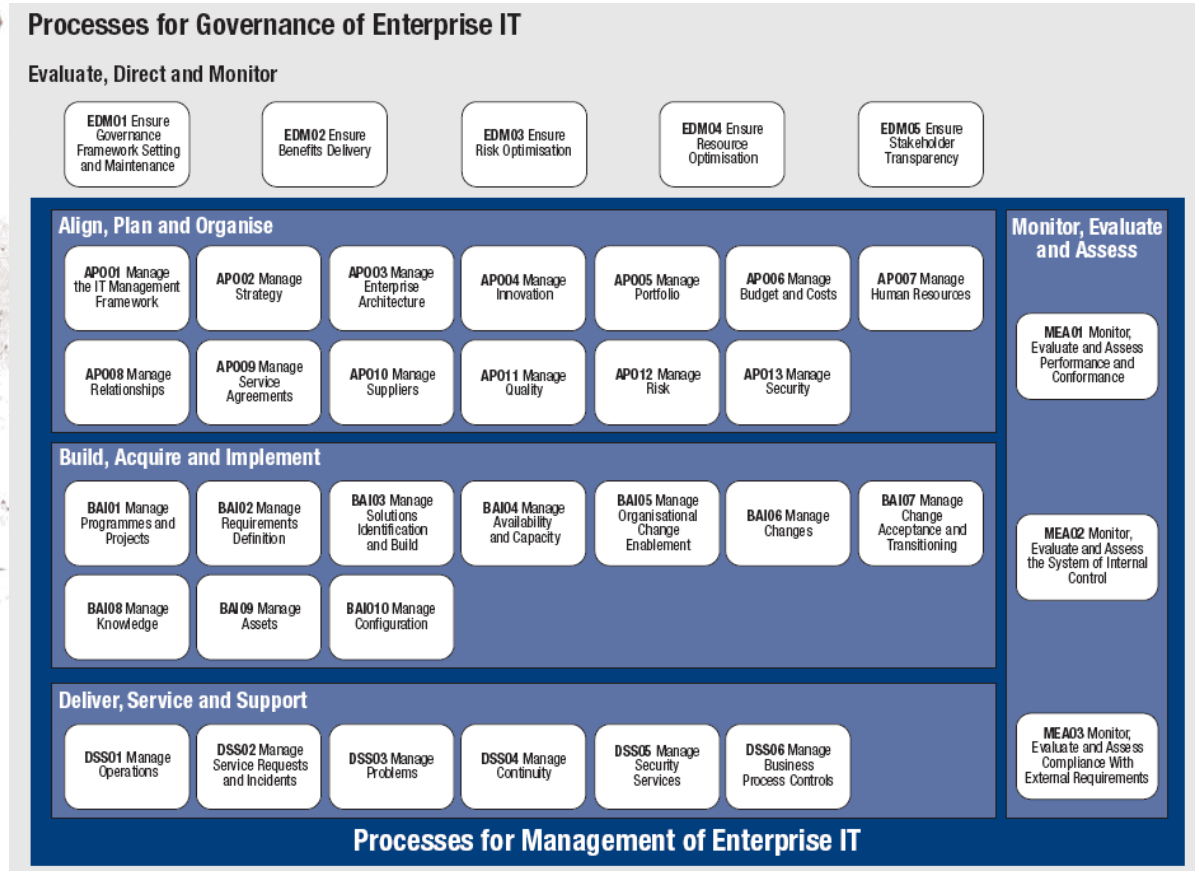
COBIT 5 Enablers

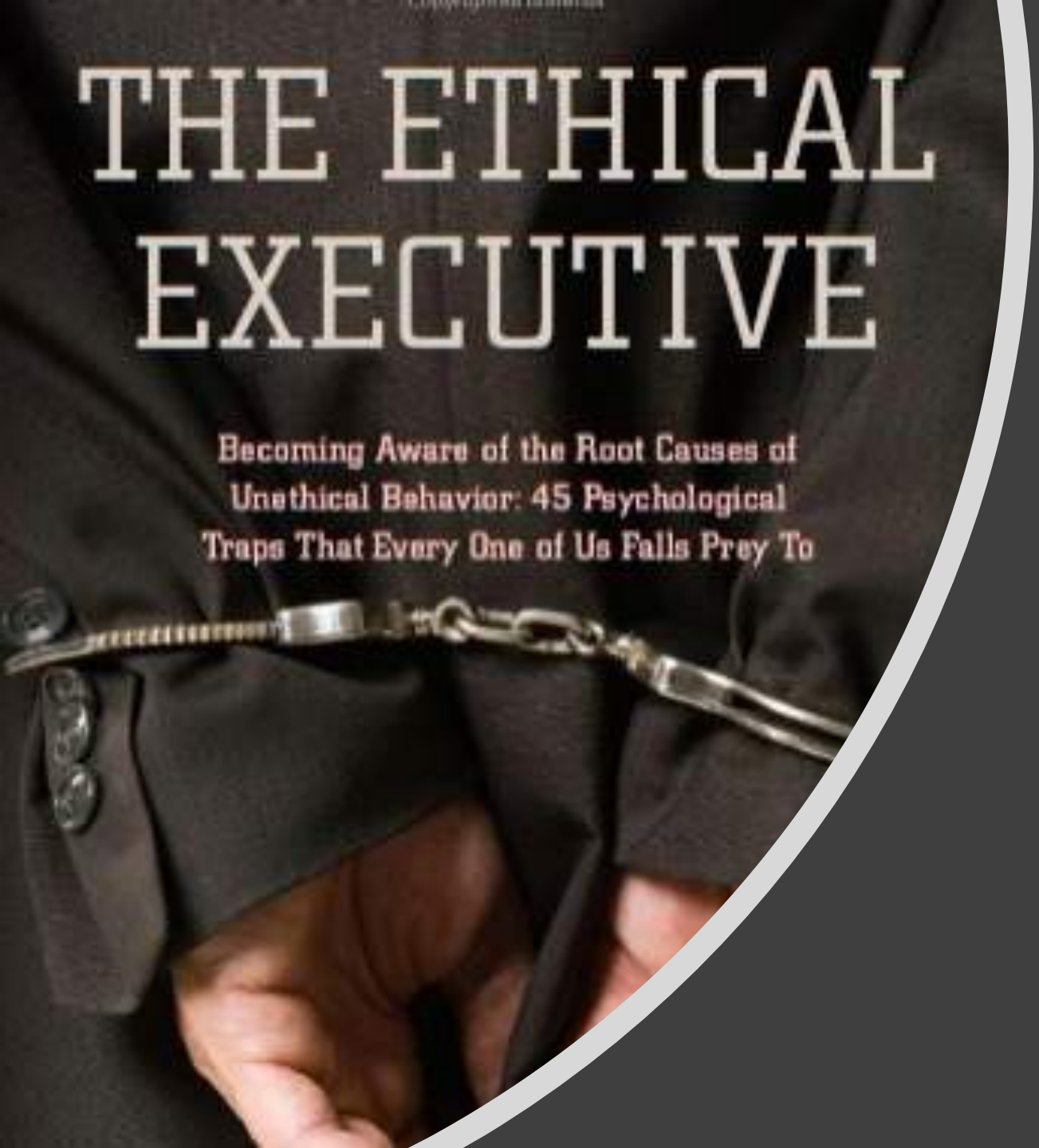


Governance (and Management) in COBIT 5

- Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against agreed direction and objectives (**EDM: Evaluate-Direct-Monitor**).
- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM: Plan-build-Run-Monitor).**
- Exercising governance and management effectively in practice requires appropriately using all enablers.
- The COBIT process reference model allows us to focus easily on the relevant enterprise activities.

Governance in COBIT 5





Compliance in COBIT 5:

Sarbanes–Oxley Act of 2002

Fraudulent Statements

- Financial statements can be falsified to:
  - Deceive investors and creditors
  - Cause a company's stock price to rise
  - Meet cash flow needs
  - Hide company losses and problems

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

- **COSO** (http://www.coso.orgi) is a voluntary private sector organization **dedicated to improving the quality of financial reporting** through business ethics, effective internal control and corporate governance.
- It was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector organization often referred to as the Treadway Commission.
- Key sponsoring organizations include the
  - American Institute of Certified Public Accountants (AICPA),
  - American Accounting Association (AAA),
  - Financial Executives International (FEI),
  - Institute of Internal Auditors (IIA) and
  - Institute of Management Accountants (IMA).

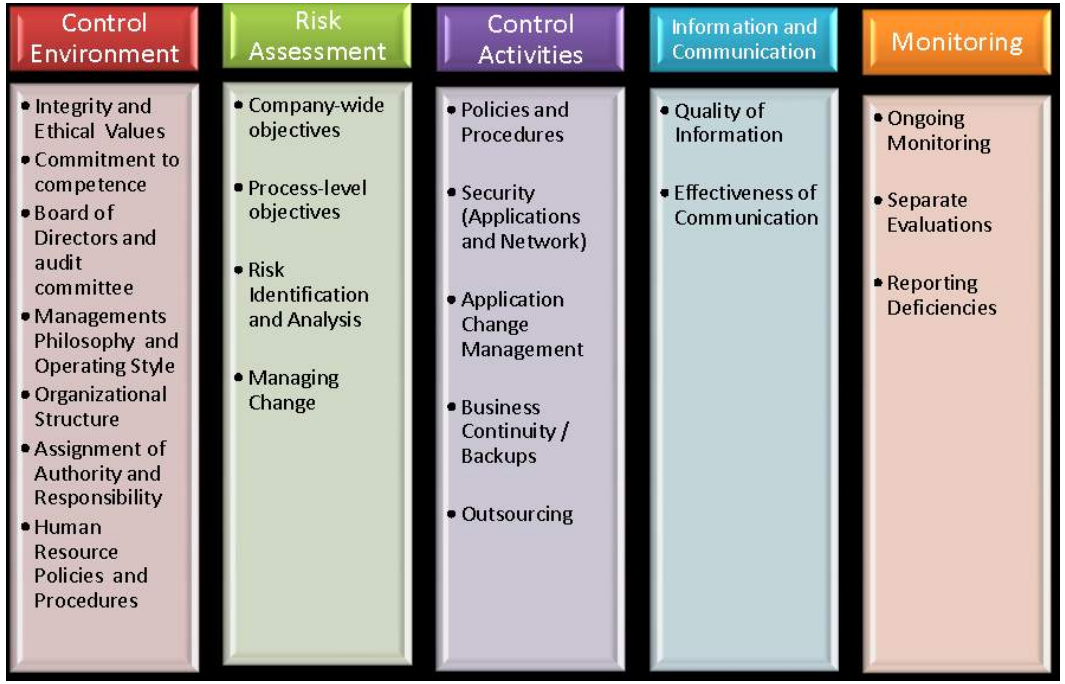
COSO: Internal Control – Integrated Framework

COSO identifies **five essential components of effective internal control**. They are:

- **Control environment**
- **Risk assessment**
- **Control activities**
- **Information and communication**
- **Monitoring**

The COSO framework has been rapidly adopted by financial auditors as a means of implanting controls for the financial reporting process.

✓ Internal Control Framework



✓ Control Activities

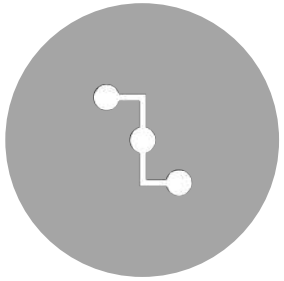
Policies and Procedures	Security (Applications and Network)	Application Change Management	Business Continuity
•IT-Security Policy •IT-Access Control Policy •IT-Appropriate Usage Policy •Email-Internet Policy •End-user Computing	•Application Authorization Matrix •End User Computing Trace ability Matrix •IT – Landscape Diagram •ISO	•Project Management	•IT-Infrastructure Management •Disaster Recovery •Backup and Recovery Procedures •Job Scheduling

Enron Corporation (from Wikipedia)

- Enron Corporation, former NYSE ticker symbol ENE) was an American energy company based in Houston, Texas. Before its **bankruptcy in late 2001**, Enron employed approximately 22,000 people and was one of the world's leading electricity, natural gas, pulp and paper, and communications companies, with claimed revenues of $111 billion in 2000.
- Fortune named Enron "America's Most Innovative Company" for six consecutive years.
- **At the end of 2001 it was revealed that its reported financial condition was sustained substantially by institutionalized, systematic, and creatively planned accounting fraud, sometimes called the "Enron scandal".**
- Enron has since become a popular symbol of willful corporate fraud and corruption.

Enron Corporation (from Wikipedia)

ENRON FILED FOR BANKRUPTCY ON DECEMBER 2, 2001.



IN ADDITION, THE SCANDAL CAUSED THE DISSOLUTION OF ARTHUR ANDERSEN, WHICH AT THE TIME WAS ONE OF THE WORLD'S TOP ACCOUNTING FIRMS.

THE FIRM WAS FOUND GUILTY OF OBSTRUCTION OF JUSTICE IN 2002 FOR DESTROYING DOCUMENTS RELATED TO THE ENRON AUDIT AND WAS FORCED TO STOP AUDITING PUBLIC COMPANIES.

Enron Corporation (from Wikipedia)

- Enron had **created offshore entities**, units which may be used for **planning and avoidance of taxes**, **raising the profitability of a business**.
- This provided ownership and management with full freedom of currency movement, and full anonymity, that would hide losses that the company was taking.
- These entities made Enron **look more profitable than it actually was**, and created a dangerous spiral in which each quarter, corporate officers would have to perform more and more contorted financial deception to create the illusion of billions in profits while the company was actually losing money.
- This practice drove up their stock price to new levels, at which point the executives began to work on **insider information** and trade millions of dollars worth of Enron stock.

Enron

- Substantial breakdowns in corporate governance
  - Internal controls
  - External auditors
  - Board of directors
  - Financial institutions
  - Analysts
  - Regulators

Example 2:

WorldCom

THE COMPANY SAID AN INTERNAL AUDIT HAD DISCOVERED THAT $3.3BN IN PROFITS WERE IMPROPERLY RECORDED ON ITS BOOKS FROM 1999 TO THE FIRST QUARTER OF 2002.

THAT IS ON TOP OF THE $3.8BN IN EXPENSES THE COMPANY SAID IT HAD IMPROPERLY REPORTED AS CAPITAL INVESTMENTS.

WORLDCOM NOW SAYS IT MUST ISSUE REVISED FINANCIAL STATEMENTS FOR 2000 AND 1999 AS WELL.

THE REVISION WILL REDUCE 2000 PROFITS BY MORE THAN $3.2BN, BUT THIS MAY NOT BE THE END OF ACCOUNTING HORRORS AS THE COMPANY WARNED IT MAY FIND MORE PROBLEMS.

There are many important standards, just now:

IT Governance: Compliance

Sarbanes-Oxley

What prompted SOX (Sarbanes-Oxley)?

Sarbanes-Oxley was passed in the wake of a number of notable corporate accounting scandals including Enron and WorldCom.

Sarbanes–Oxley Act of 2002

U.S. Senator Paul Sarbanes and U.S. Representative Michael G. Oxley.

- The Sarbanes–Oxley Act of 2002 (Pub.L. 107-204, 116 Stat. 745, **enacted July 30, 2002**), also known as the 'Public Company Accounting Reform and Investor Protection Act' (in the Senate) and 'Corporate and Auditing Accountability and Responsibility Act' and commonly called **Sarbanes–Oxley, Sarbox** or **SOX**, is a **United States federal law** enacted on **July 30, 2002**, which **set new or enhanced standards** for all U.S. public company boards, management and public accounting firms.


Paul Sarbanes
Michael Oxley
hen Pres. George
Bush signing the
nes-Oxley Act
2002
CORPORATE RESPONSIBILITY

SOX on the Horizon?

The primary thing to remember is that **SOX is about mitigating the risk of fraud, financial transparency and process control**.

This will change how you do things but that does not have to be a bad thing.

EuroSOX

EuroSox Directives

The EU directives commonly referred to as **EuroSox** came in to force from 2008/9.

The accounting directive focuses on **four key revisions** to enhance confidence in financial reporting by companies:

- ❑Board members are collectively responsible for financial statements and key non-financial information
- ❑Making transactions with related parties more transparent
- ❑Provide full information on off-balance-sheet arrangements, including qualified special-purpose vehicles (QSPE)
- ❑Issue an annual corporate governance statement

SOX

SOX requires management to:

- Certify the financial statements and internal control over financial reporting in periodic reports filed with the SEC (=S 302)
- Annually assess and report on internal controls.

SOX requires auditors to:

- Provide an attestation report on management's annual assessment (=S 404).

IT relevant Sections

- **S 302:** Corporate Responsibility For Financial Reports
- **S 404:** Management Assessment Of Internal Controls
- **S 409:** Real Time Disclosure

Generally relevant Sections

- **S 101:** Establishment, Board Membership & Duties Of The Board
- **S 103:** Auditing, Quality Control, Independence Standards & Rules
- **S 106:** Foreign Public Accounting Firms
- **S 401:** Disclosures In Periodic Reports & Study and Report on Special Purpose Entities
- .....

SOX: Summary of Relevant Sections

Section	Requirements	Relevance/Impact
Section 302	CEOs and CFOs must certify financial and other information in their companies' quarterly and annual reports.	CEO, CFO, or any executive who executes signoff authority for financial statements.
Section 404	Requires an annual management report on and auditor attestation of a company's implemented internal controls over financial reporting.	CEO, CFO, any executive who executes signoff authority for financial statements, CIO and IT Operations.
Section 409	Requires disclosure on a rapid and current basis such additional information concerning material changes in its financial condition or operations.	CEO, CFO, any executive who executes signoff authority for financial statements, CIO and IT Operations.

SOX
Sec. 302

Sec. 302. Corporate Responsibility for Financial Reports

(a) REGULATIONS REQUIRED.—The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

(1) the signing officer has reviewed the report;

(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;

(4) the signing officers—

(A) are responsible for establishing and maintaining internal controls;

(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

(C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and (D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and

(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

SOX
Sec. 404

Sec. 404. Management Assessment of Internal Controls

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board.

Any such attestation shall not be the subject of a separate engagement.

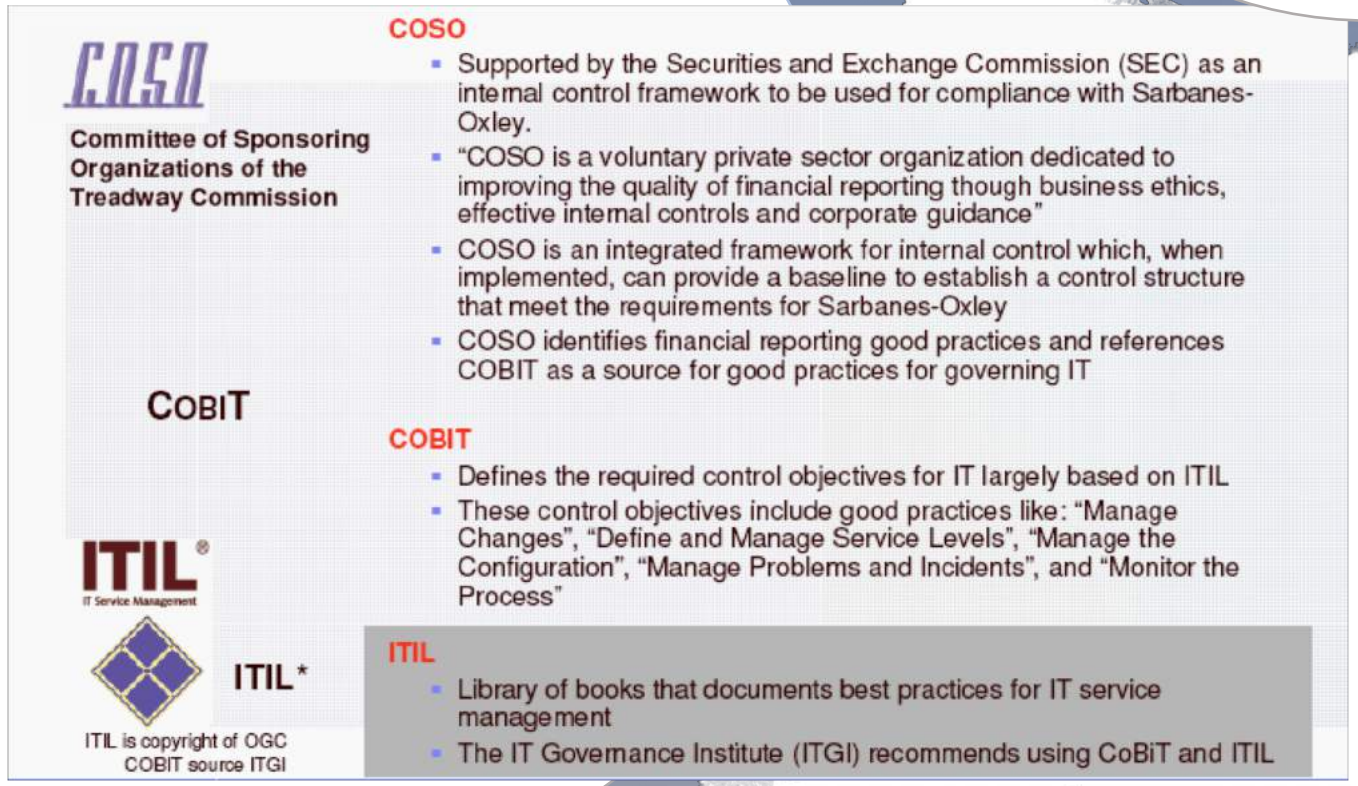
Penalties

Section 802(a) of the SOX states:

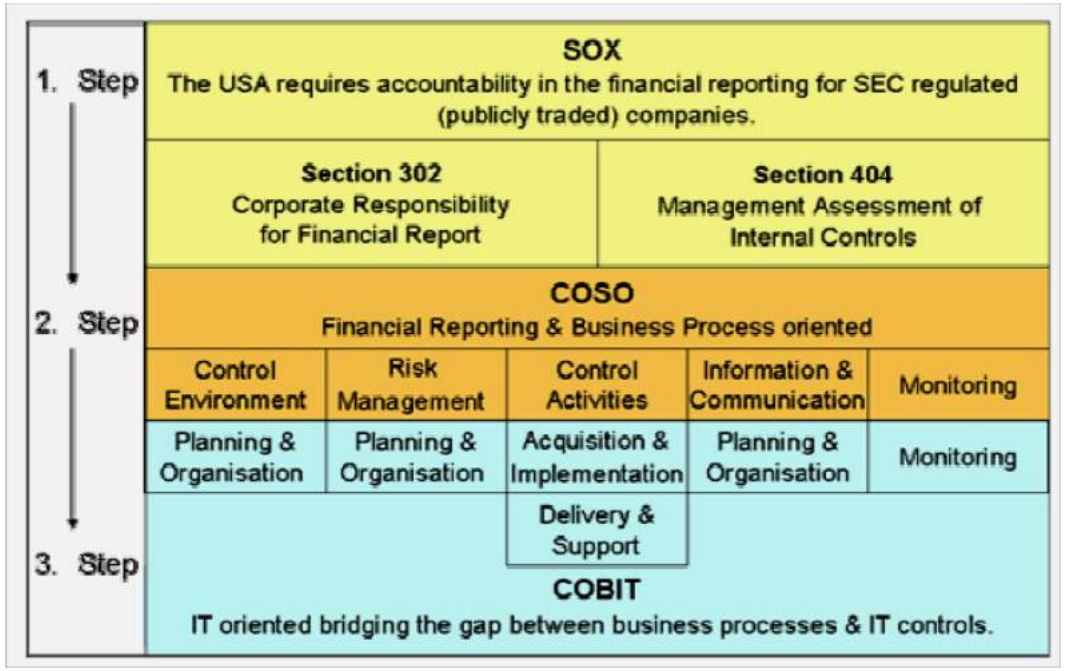
" Whoever **knowingly** alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, **shall be fined** under this title, **imprisoned not more than 20 years**, or both."

SOX Compliance

Becoming SOX compliant is not optional: management **MUST** promote an internal control culture and adopt compliance behaviors. Industry analysts, the SEC and logic suggest using existing industry recognized frameworks and models.



SOX Compliance



Who Does the Sox Act Affect?

- External auditors
- Internal auditors
- Boards of directors and their committees
- Top executives
- Senior managers
- Attorneys, both internal and external
- Regulators

Responsibilities of Board Members

Board	Board members are collectively responsible for financial statements and key non-financial information
Board	Board members issue an annual corporate governance statement
Board	Board members assure effective corporate governance, internal controls and risk management
Board	Board members assure measures that safeguard shareholders' investments
Board	Board members assure that audit committees are established
Board	Board members assure that corporate governance standards are improved

Financial Statement Certification

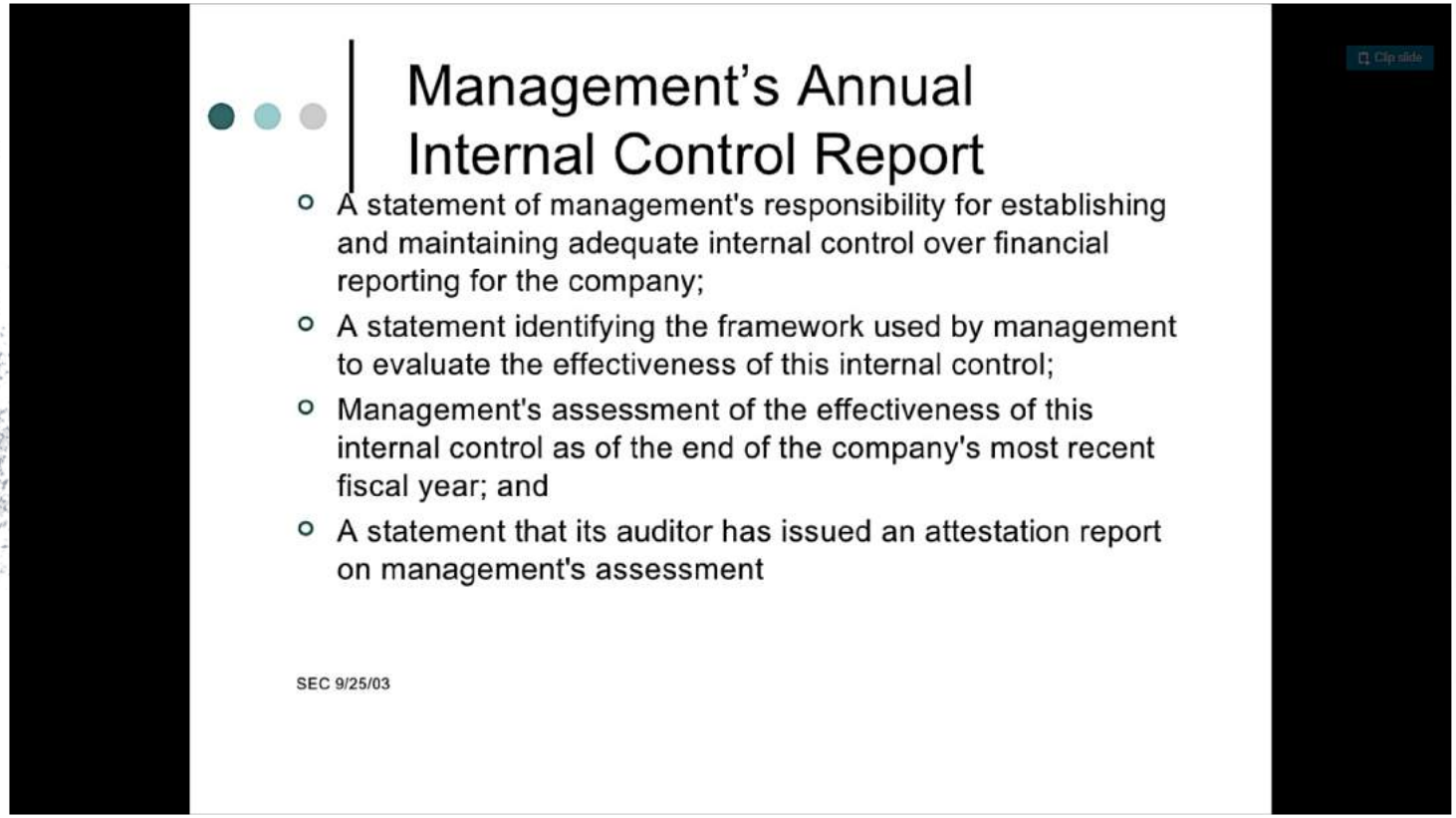
The CEO and CFO must certify in each period filing that the financial information:

"does not contain any untrue statement of a material fact"

and

"fairly presents in all material respects the financial condition and results of operations of the issuer."

Management’s Annual Internal Control Report



What are Internal Controls?

The five components in a control system:

1. Control environment (how do people feel?)
2. Risk assessment (what could go wrong?)
3. Control activities (procedures to control against risks)
4. Information and communication (timely feedback, truth-telling)
5. Monitoring (ongoing assessment of the environment, and the risks, and the effectiveness of the procedures)

Compliance in COBIT 5

- The MANAGEMENT **Monitor, Evaluate and Assess** domain contains a compliance focused process: MEA03 Monitor, evaluate and assess compliance with external requirements.

Process Description

- Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.

Process Purpose Statement

- Ensure that the enterprise is compliant with all applicable external requirements.

Compliance in COBIT 5

- Legal and regulatory compliance is a key part of the effective governance of an enterprise, hence its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03).
- In addition to MEA03, all enterprise activities include control activities that are designed to ensure compliance not only with externally imposed legislative or regulatory requirements but also with enterprise governance-determined principles, policies and procedures.

Compliance in COBIT 5 (cont.)

- In addition to activities, **COBIT 5 suggests accountabilities, and responsibilities** for enterprise roles and governance/management structures (**RACI charts**) for each process. These include a compliance-related role.

MEA03 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
MEA03.01 Identify external compliance requirements.					A	R										R	R	R								R
MEA03.02 Optimise response to external requirements.		R	R	R	A	R	I		R							R	R	R	I	R	R	R	R	R	R	R
MEA03.03 Confirm external compliance.	I	R	R	R	R	R	I	I	C							A	I	R	C	C	C	C	C	C	C	R
MEA03.04 Obtain assurance of external compliance.	I	I	I	I	C	C	I		C							C	A	R	C	C	C	C	C	C	C	C

- **RACI** is an **acronym** derived from the four key responsibilities most typically used: **Responsible, Accountable, Consulted**, and **Informed**.

Examples of COBIT Controls

NETWORK SECURITY –

FIREWALLS, SECURE NETWORK CONFIGURATION INCLUDING 802.11X

ANTIVIRUS AND ANTI-SPYWARE UPDATED REGULARLY

- IEEE 802.11: standard for defining communication over a wireless LAN (WLAN)

Examples of COBIT Controls

Backups & Restore – Regularly tested procedures

IT Continuity – Disaster Recovery Procedures

Examples of COBIT Controls

Files Access Privilege Controls

Identity Management –

password strength/age and access. Who has access and is that appropriate now?

Examples of COBIT Controls

Risk Evaluation Programs –

Risk Assessment and internal auditing.

Employee IT Security Training –

Training of end users related to utilization of resources.

Examples of COBIT Controls

Management support/buy in –

Executive level oversight of projects related to IT.

IT as part of strategic planning –

The business must be supported by technologies.

Examples of COBIT Controls

Change Management

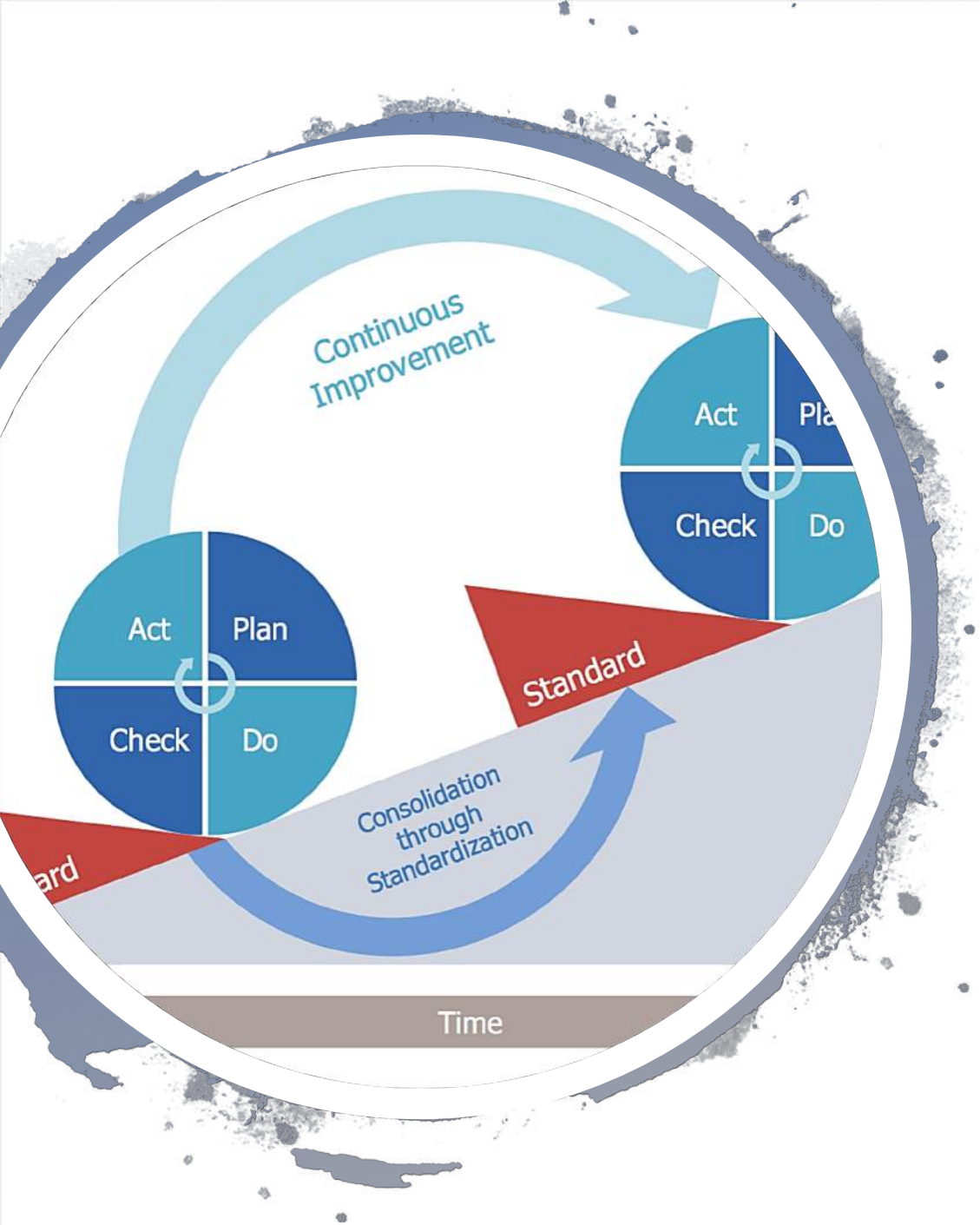
Standardized change control is a great place to find fast rewards in pursuit of compliance.

- **Change Approval**
- **Change Categorization**
- **Change Documentation**
- **Change Prioritization**
- **Formal Request for Change Process**
- A body of subject matter experts that oversee change.

Examples of COBIT Controls

Consistent Logging

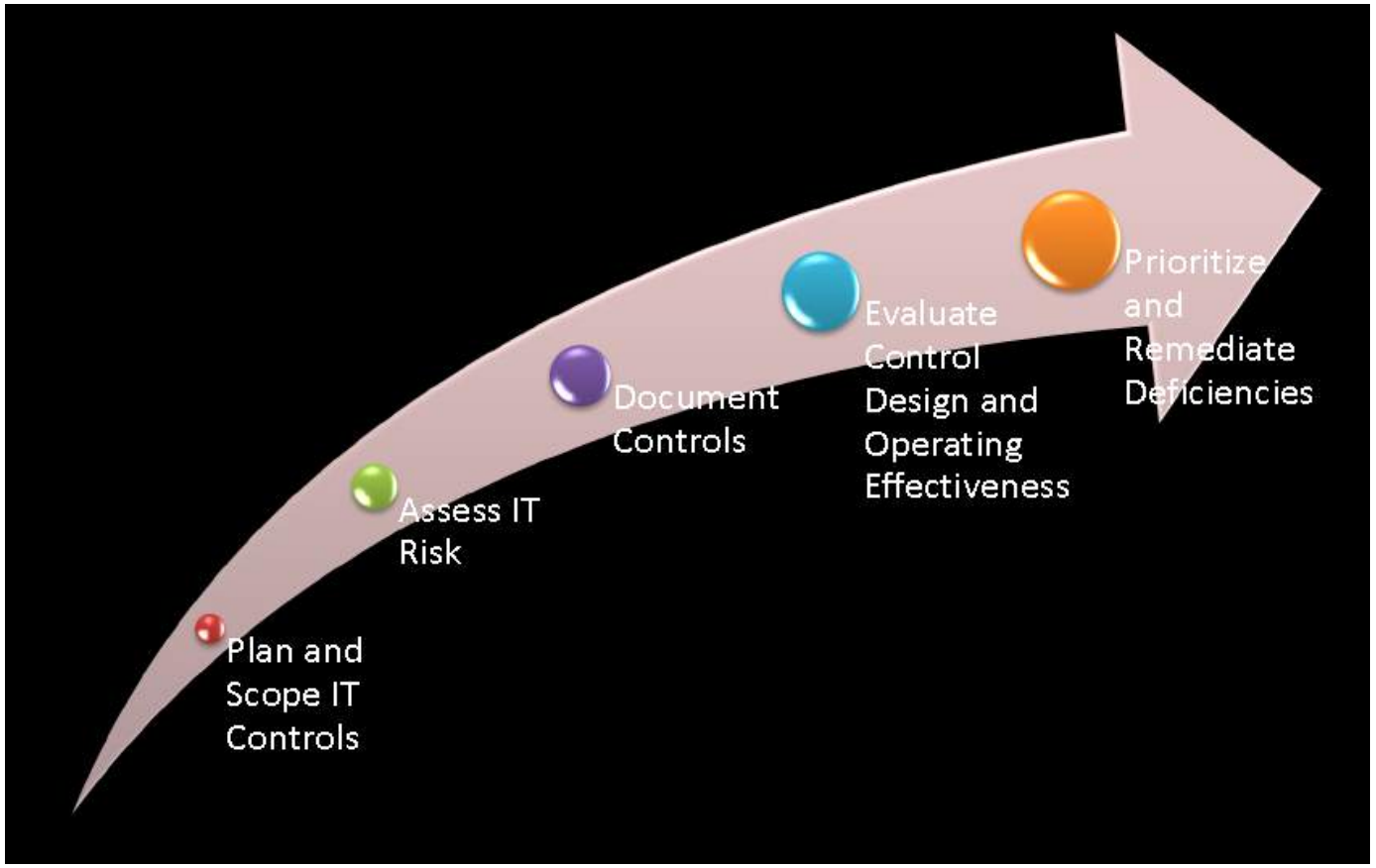
- Change Management
- Configuration Mgmt.
- Event Management
- Incident Management
- Knowledge Mgmt.
- Problem Management



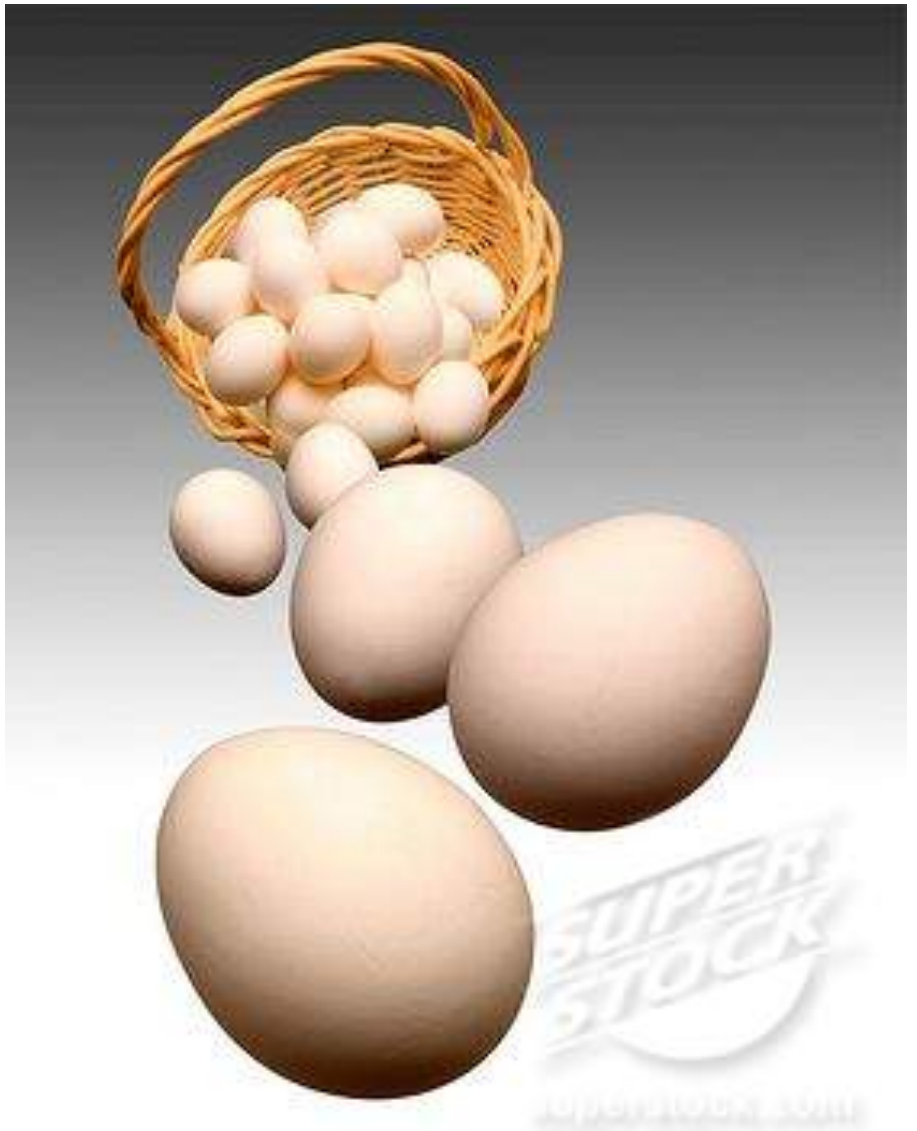
Remember W. Edward Deming?

- SOX Compliance is **not a fix it and forget it** endeavor.
- As companies and the ecosystems that support them change new compliance quandaries will come up.

IT Compliance Roadmap

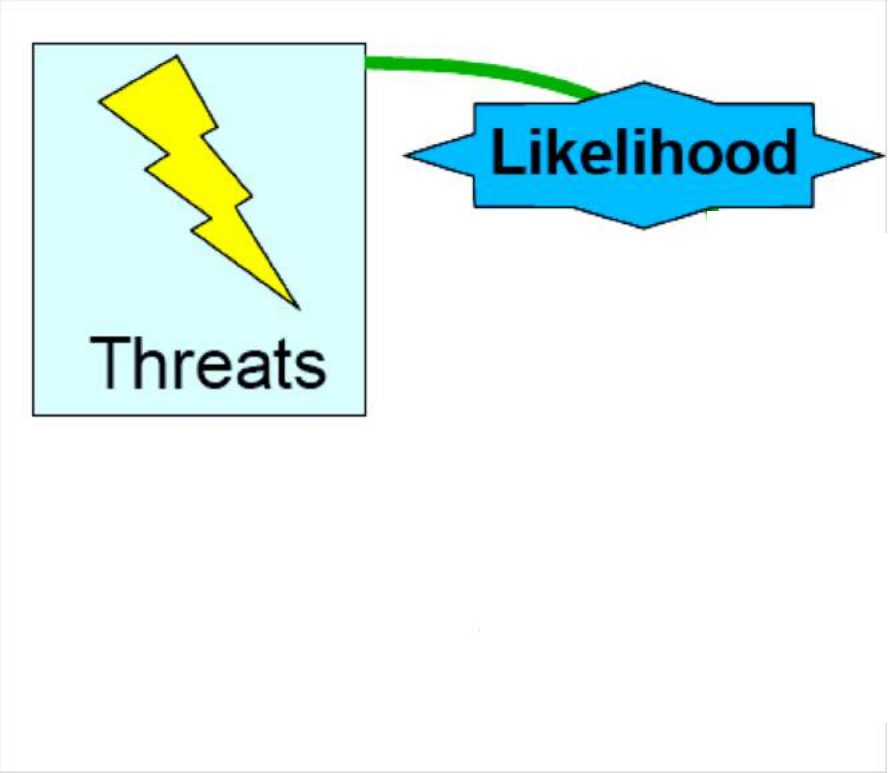


Risk Management and Governance in COBIT 5

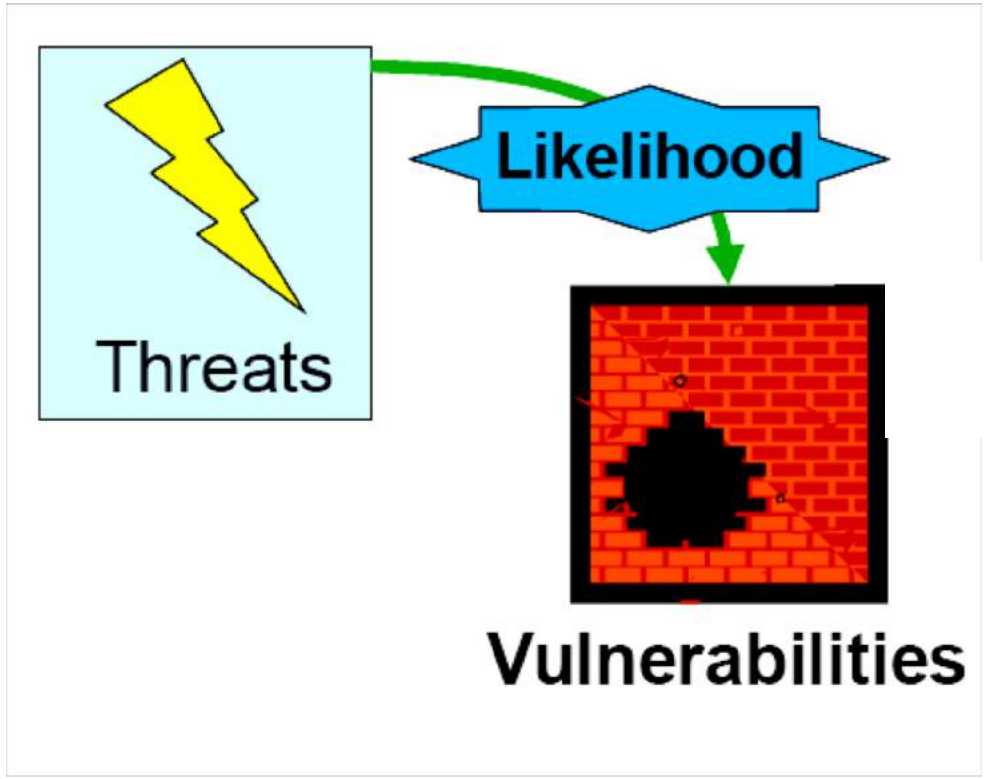


Threats, Vulnerabilities, Assets

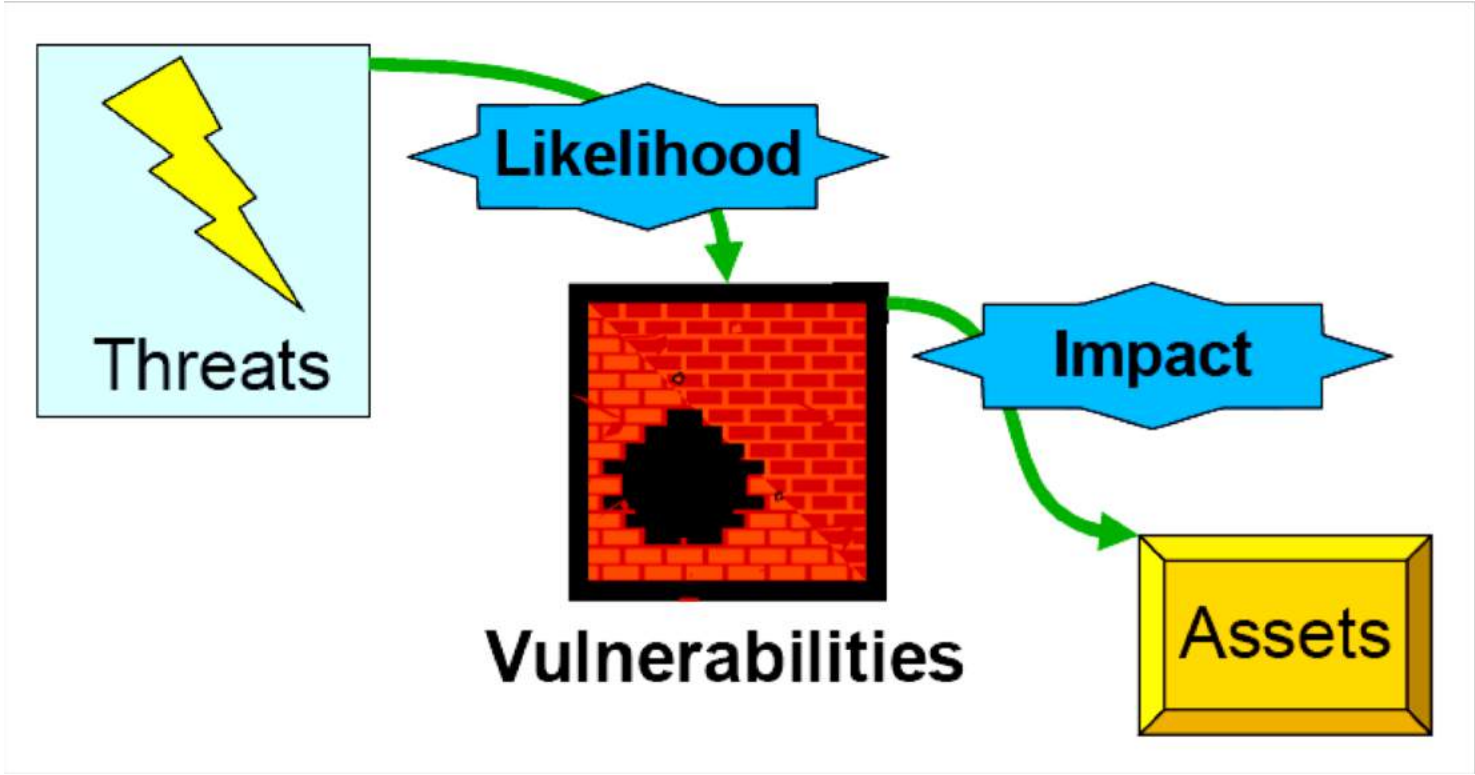
Threats, Vulnerabilities, Assets



Threats, Vulnerabilities, Assets



Threats, Vulnerabilities, Assets



Risk = Probability * Damage Potential

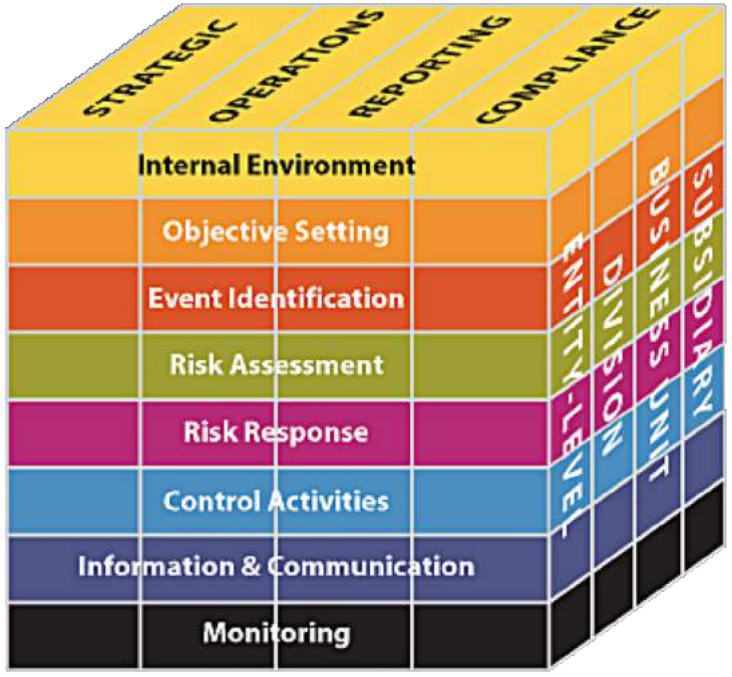
ISO 31000
Risk Definition

Risk

Effect of uncertainty on objectives.

An effect is a deviation from the expected – positive and/or negative.

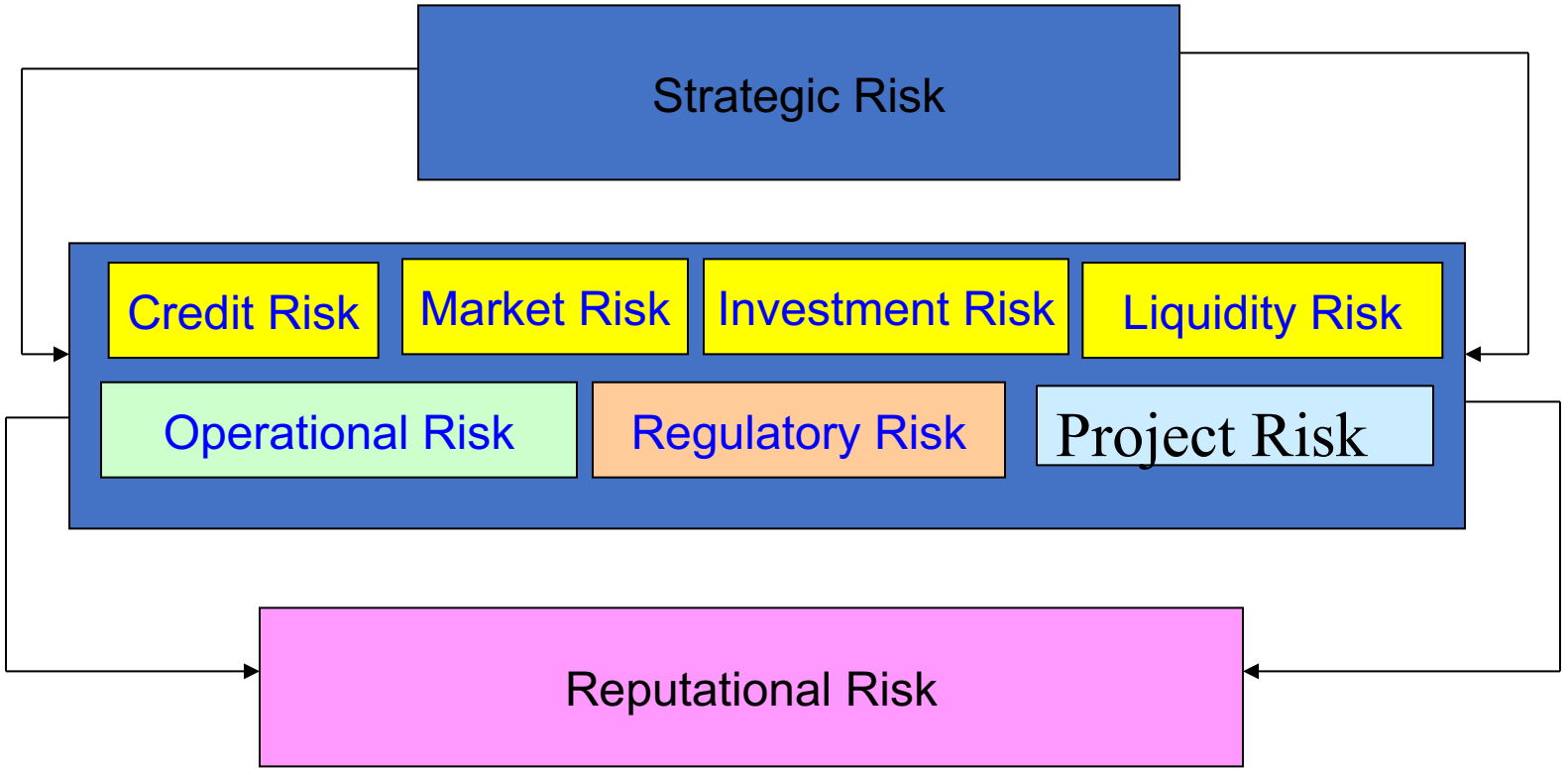
COSO Enterprise Risk Management



These are the **high level goals that are aligned with and support the institution's mission**.

- **Strategic** – high-level goals, aligned with and supporting its mission
- **Operations** – effective and efficient use of its resources
- **Reporting** – reliability of reporting
- **Compliance** – compliance with applicable laws and regulations.

Enterprise Risk Framework

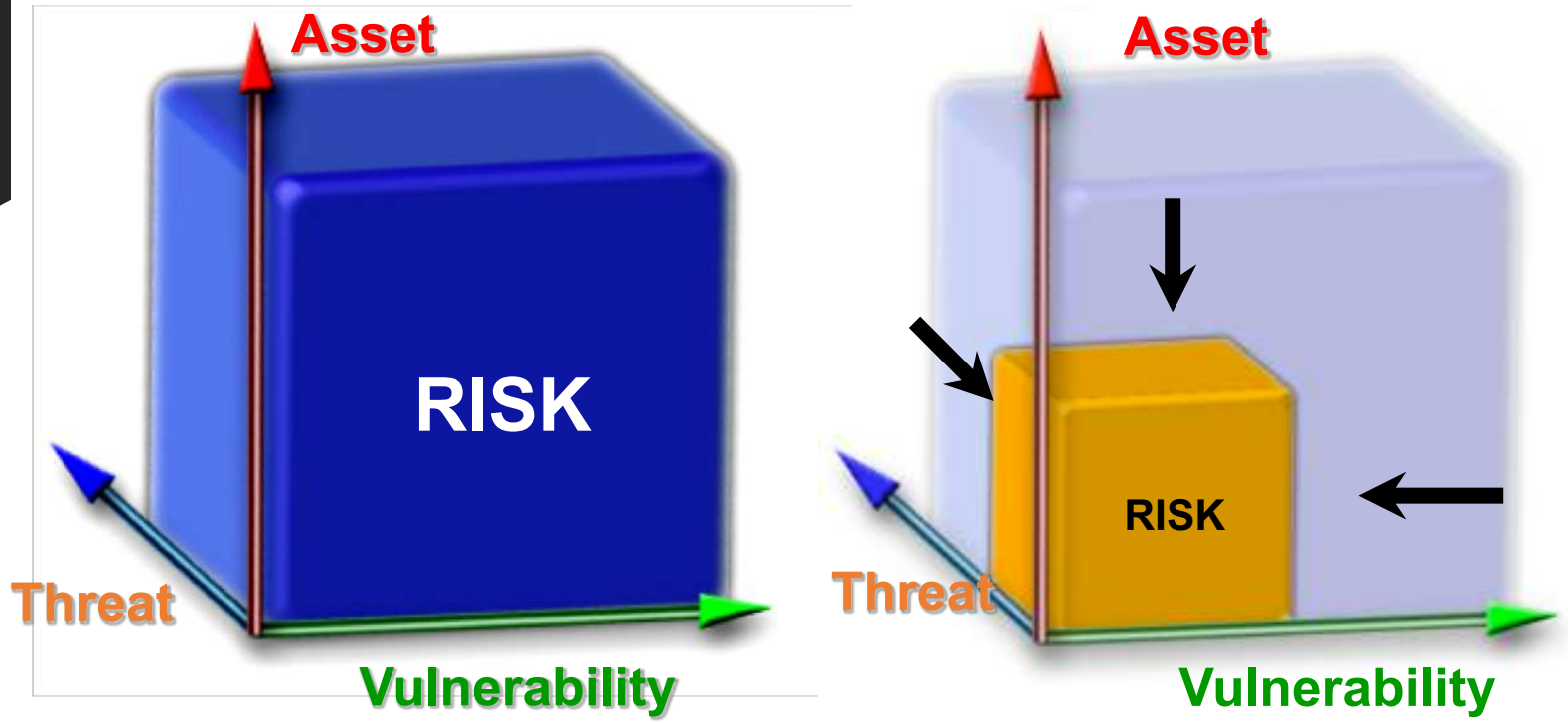


Risk Heat Map

Probability						
	Almost Certain (5)	5	10	15	20	25
	Likely (4)	4	8	12	16	20
	Possible (3)	3	6	9	12	15
	Unlikely (2)	2	4	6	8	10
	Rare (1)	1	2	3	4	5
	Immediate action and weekly review	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
	Urgent action and monthly review					
	Timely action and quarterly review	Impact on Organization				
	General action and yearly review					

- Scoring
- TARA

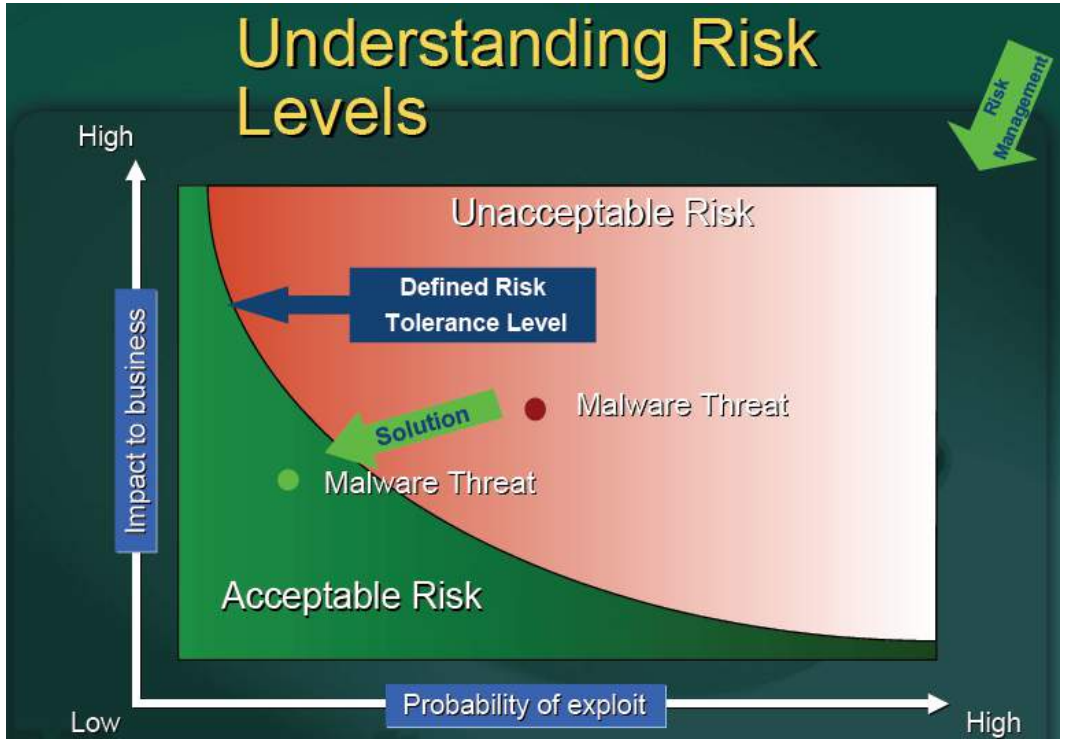
Residual Risk



Baseline Risk

Residual Risk after Countermeasures Applied

How Much Can You Afford?



Risk Appetite

Hmmmm!!!
Risky! (yummy!!!)

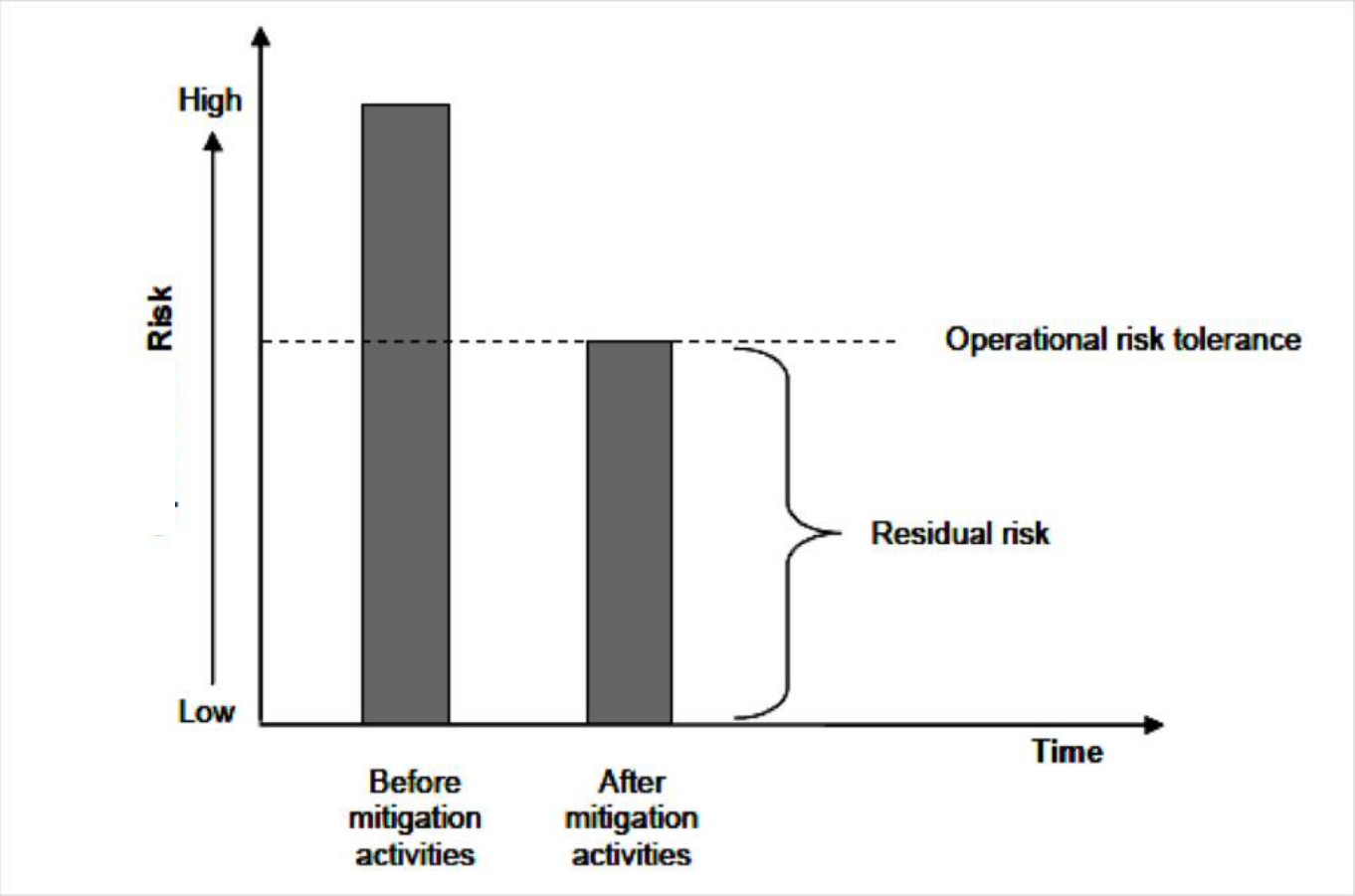
Risk Appetite

The level of uncertainty a company is willing to assume given the corresponding reward associated with the risk.

A company with **a high risk appetite would be a company accepting more uncertainty for a higher reward**, while a company with a low risk appetite would seek less uncertainty, for which it would accept a lower return.

Risk appetite is about the pursuit of risk.

Risk Tolerance



Risk Tolerance

A stated amount of risk a company is willing and able to keep in executing its business strategy — in other words, the limits of a company's capacity for taking on risk.

Risk tolerance is about what you can bear.

Risk Management

All risks will disappear!

Risk Governance in COBIT 5

- The **GOVERNANCE** domain **contains five governance processes**, one of which focuses on **stakeholder risk-related objectives**:

EDM03 Ensure risk optimisation.

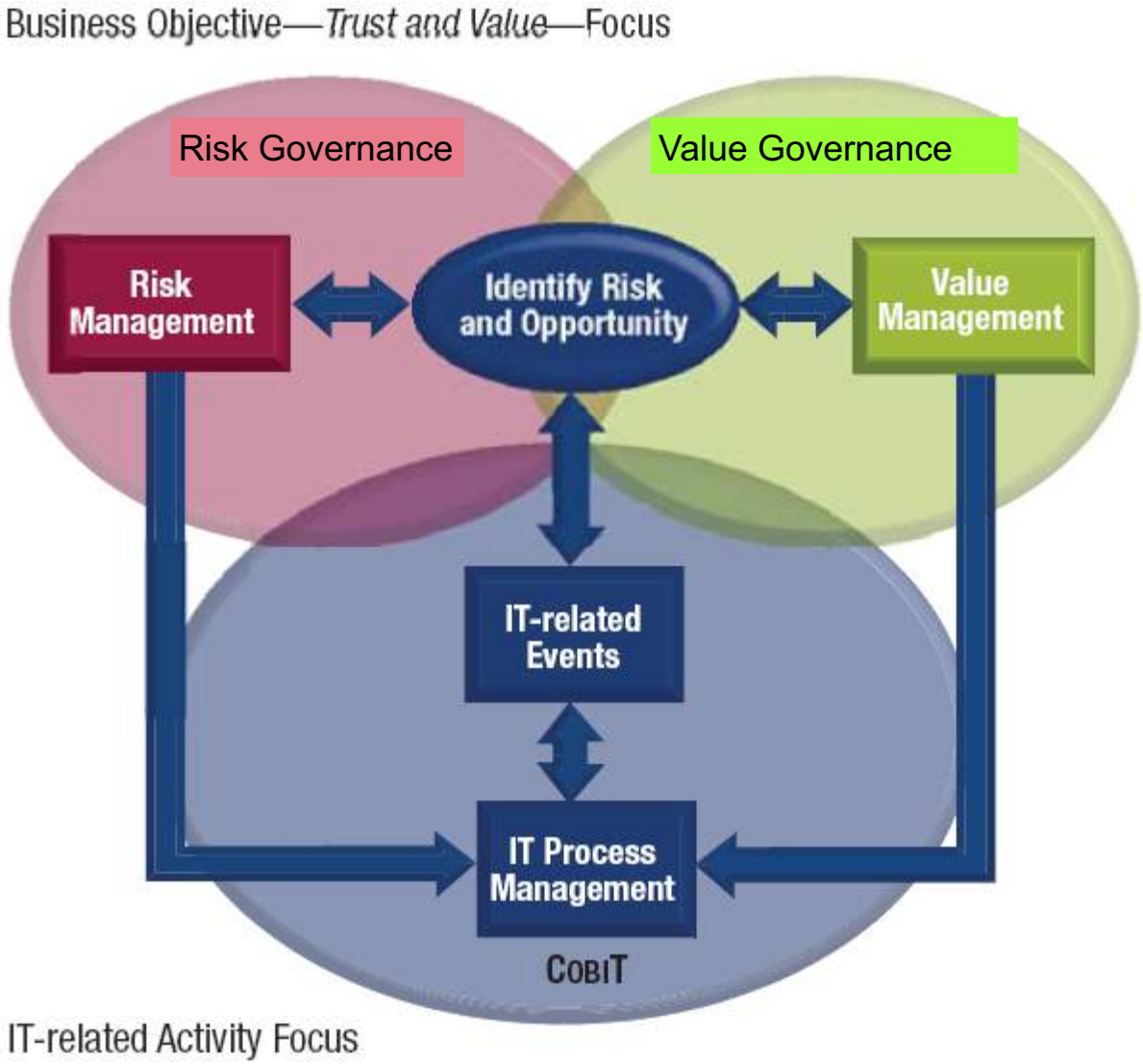
Process Description

- Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.

Process Purpose Statement

- Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.

Risk Governance



Risk Management in COBIT 5 (cont.)

- The MANAGEMENT **Align, Plan and Organise** domain contains a risk-related process:

  APO12 Manage risk.

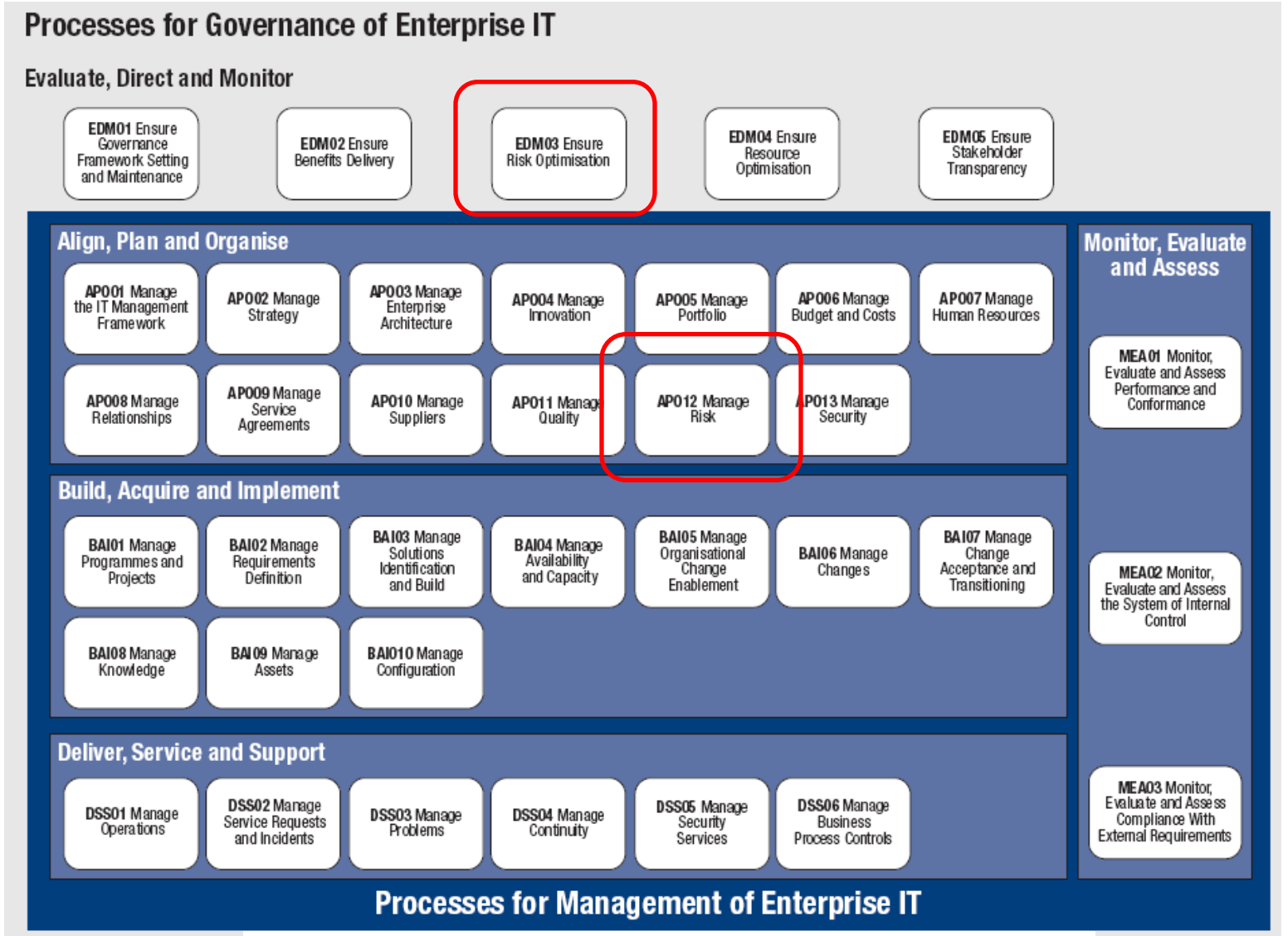
Process Description

- Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.

Process Purpose Statement

- Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.

Risk Governance and Management in COBIT 5



Risk Management in COBIT 5 (cont.)

- All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities

- **EDM03 Ensure risk optimization**: ensures that the enterprise stakeholders approach to risk is articulated to direct how risks facing the enterprise will be treated.
- **APO12 Manage risk**: provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise.
- All other processes include practices and activities that are designed to treat related risk (avoid, reduce/mitigate/control, share/transfer/accept).

Risk Management in COBIT 5 (cont.)

- In addition to activities, COBIT 5 suggests **accountabilities**, and **responsibilities** for enterprise roles and governance/management structures (**RACI charts**) for each process. These include risk-related roles.

APO12 RACI Chart

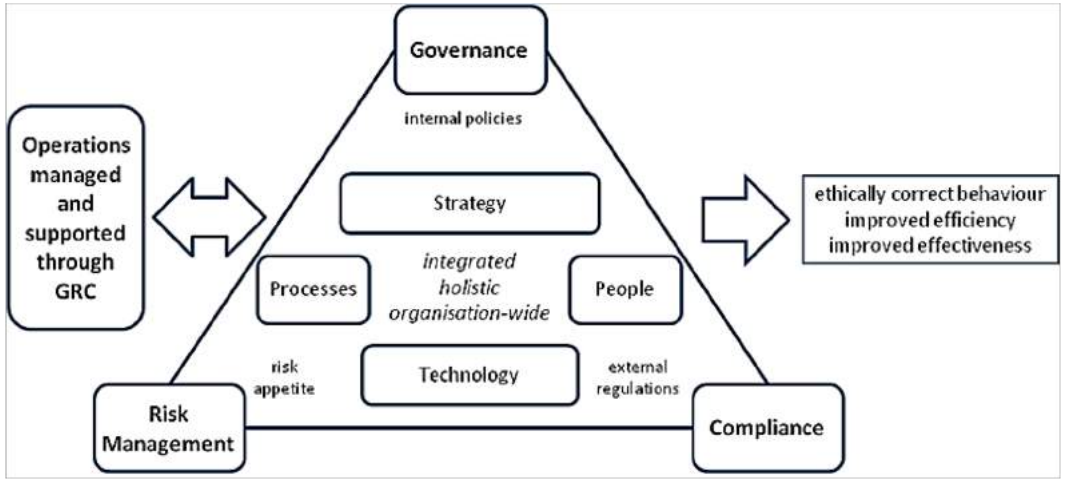
	Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
Align, Plan and Organise	APO12.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
	APO12.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
	APO12.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
	APO12.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
	APO12.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
	APO12.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Governance, Risk Management, and Compliance (GRC)

Risks Based Approach to Governance

A ship in port is safe,
but that's not what ships are built for

Governance, Risk Management, and Compliance




Governance
Strategy management
Business processes
Policies and procedures
Performance management
Risk management
Control activities
Audits
GRC
Compliance
Risk


Governance
•Strategies
•Directions
•Controls
Risk Management
•Identify
•Analyze
•Measure
•Respond
Compliance
•Adherence
•Report

GRC

The Context of GRC

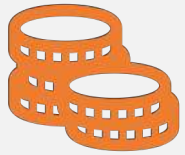
- **Governance means:**
  - Execution on a strategy
  - Putting in place right policies and procedures
  - Communication of the policies
  - Checking of the policies in action
  - Updating and evolution of the policies
  - Framework for risk and compliance
- **Risk means:**
  - Understanding and managing the risks related to your business
  - Reduce the risk of failing the compliance with a specific regulation
- **Risk means:**
  - Satisfying the external and internal standards that have been set forth for your business.

Goal of GRC

- The goal of GRC is to help a company efficiently:
  - Put policies and controls in place;
  - Fulfill compliance obligations;
  - Gather information that enables to proactively run the business;
  - Derive a competitive advantage from understanding risks.

GRC makes sure that organizations do things the right way effectively;

Drivers for GRC

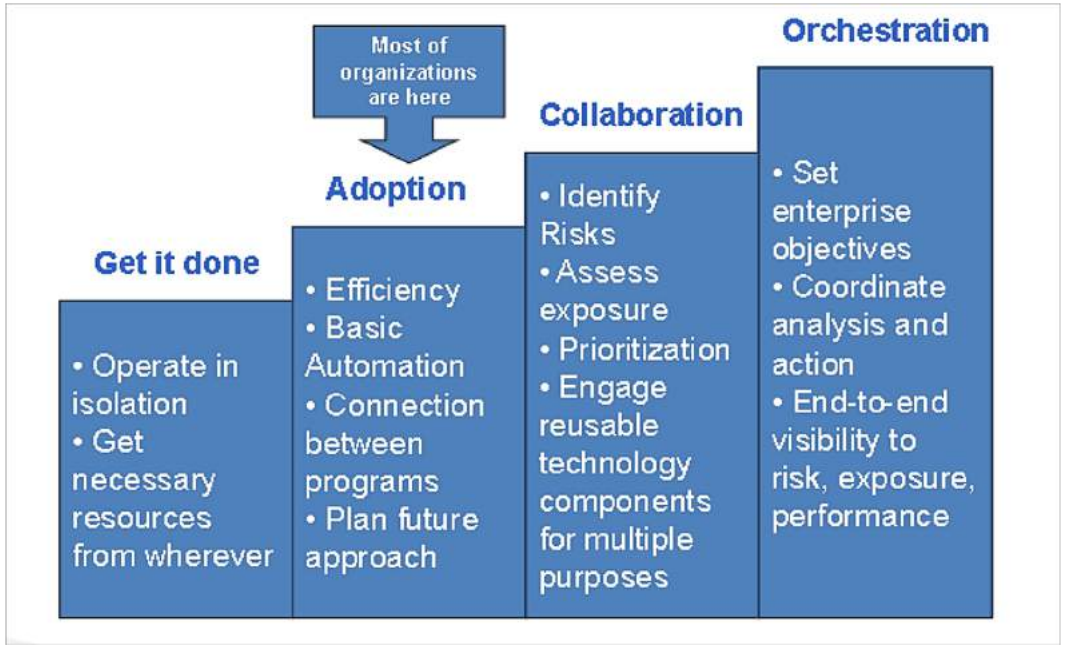


Inaccurate financial reporting will damage the financial system

Failing an audit, which must be reported in public financial statements

Reducing costs

GRC Maturity Model



About Governance in GRC

Governance in GRC is a framework within which a risk and compliance program is established

Governance defines how to determine the risks, their mitigation, procedures, policies, and compliance in GRC

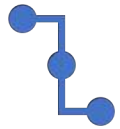
About Compliance

In relation with external environment of organization, **compliance is the process of meeting the requirements dictated by laws and regulations**

In relation with internal environment of organization, compliance is concerned with **self-defined rules or the policies defined to determine how a company does business**

Main areas of compliance are **finance, trade, environmental, health, and safety**

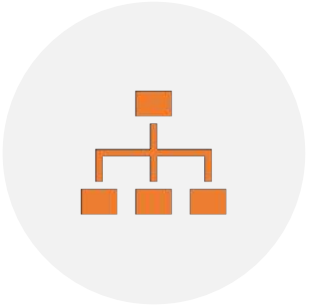
The **most important mandate** from a compliance perspective is to **have comprehensive and appropriate controls to detect the violation of the regulations**



In recent years, **SOX compliance is the one that has got the most attention and resources**

Security
(in the Context of GRC)

ACCESS CONTROL



ROLES

SEGREGATION OF DUTIES

About Access Controls and Roles

ACCESS CONTROL REFERS TO WHAT A PERSON CAN DO IN A COMPUTER APPLICATION BASED ON THE SIGN-ON (AUTHENTICATION) PROCESS.

INITIALLY PERMISSIONS WERE DIRECTLY ASSIGNED TO INDIVIDUAL USERS.

INTRODUCTION OF ROLE-BASED ACCESS MADE IT POSSIBLE TO ORGANIZE AND STREAMLINE THE PERMISSIONS BASED ON THE JOB FUNCTIONS AND BUSINESS RESPONSIBILITIES.

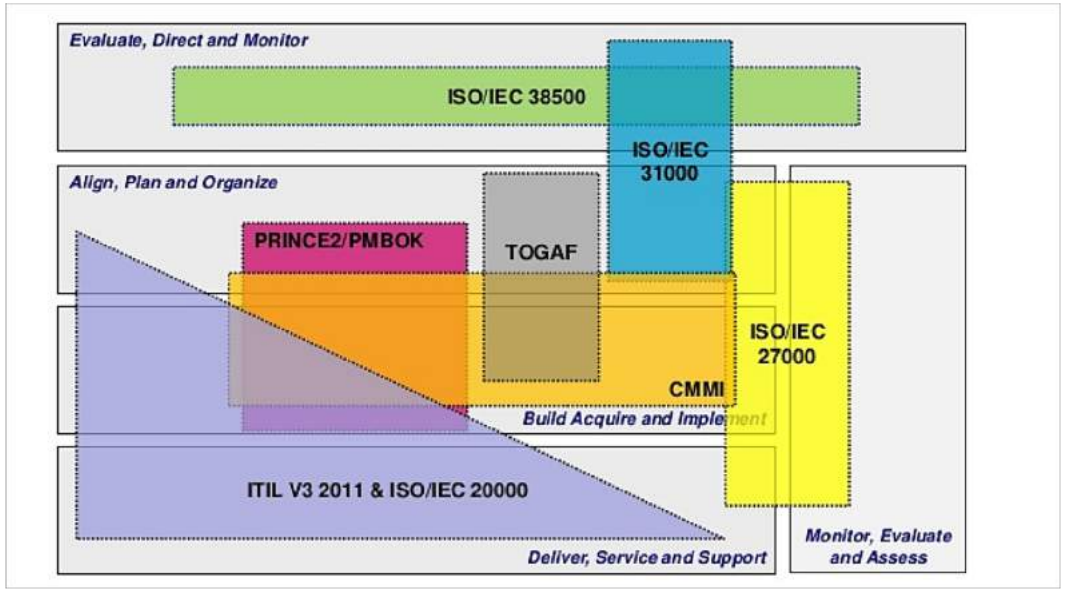
ROLE-BASED ACCESS ALLOWED TO MANAGE AND TRACK THE SEGREGATION OF DUTIES IN BUSINESS APPLICATIONS.

Main Features for Efficient and Effective GRC Management

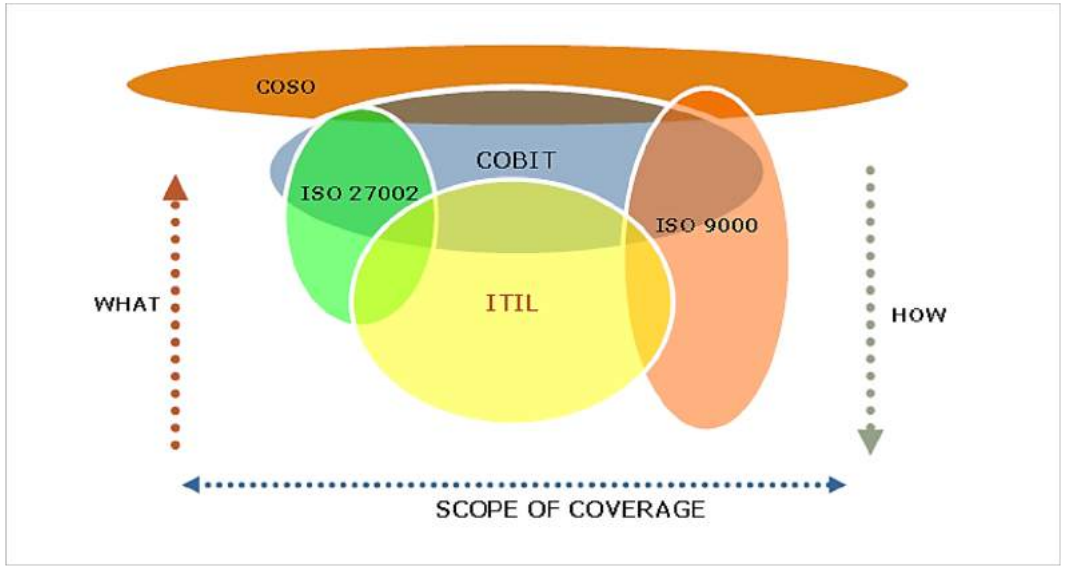
- Establish, manage and communicate the corporate and IT strategic plan;
- Enable active monitoring of current performance against goals;
- Manage enterprise and IT risks;
- Provide program, portfolio and project management for Corporate and IT investments;
- Provide a framework for defining and managing IT services;
- SLA (Service Level Agreement) Management;
- Establish the process of recording, assessing and prioritization of change requests;
- Provide a workflow to authorize changes;
- Plan and perform audits;
- Establish the full cycle of recording, classification, investigation and diagnose of incidents and problems;

Instead of

COBIT 5 Mapping Summary



COBIT and Other IT Governance Frameworks



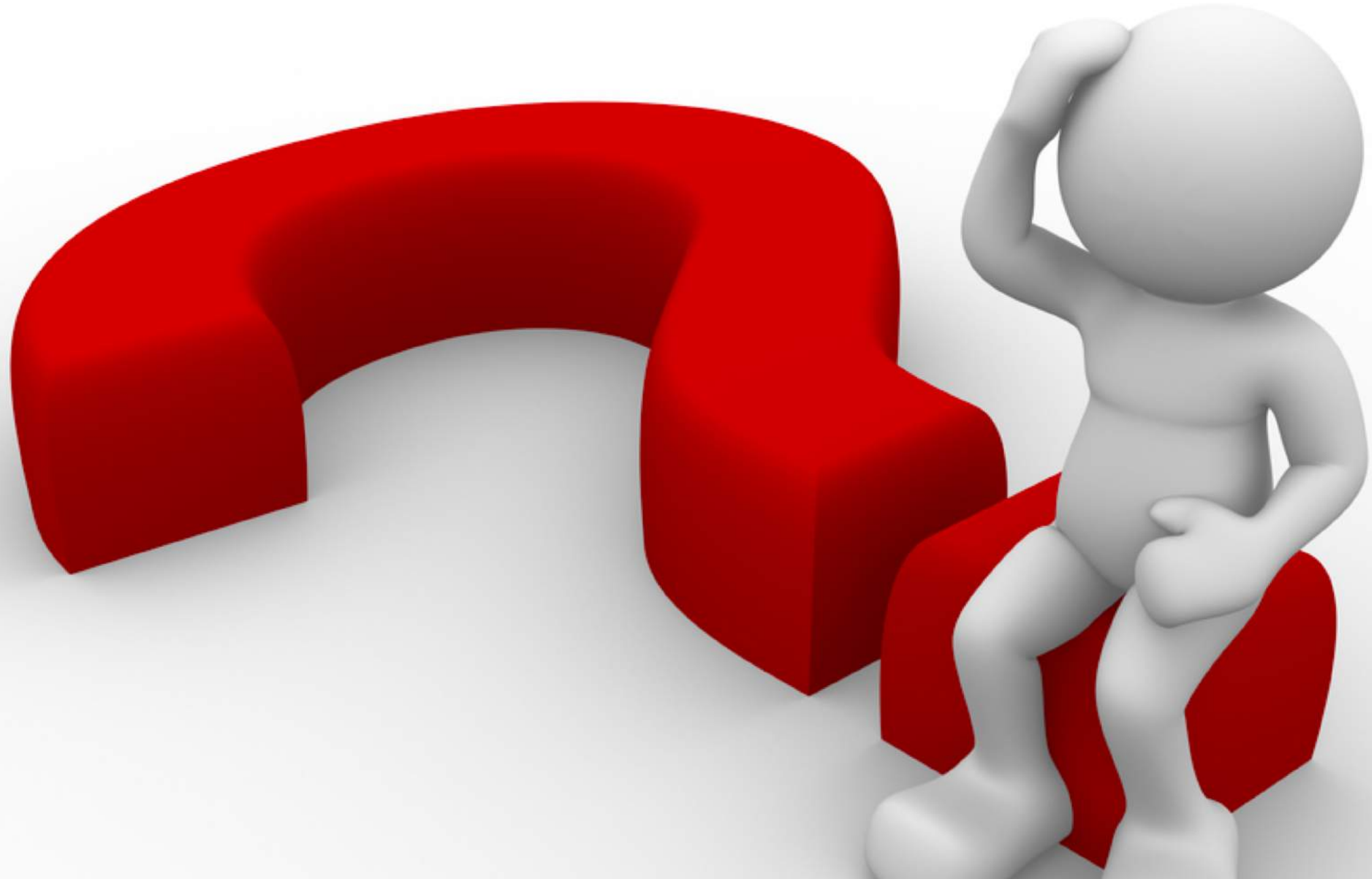
The Major Objectives of IT Governance are to:

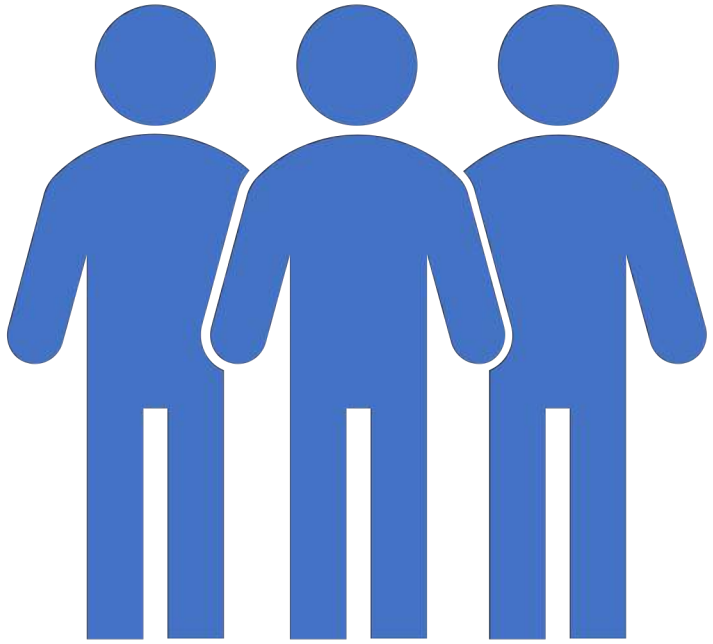
Enable	enable the strategic and tactical alignment of IT ·
Understand	understand the value and impact of IT investments (dollars, human resources, and capital)
Identify	identify opportunities for improved IT utilization
Support	support visible and transparent decision making
Establish and s ustain	establish and sustain effective IT policies
Establish	establish performance measurements
Identify and m itigate	identify and mitigate risks
Satisfy	satisfy regulatory and formal compliance requirements

Summary of COBIT 5

The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities:

- **Governance activities** related to GEIT (5 processes)
- **Risk management process**—and supporting guidance for risk management across the GEIT space
- **Compliance**—a specific focus on compliance activities within the framework and how they fit within the complete enterprise picture
- **Inclusion of GRC** arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements—silos of activity!





Next Session: 13.04.19

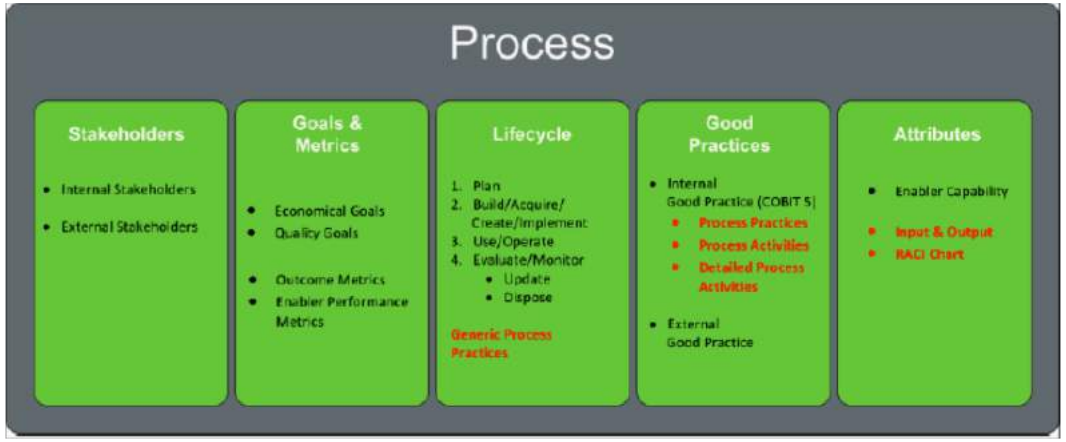
IS Infrastructure

Appendix

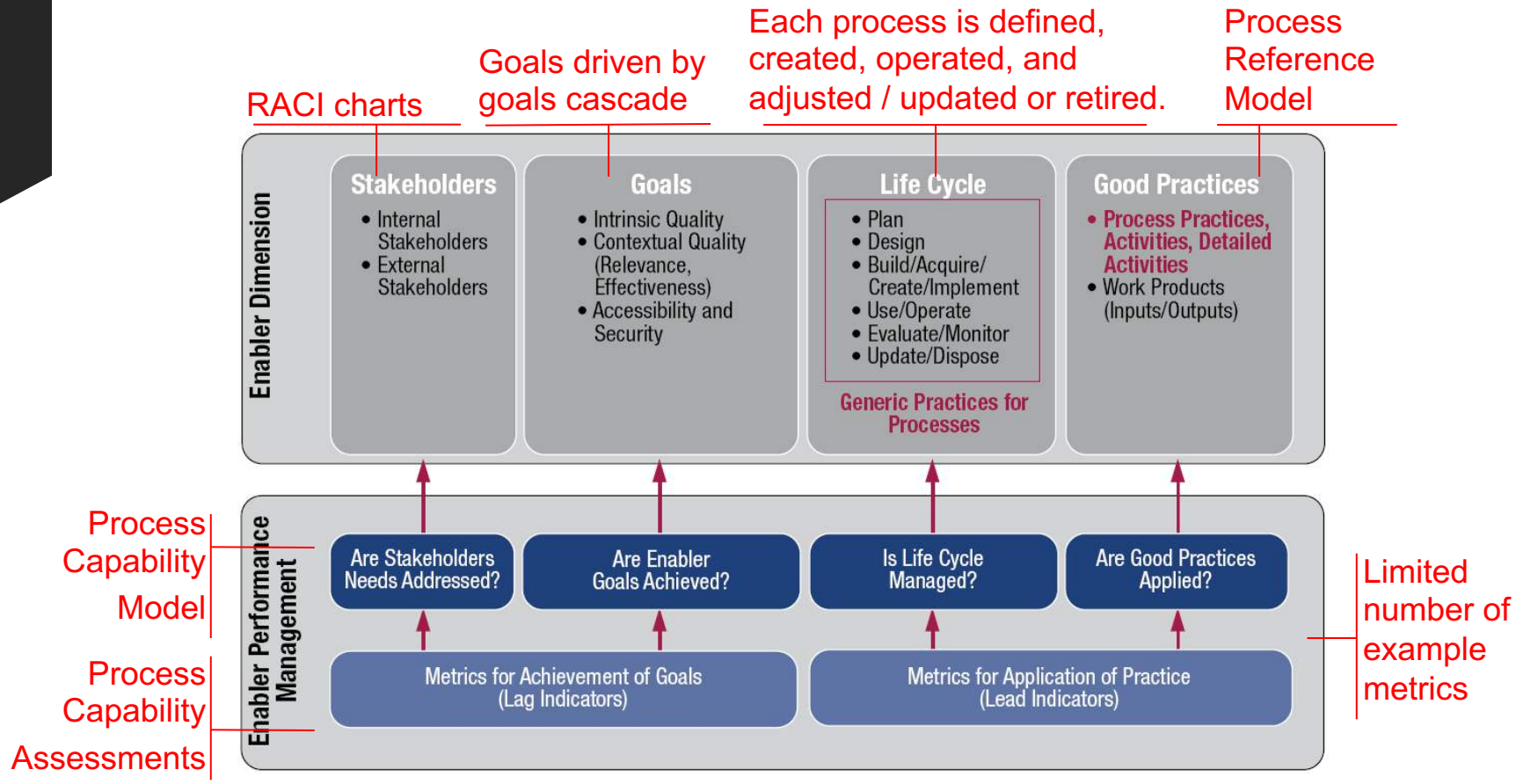
Enabler Common Dimensions Model

Enabler	Stakeholders	Goals	Life Cycle	Good Practices
Processes	• Staff • Management • Business partners • Customers	• Consistently control the conversion of org inputs (which can be other processes) into desired outputs with the influence of enterprise policies and procedures • Based on the Goals Cascade	1. Defined 2. Created 3. Operated 4. Monitored 5. Adjusted / Updated 6. Retired	
Org. Structures	• Staff • Management		1. Defined 2. Created 3. Operated 4. Monitored 5. Adjusted / Updated 6. Retired	• Escalation procedures • Delegation of authority • Span of control • Level of authority
Culture, Ethics & Behaviour	• Staff • Management • Business partners • Customers	• Guide individual and enterprise behaviour to archive maximum value creation. • Learn from mistakes	1. Defined 2. Created 3. Operated 4. Monitored 5. Adjusted / Updated 6. Retired	• Communication • Enforcement • Incentives and rewards • Rules and Norms • Champions
Information	• Staff • Management • Business partners • Customers • Volunteers • Regulators • Shareholders	• Effectiveness • Efficiency • Integrity • Availability • Confidentiality • Compliance	1. Business IT Processes generate & Process Data into Information. 2. Information is transformed into Knowledge. 3. Knowledge creates value. 4. Value drives Business IT processes(see No.1)	• Physical (Carrier, Media) • Empirical (User Interface) • Syntactic (Language, Format) • Semantic (Meaning), Type, Currency, Level • Pragmatic (Use), Includes Retention, Status, Contingency, Novelty • Social (Context)
Principles Policies and Frameworks	• Staff • Management • Regulators • Customers • Board Members	• Support enterprise gaols • Frameworks create consistent view of policies and offer a structure for policy maintenance.	1. Create 2. Review 3. Amend 4. Dispose	
People, Skill and Competencies	• Staff • Management • Business partners • Customers • Shareholders	• Elevate educational qualifications and tech. skills level of staff • Retain Industry Knowledge	1. Defined 2. Created 3. Operated 4. Monitored 5. Adjusted / Updated 6. Retired	• Define skills requirements • Refine skills categories into levels (trainee, Expert, etc) • Maintain skills description
Services, Infrastructure And Applications	• Staff • Management • Business partners • Customers • Shareholders	• Applications • Infrastructure • Technology • Service levels	1. Defined 2. Created 3. Operated 4. Monitored 5. Adjusted / Updated 6. Retired	• Define architecture principles • Define architecture viewpoints • Target transition • Baselines

Process Enabler Model



Enabler Dimensions - Processes



Source: COBIT® 5: Enabling Processes, figure 8. © 2012 ISACA® All rights reserved.

148

Enabler Processes: Content Structure for All Processes

- *Process Identification*
- *Process Description*
- *Process Purpose Statement*
- *Goal Cascade Information*
- *Process Goals and Metrics*
- *RACI Chart*
- *Detailed Description of Process Practices*
  - *Practice title and description*
  - *Practice inputs and outputs w/indication of origin & destination*
  - *Process activities further detailing the practices*
- *Related Guidance*