MONASH University

FIT2090
BUSINESS INFORMATION SYSTEMS AND PROCESSES

Lecture 10 IT Governance

CLAYTON, FACULTY OF INFORMATION TECHNOLOGY
MONASH UNIVERSITY

GROUP OF EIGHT AUSTRALIA

Why are Controls like Governance Needed?

1. To provide reasonable assurance that the goals of each business process are being achieved.
2. To mitigate the risk that the enterprise will be exposed to some type of harm, danger, or loss (including loss caused by *fraud* or other intentional and unintentional acts).
3. To provide reasonable assurance that the company is in compliance with applicable legal and regulatory obligations.

What is governance?

- The term '**governance**' is derived from the Greek word "**Kubernan**" meaning the process of continuously adjusting.
- Governance refers to "a set of processes, rules, customs, policies, and traditions that determine how to direct and control management activities"
- Hence, governance means adjusting management activities in line with business goals
- Governance applies to many areas of business (i.e. it is not restricted to IT only)
  - Financial governance
  - Marketing governance
  - IT governance
- Senior management is eventually responsible for GOOD governance

What is governance?

GOOD governance implies:

- Greater control on financial matters (less corruption, scandals)
- Greater clarity into management decision making and accountability
- Less abuse of loopholes in company policies by some opportunist employees (Avoid negative publicity)
- Better organisational performance

Source: Unescap (2005)

What is governance?

- Interest in corporate governance has grown because
  - financial scandals leading to bankruptcies (e.g. Enron, Tyco and Worldcom in the US and OneTel and Ansett in Australia)
  - Media reported that several executives received outrageously excessive compensation
- E.g. Richard Grasso at the NYSE (New York Stock Exchange) was fired by the board of directors after his US$139 million annual salary became public
- This example highlights the need for good corporate governance in order to identify problems early

Sarbanes-Oxley Act (SOX) of 2002

- Created public company accounting oversight board (PCAOB).
- Strengthened auditor independence rules.
- Increased accountability of company officers and directors.
- Mandated upper management to take responsibility for the company's internal control structure.
- Enhanced the quality of financial reporting.
- Increased white collar crime penalties.

Key Elements of SOX

- Section 201—prohibits audit firms from providing a wide array of nonaudit services to audit clients; in particular, the act prohibits consulting engagements involving the design and implementation of financial information systems.
- Section 302—CEOs and CFOs must certify quarterly and annual financial statements.
- Section 404—Mandates the annual report filed with the SEC include an internal control report.

What is IT governance?

- Van Grembergren (2002) defines IT governance “as the organisational capacity (exercised by the board, executive management and IT management) to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT”.
- According to IT Governance Institute (2003), IT governance as: “It is an *integral part of enterprise governance* and consists of leadership, and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategy and objectives.” IT governance is not independent of enterprise/corporate governance

What is IT governance?

According to Luftman et al. (2004), “IT governance describes the selection and use of organisational processes to make **DECISIONS** about IT matters.

According to them, IT governance is about:

- **WHO** makes IT related (including investment) decisions (i.e. Who has the power to make such decisions?)
- **WHY** they make these decisions (alignment)
  - To bring alignment between IT and business
  - To better support business goals
  - To add value to business deliverables
  - To better support value adding processes (Porter’s value chain processes)
- **HOW** they make these decisions (decision making process)

What is IT Governance?

- Decisions about IT investments are made either by business management without active involvement of IT management or vice versa –> an investment that performs poorly or not at all
- E.g. when senior IT managers alone are involved in deciding to web-enable customer relationship process by introducing web-enabled CRM solution, it may be:
  - highly reliable
  - and easy to upgrade
  - but may be inadequate to match the business needs
- When only senior business managers are involved for deciding a CRM solution, it may:
  - satisfy the business needs but may be incompatible with other systems and data integration may become a serious challenge

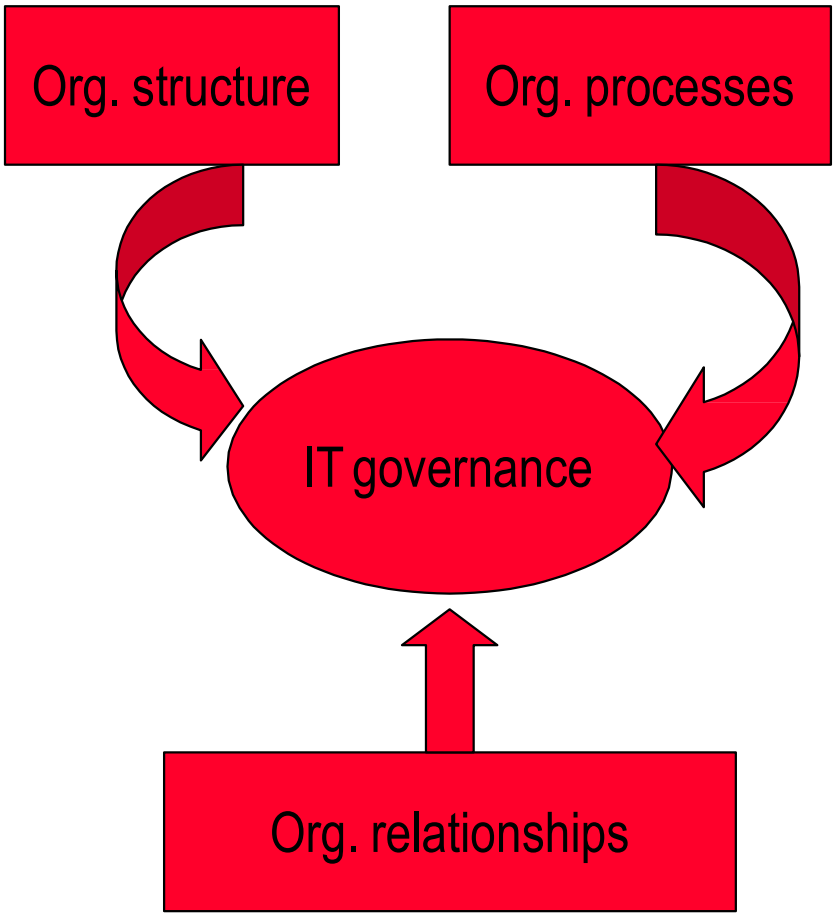
What is IT Governance? …

- IT function overpromises (& underdelivers) return on IT investments. Hence, there exists a **serious gap** between business expectations from IT investment and ability of IT function to meet those expectations
- The **CREDBILITY GAP** (which results in poor IT governance) is manifested in terms of the following **symptoms**:
  - Frequently fired IT managers
  - Frequent IT reorganisations
  - Little communication between IT and users
  - Ongoing conflicts between IT and business
  - IT projects are not used & unhappy users

What is IT governance? A conceptual diagram

IT governance can be expressed using a mixture of:

- organisational structures (e.g. CIO included as a board member, IT strategy committee, IT steering committee)
- processes (e.g. SLA, COBIT, ITIL, IT alignment maturity models)
- and relationship mechanisms (e.g. career cross-over, joint incentive)



What are the motivations for organizations to implement IT governance infrastructures?

- Compliance with government regulations (e.g. Sarbanes Oxley Act in USA and Basel II Committee in Europe)
- To avoid being in a competitive disadvantageous position
- High failure rate of IT projects
- Increasing costs of IT (e.g. IT budget exceeding 4% of annual revenue). Hence, to avoid wastage of money

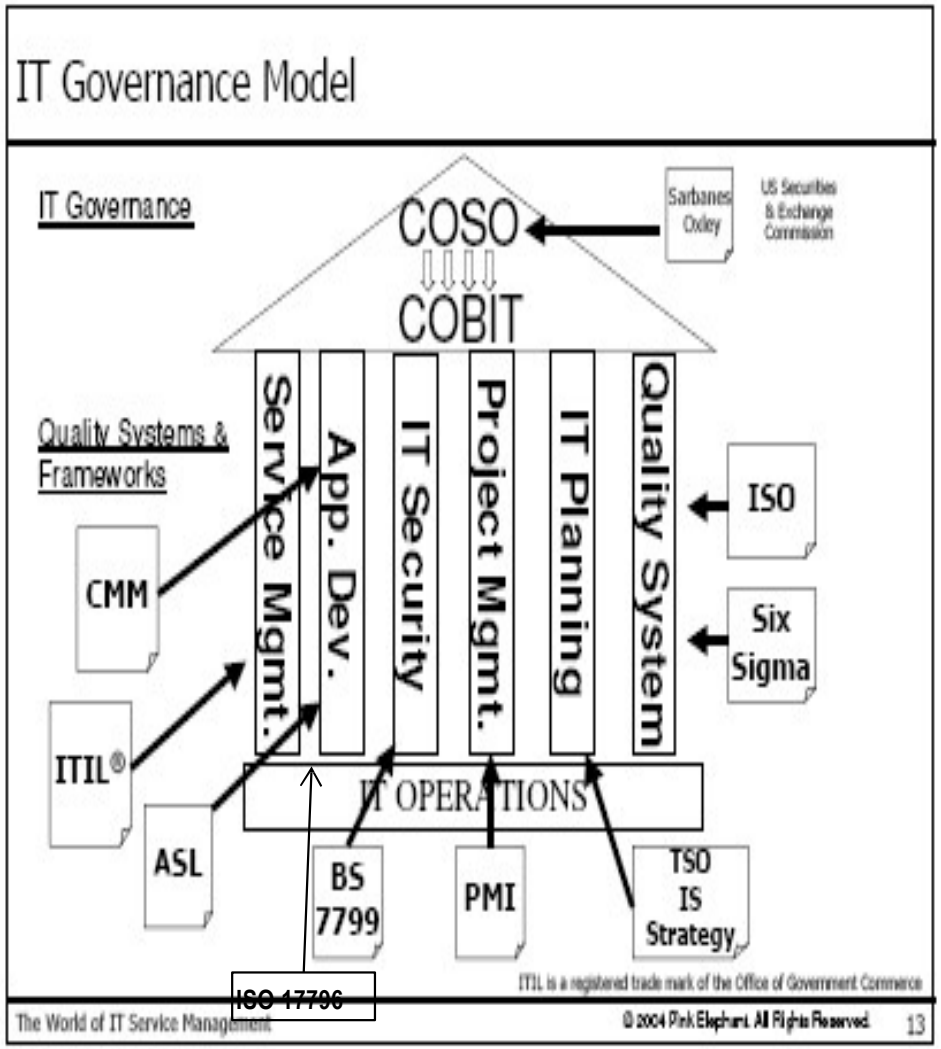
IT Governance Frameworks

The following two frameworks are widely used:

- ITIL (IT Infrastructure Library) is a framework for IT services management
- COBIT (Control OBjectives for Information and related Technology) is a more comprehensive framework than ITIL and covers wider governance issues than ITIL
- Other relevant standards and frameworks include:
  - COSO (generic control framework)
  - ISO 9000 (Quality standards)
  - ISO 17796 (Info. security standards)
  - ISO 27000 (Info. security standards)

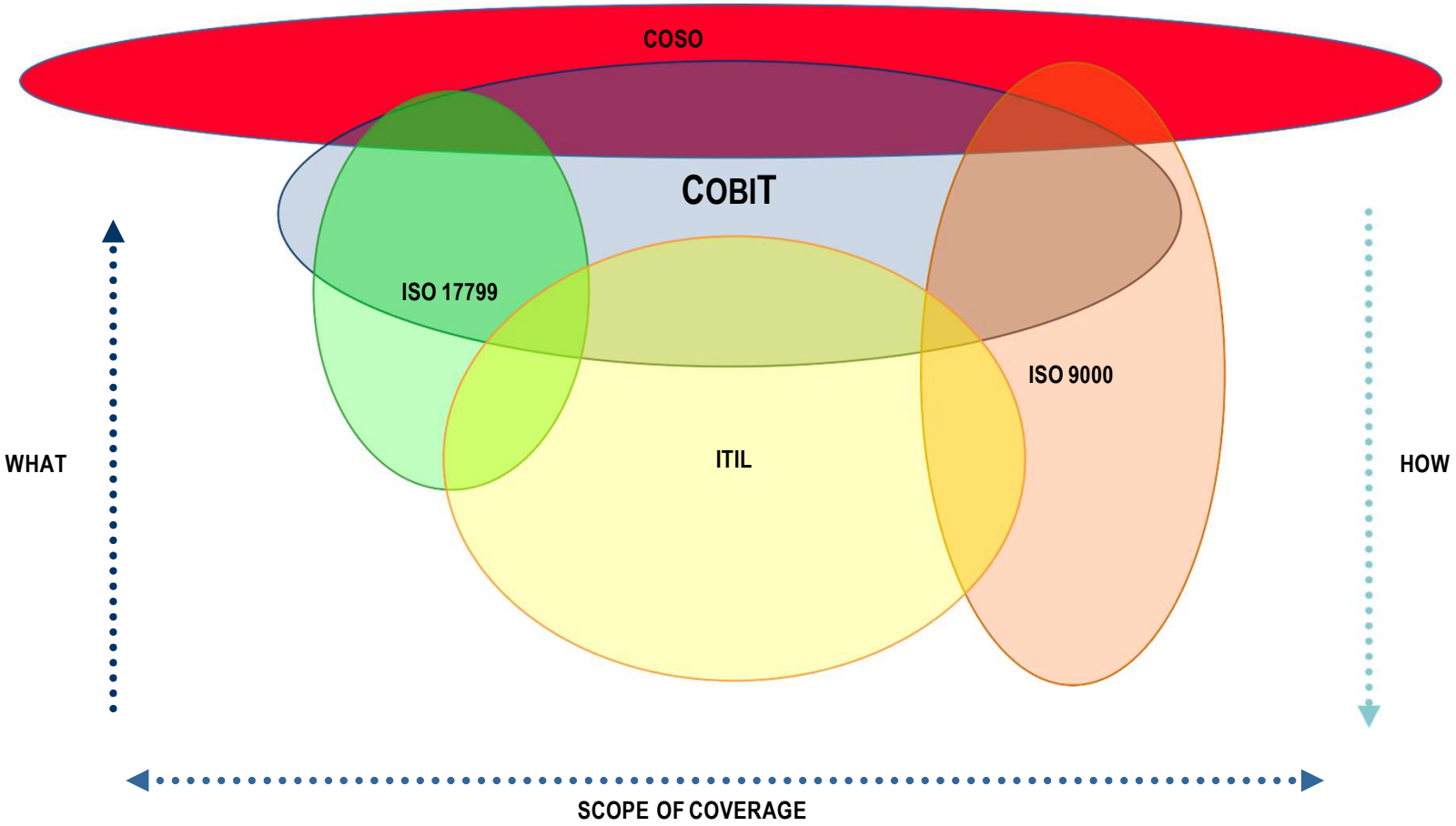
IT Governance Frameworks

- The relationship among these frameworks, standards and tools is shown in Figure.
- ITIL primarily focuses on the management (support and delivery) aspects of IT services to support business aims.
- In Version 3, ITIL is however trying to address:
  - Application Development
  - and Security aspects of IT function as well



Relationship among IT Governance Frameworks

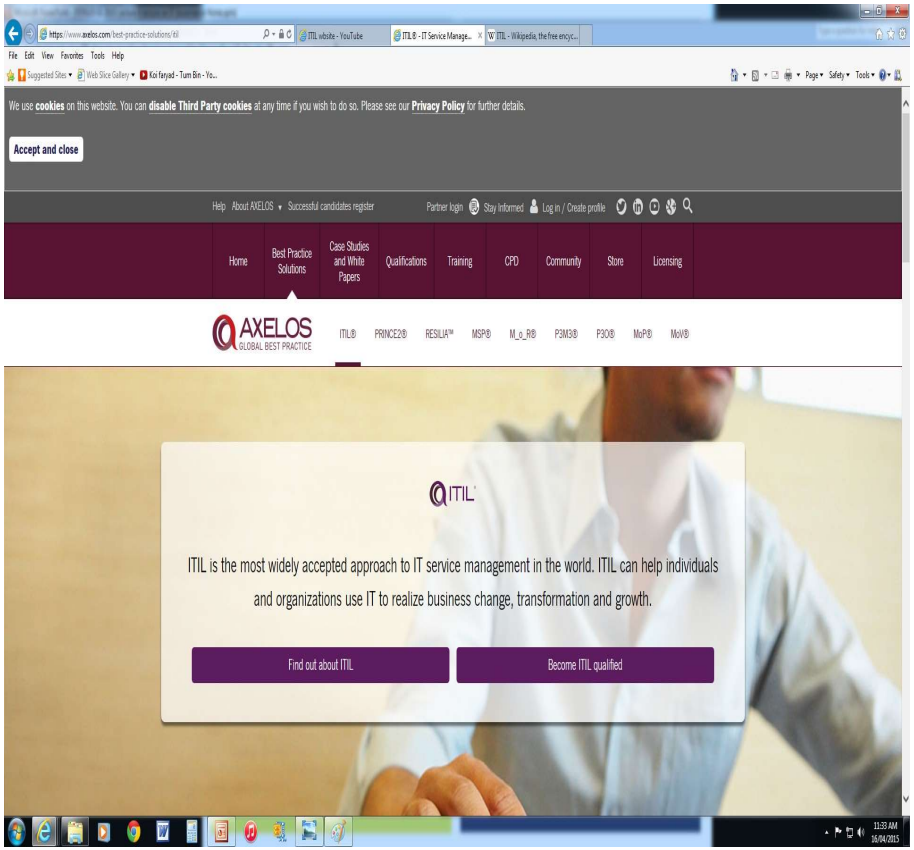
Organisations will consider and use a variety of IT models, standards and best practices. These must be understood in order to consider how they can be used together, with **COBIT acting as the consolidator ('UMBRELLA')**.



ITIL framework - Background

- The UK Government's Central Computer and Telecommunications Agency (CCTA) in the 1980s developed ITIL
- ITIL represents a REPOSITORY of BEST PRACTICES in IT Service Management and related processes
- Over 15,000 organisations worldwide have adopted ITIL, including: British Airways, HP, IBM & MicroSoft, **CenterLink (Australia)**
- Since the 1980s, there were 3 major revisions of ITIL
- Since July 2013, ITIL has been owned by AXELOS Ltd

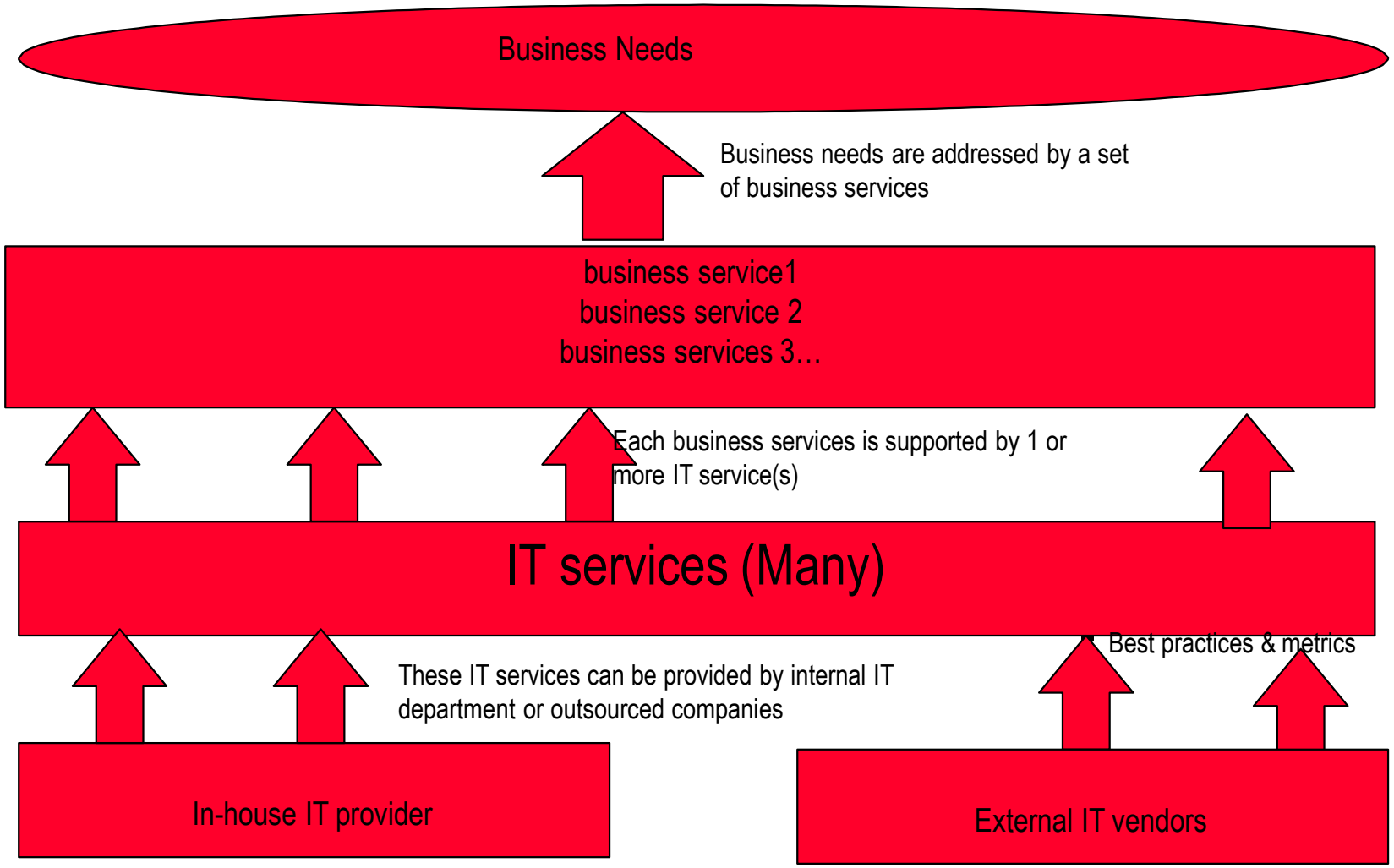
ITIL website at: **https://www.axelos.com/best-practice-solutions/itil**



ITIL Core Concepts

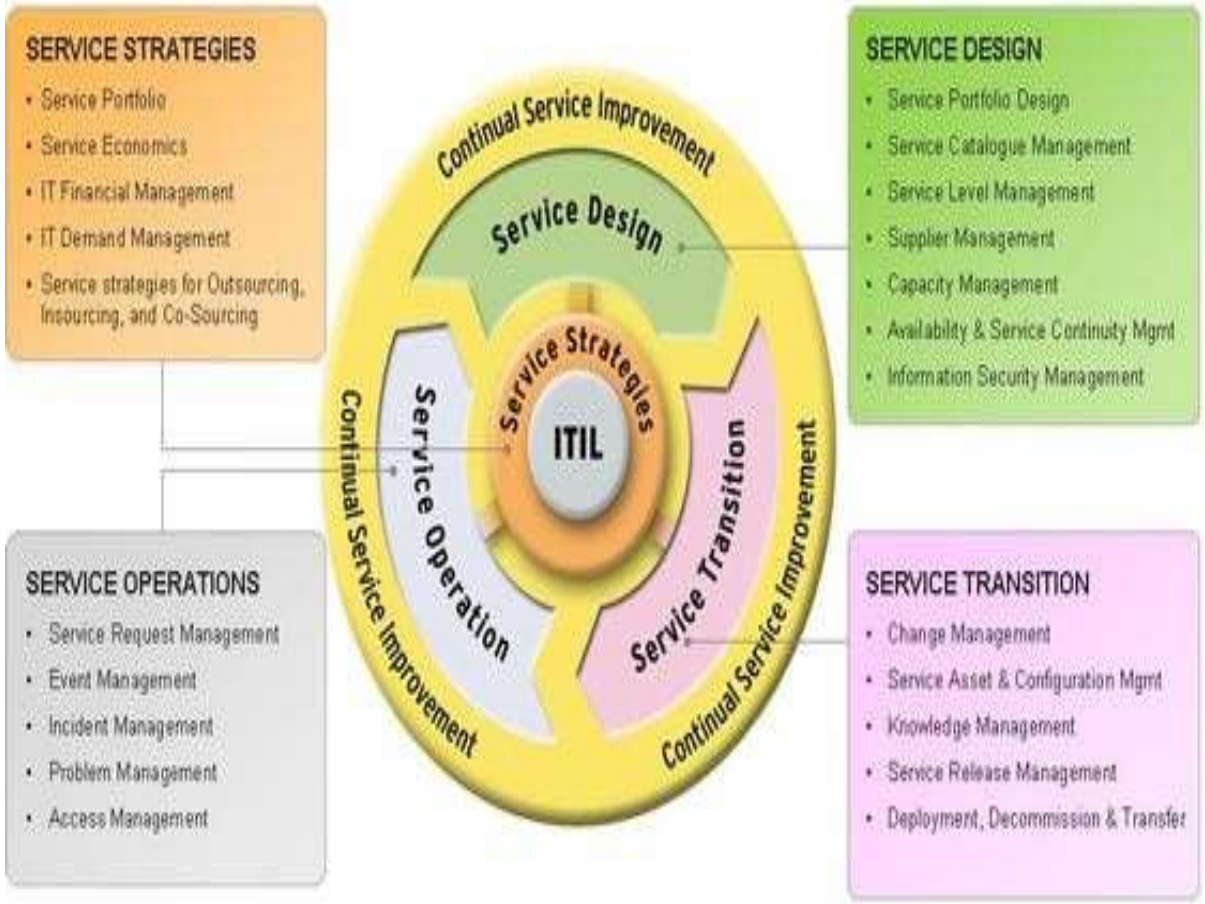
- At the core of ITIL, lies the concept of "**SERVICE**"
- A service is '*something that provides value to customers*".
- Services that customers (end-users) can directly consume are called business services.
- Examples:
  - payroll service
  - delivery of financial services to customers of a bank
- Successful delivery of Business Services often depends on:
  - one or more IT Services
- IT services can be provided by (see next slide):
  - internal IT department
  - external IT vendors

ITIL Core Concepts



ITIL Version 3

- ITIL consists of 5 sets of IT processes to create and deliver IT services
  - ITIL service strategy
  - ITIL service design
  - ITIL service transition
  - ITIL service operations
  - ITIL continual service improvement



ITIL youtube video

- https://www.youtube.com/watch?v=M9_0_BkqwzM
- This video suggests that:
  - ITIL helps the IT department to deliver better level of IT services to the end-users and includes 5 types of processes (tasks) carried out by an IT department

ITIL Life Cycle	Description
ITIL service strategy	Assessing the current situation and the customer needs. Informing IT strategy to align It with core business
ITIL service design	Planning and designing of IT services provided by the IT department to support core business
ITIL service transition	Transition of new and revised IT services from planning and development phase into operational phase. It includes: change management,
ITIL service operations	To ensure that IT services are delivered within agreed upon service levels. It includes problem management, incident management, and access management
ITIL continual service improvement	Identifies for improvement opportunity of IT services. It includes KPIs to measure performance of IT services and IT processes

ITIL Process 1: Service strategy

The LIFECYCLE starts with Service Strategy. It involves:

- Identifying what IT services are to be offered (**IT Service Portfolio**)
- Who the IT services offered to (Who are customers)
- What is the demand of the IT services among customers
- How the customers will measure the value of the IT services
- How the resources will be assigned to deliver IT services

Generally, **IT SERVICE VALUE** is made of 2 components:

- **Service utility**: What the customers get from the service
  - Example: time savings and convenience
- **Service warranty**: the quality of service in terms of availability and security of service
  - Example: Is the transaction secure? 24x7 availability

ITIL Service Strategy: IT Financial Management

- These processes are concerned with determining the costs of IT services
- Organisations closely monitor costs and map them to each IT service

IT services	Type of Costs			
	Development	maintenance	Capital	Operations
Help desk	$	$	$	$
Printing	$	$	$	$
Data security	$	$	$	$

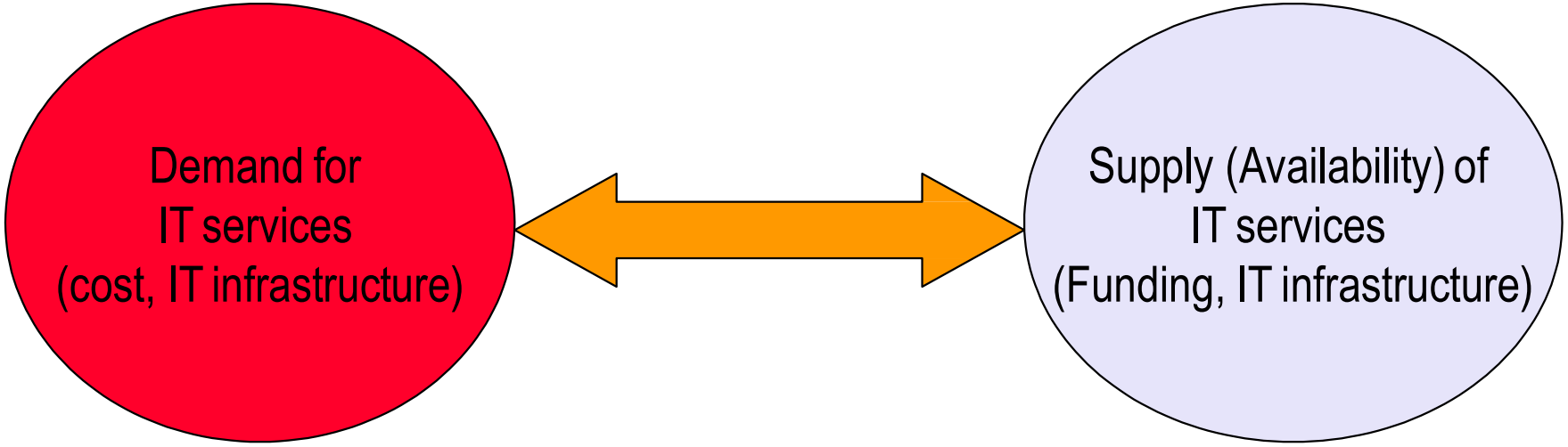
ITIL Process 2: Service design

Once IT services are identified, the service design stage is then concerned with designing secure IT infrastructure, applications, databases, risks mitigation, vendors for delivering each identified IT service

IT service	Infrastructure	Applications	databases	Risks mitigation	Vendors/ in-house
Help desk					
Printing					
Data security					

ITIL Service Design: Capacity Management

- Customer expectations often exceed technical capabilities.
- Capacity Management includes those processes which ensure that the capacity of IT services and the IT infrastructure is adequate to deliver:
  - the agreed service level targets in a
    - cost effective
    - and timely manner



ITIL Service Design: Availability Management

- The interdependency today between business processes and IT operation is that when IT stops, the business stops as well
- Processes within **Availability management** ensure that plans are in place for quick restoration of IT services in the event of IT infrastructure component failure
- Example: netbanking availability, ATM availability, airline reservation system availability
- Failure to provide business services due to unavailability of IT means:
  - Customer dissatisfaction
  - Financial loss
  - Loss of reputation of the business

ITIL Process 3: Service Transition

- The roles of Service Transition are:
  - to deliver IT services (that have been designed) to customers
  - and put them into operational use for customers
- If business circumstances or requirements have changed since service design, then modifications are made during this stage in order to deliver the required IT service
- As such, there is a strong focus on CHANGE MANAGEMENT at this stage

ITIL Service Transition: Change Management & Release Management

A **CHANGE is an action** that results in a new status of a process

- Change management includes those IT processes which ensure that no changes are made in IT services without:
  - proper authorisation
  - and testing
- **Release management** includes those processes which ensure that:

  -only Authorised and Correct versions of software and hardware are made available for operation

ITIL Process 4: Service Operation

- Once transitioned, Service Operation then delivers:
  - the IT services on an ongoing basis
  - overseeing the daily overall health (e.g. service warranty) of the IT service
- This includes:
  - managing disruptions to service through rapid restoration of incidents (Incident management, help desk)
  - determining the root cause of problems (including help desk) and detecting trends associated with recurring issues (problem management)

ITIL Process 5: Continual Service Improvement (CSI)

- This stage collects data (performance metrics) about the performance of the delivered IT services
- For the Internet banking application, this stage would ask such questions as:
  - Does the delivered online banking solution take too long (time data) to perform transactions?
  - Are the reports generated by the system used by the customers (number of reports prepared by users)?
  - Etc.
  - Etc.

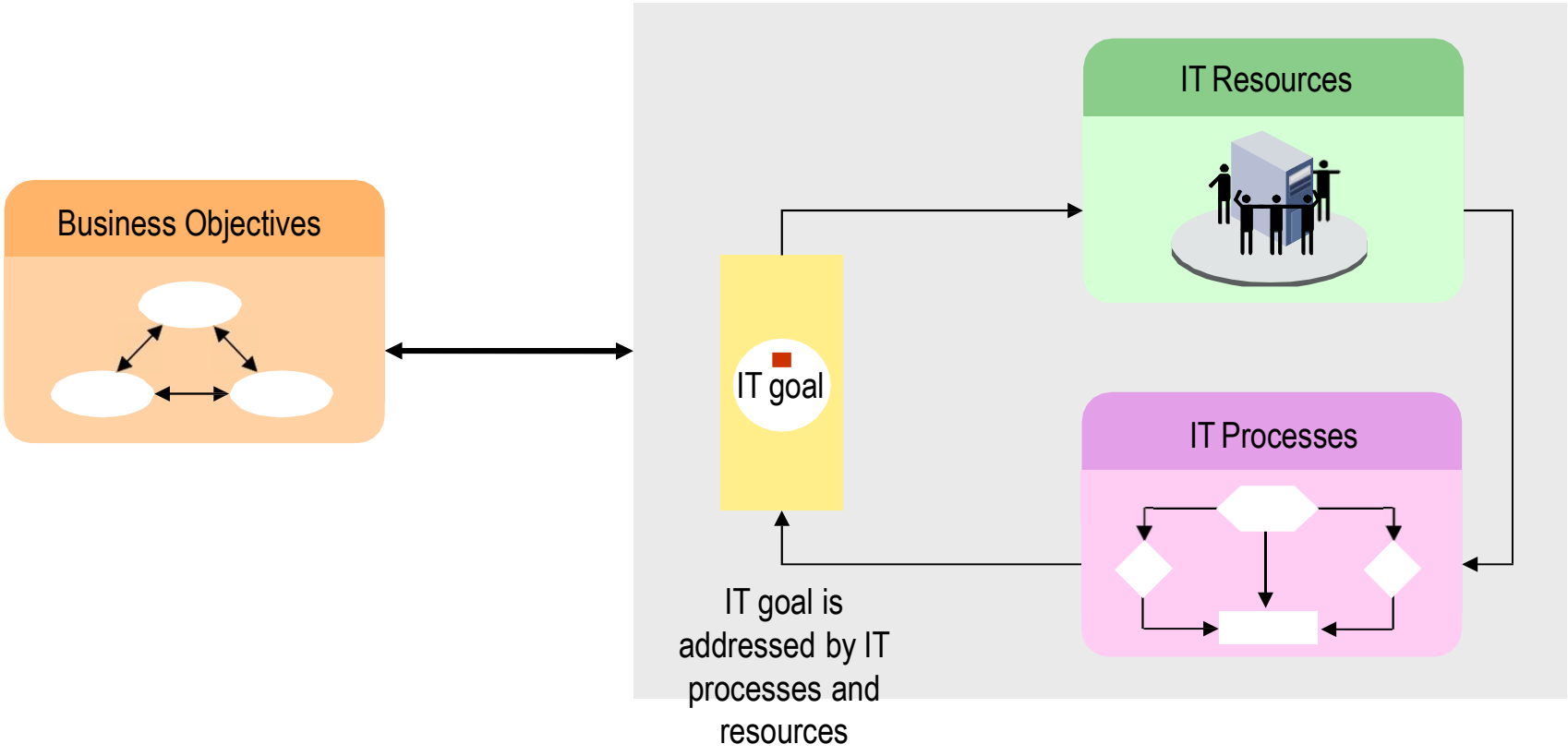
ITIL: Another simple but interesting video

- https://www.youtube.com/watch?v=vBguassbAzo
- This video suggests that:
  - ITIL helps organisations to lower costs and improve delivery of IT services
  - ITIL helps IT departments to deliver value to their organisations

ITIL Life Cycle	Restaurant Service Life Cycle
ITIL service strategy Key issues: strategic needs, budget constraints	Restaurant theming (made at HQ): Key factors: Atmosphere, cuisine and price
ITIL service design Key issues: defining IT services that meets business requirements	Menu design (By chef) Key factors: ingredients, production costs, suppliers
ITIL service transition IT plans each releases and changes	Kitchen practice, prepare and document all recipe
ITIL service operations Service desk takes ownership of delivering all IT services	Waiters focus on delivery and own overall customer satisfaction
ITIL continual service improvement To constantly measure and improve the business contribution of each IT service	Maitre d' to coordinate restaurant activities and keeping up the standards of the restaurant

COBIT: An IT Governance Framework

- A range of IT resources are needed to support IT processes
- IT goals are addressed by IT processes and resources

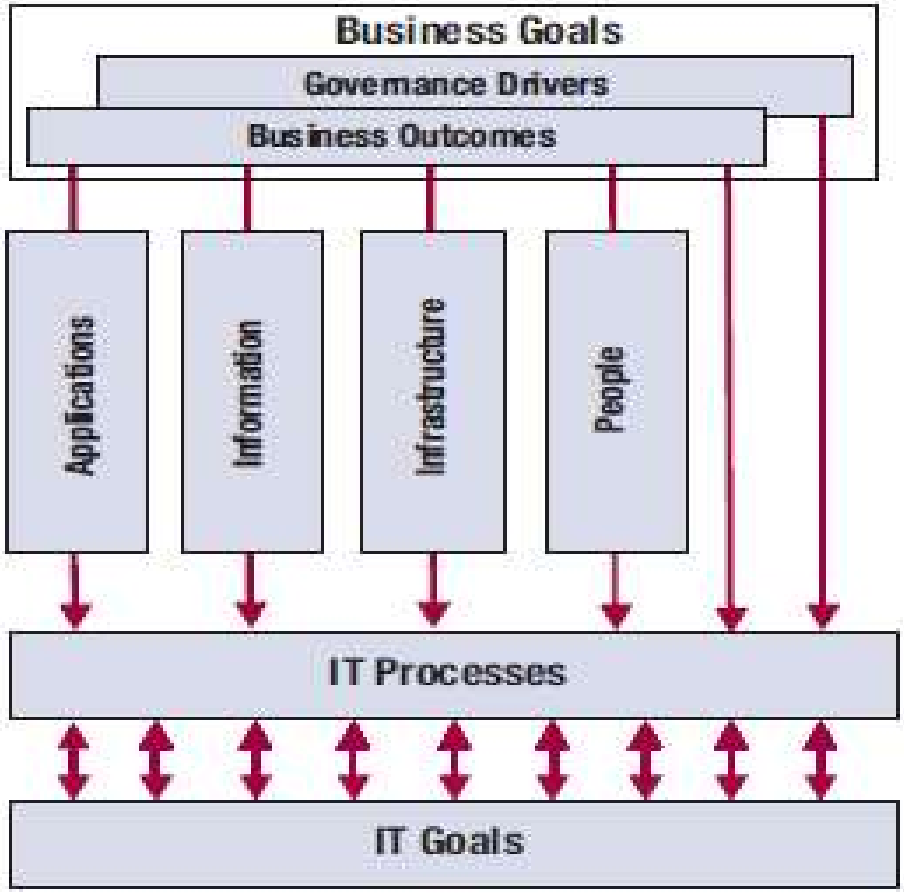


COBIT: An IT governance framework

(Many IT resources are needed to support IT processes)

- IT resources include:
  - People
  - Applications
  - Information
  - Infrastructure

- IT resources support execution of IT processes which in turn address IT goals



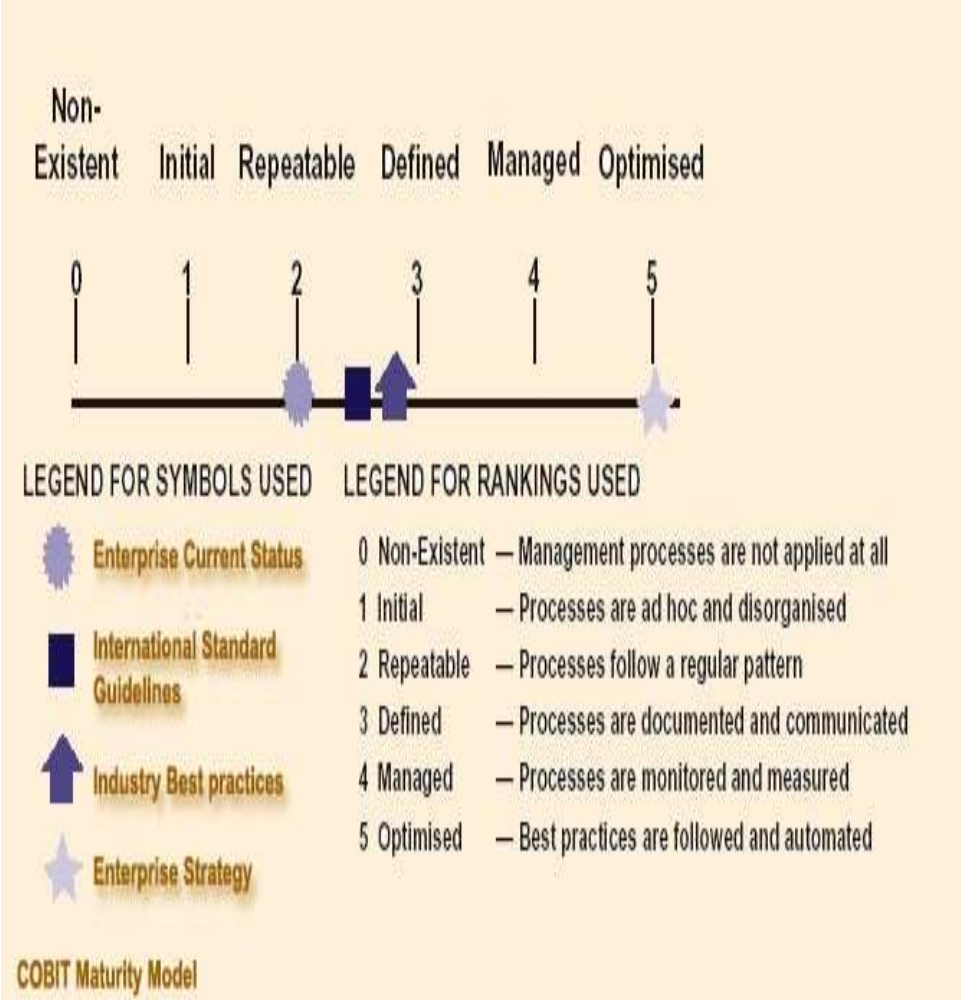
COBIT: An IT Governance Framework (Concept of control in COBIT)

- Performance of each IT process is measured
- For DS5 Ensure System Security
  - KPI is: Number of incidents because of unauthorised access
- DS2: Manage third-party services
  - KPIs: Number of review meetings
  - Number of contract amendments
  - Frequency of service level reports
  - Number of outstanding issues
  - Percent of contracts outstanding for legal review

COBIT: An IT governance framework (Maturity level of IT processes)

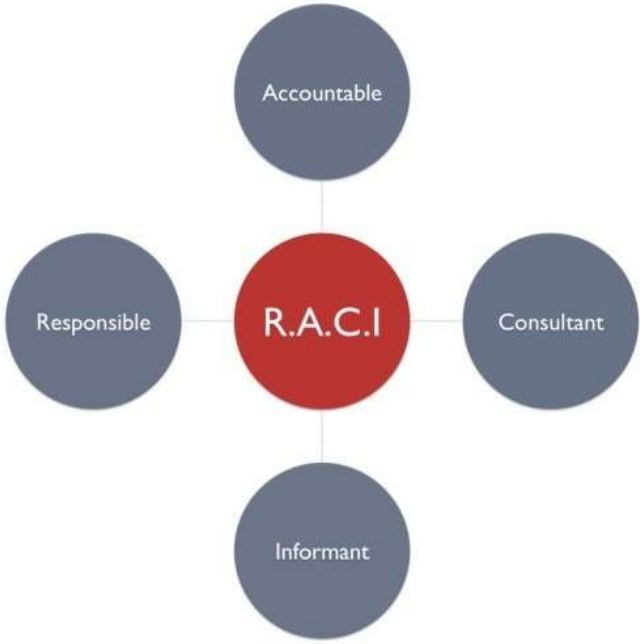
For each COBIT IT process, the maturity level can be evaluated on a scale of 0 to 5 and can be used for benchmarking purpose:

- 0 (Non-existent): the process is not applied at all
- 1 (Initial): the process is ad-hoc in nature and disorganised
- 2 (Repeatable): The process follows a regular pattern
- 3 (Defined): The process is *well documented* and communicated
- 4 (Managed): The process is monitored and measured
- 5 (Optimised): best practices are followed and automated



COBIT: An IT Governance Framework …
– IT Process Ownership and RACI

- Each IT process included in COBIT must be assigned an owner
- A range of people needs to be consulted for each IT process
- Generally, **RACI** chart which defines:
  - Who is **R**esponsible
  - Who is **A**ccountable
  - Who is to be **C**onsulted
  - and Who is to be **I**nformed for each IT process
- An example is shown on the next slide



COBIT: An IT governance framework
(IT Process ownership and RACI: An example)

Figure 3—PO9 Functions Perimeter Table

Process	Activity	Outputs	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
PO1	Build an IT strategic plan.	Strategic plan		A	C	C	R	I	C	C	C	C	I	C
	Build IT tactical plans.	Tactical plan		C	I		A	C	C	C	C	C	R	I
	Analyze program portfolios and manage project and service portfolios.	IT service portfolio		C	I	I	A	R	R	C	R	C	C	I
PO10	Build project charters, schedules, quality plans, budgets, and communication and risk management plans.	Project risk management plan				C	C	C	C	C	C	C	A/R	C
DS2	Identify, assess and mitigate supplier risks.	Supplier risks			I		A		R		R	R	C	C
DS4	Regularly test the IT continuity plan.	Contingency test results					I	I	A/R		C	C	I	I
DS5	Conduct regular vulnerability assessments.	Security threats and vulnerabilities			I		A	I	C	C	C			R
ME1	Identify and collect measurable objectives that support the business objectives.	Historical risk trends and events		C	C	C	A	R	R		R			
ME4	Review, endorse, align and communicate IT performance, IT strategy, and resource and risk management with business strategy.	Enterprise appetite for IT risks	A	R	I	R								C

Summary

- Reasons why organisations outsource (full/partial) their IT function
- Differences between various types of IT outsourcing practices
- Risks associated with IT outsourcing
- The control and governance of IS
- IT Governance frameworks

Reading:

Information Systems Audit Control Association. (2012). *COBIT 5 : a business framework for the governance and management of enterprise IT.* Rolling Meadows, IL.: ISACA.

See also ISACA website,
https://www.isaca.org/resources/cobit