2022/23 Semester 1

IS3103 Information Systems Leadership and Communication

Lecture 4
IS Governance and Service Delivery

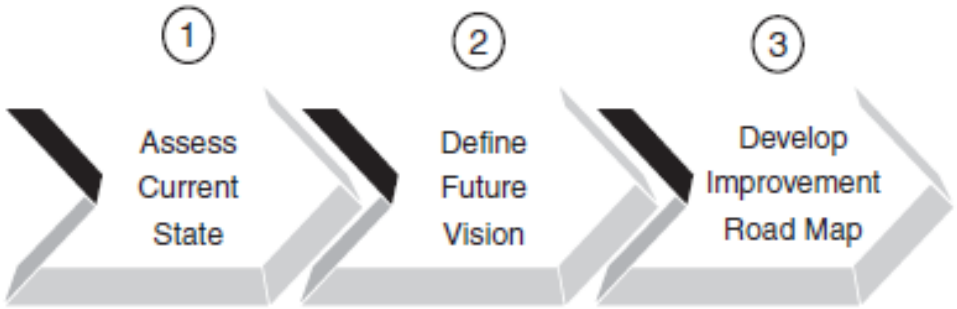
A/Prof OH Lih Bin
ohlb@comp.nus.edu.sg | 6516 3796 | COM2-0421

Department of Information Systems & Analytics
NUS School of Computing

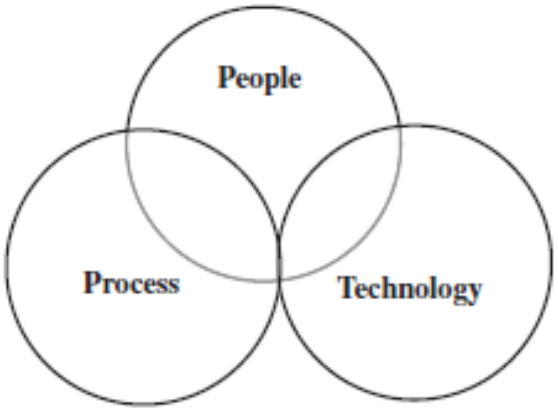
Developing IS Strategic Plans (Digital Transformation Roadmap)

For Project

IT assessment approach is made up of three steps:



Development of your improvement road map is structured around three elements, which incorporate the core competencies of a value-centric IT organization.



Developing IS Strategic Plans

- Step 1: Understand the current state of the IT organization
  - Has the organization been successful in meeting the needs of the business?
  - Are the relations between the IT organization and its business partners collaborative?
  - Does the business feel that investments in the IT organization are providing the desired benefits?
  - *Note: not just on IT infrastructure, need to consider business-IT alignment issues*

Developing IS Strategic Plans

- Step 2: Defining the future vision for the IT organization
  - understand the *future* business strategy and how the IT organization can enable the business to achieve its goals
  - interviews with key internal staff and external business partners, are required to understand their future direction and areas that technology can assist
  - conduct external research on how leading companies in your industry are providing technology solutions to support their business

Developing IS Strategic Plans

- Step 3: Developing a road map to get you from where you are today to your future vision
  - taking into account how much your company is willing to invest in the IT organization, along with realistic estimates for the time required to achieve your future state

Developing IS Strategic Plans

- Three Critical Elements of IS Strategic Plans
  - Technology
    - technology solutions should be flexible, cost effective, and can scale to meet future demands of the business
    - do not focus primarily on this area to the detriment of the others
  - People
    - having the right team aligned with your business partners
    - assess whether you need to hire more senior-level staff, addressing skill-set gaps, or conducting additional training
  - Process
    - frameworks such as the Control Objectives for Information and Related Technology (COBiT) and Information Technology Infrastructure Library (ITIL) exist with best practices for managing an IT organization

IS Governance
(IT Governance/Enterprise Governance of IT)

- Governance is about systematically determining:
  - who has input to a decision (an input right)
  - who makes each type of decision (a decision right)
  - how these people (or groups) are held accountable for their role
- *IS governance* specifies the framework for decision rights and accountability to ensure desirable behavior in the *use of IT*

Figure 2: Five Major IT Decisions Need to be Made	
IT Principles	High-level statements about how IT is used in the business
IT Architecture	An integrated set of technical choices to guide the organization in satisfying business needs. The architecture is a set of policies and rules for the use of IT and plots a migration path to the way business will be done (includes data, technology, and applications)
IT Infrastructure Strategies	Strategies for the base foundation of budgeted-for IT capability (both technical and human), shared throughout the firm as reliable services, and centrally coordinated (e.g., network, help desk, shared data)
Business Application Needs	Specifying the business need for purchased or internally developed IT applications
IT Investment And Prioritization	Decisions about how much and where to invest in IT including project approvals and justification techniques

Six Archetypal Approaches to IT Decision Making

- Ranging from highly centralized to highly decentralized
- Most companies employ a variety of them, using different approaches for different decisions

Figure 3: IT Governance Archetypes

Decision rights or inputs rights for a particular IT decision are held by:		CxO Level Execs	Corp. IT and/or Business Unit IT	Business Unit Leaders or Process Owners
Business Monarchy	A group of, or individual, business executives (i.e., CxOs). Includes committees comprised of senior business executives (may include CIO). Excludes IT executives acting independently.	✓		
IT Monarchy	Individuals or groups of IT executives.		✓	
Feudal	Business unit leaders, key process owners or their delegates.			✓
Federal	C level executives and at least one other business group (e.g., CxO and BU leaders)—IT executives may be an additional participant. Equivalent to a country and its states working together.	✓	✓	✓
		✓		✓
IT Duopoly	IT executives and one other group (e.g., CxO or BU leaders).	✓	✓	
			✓	✓
Anarchy	Each individual user			

Centralized ↓ Decentralized

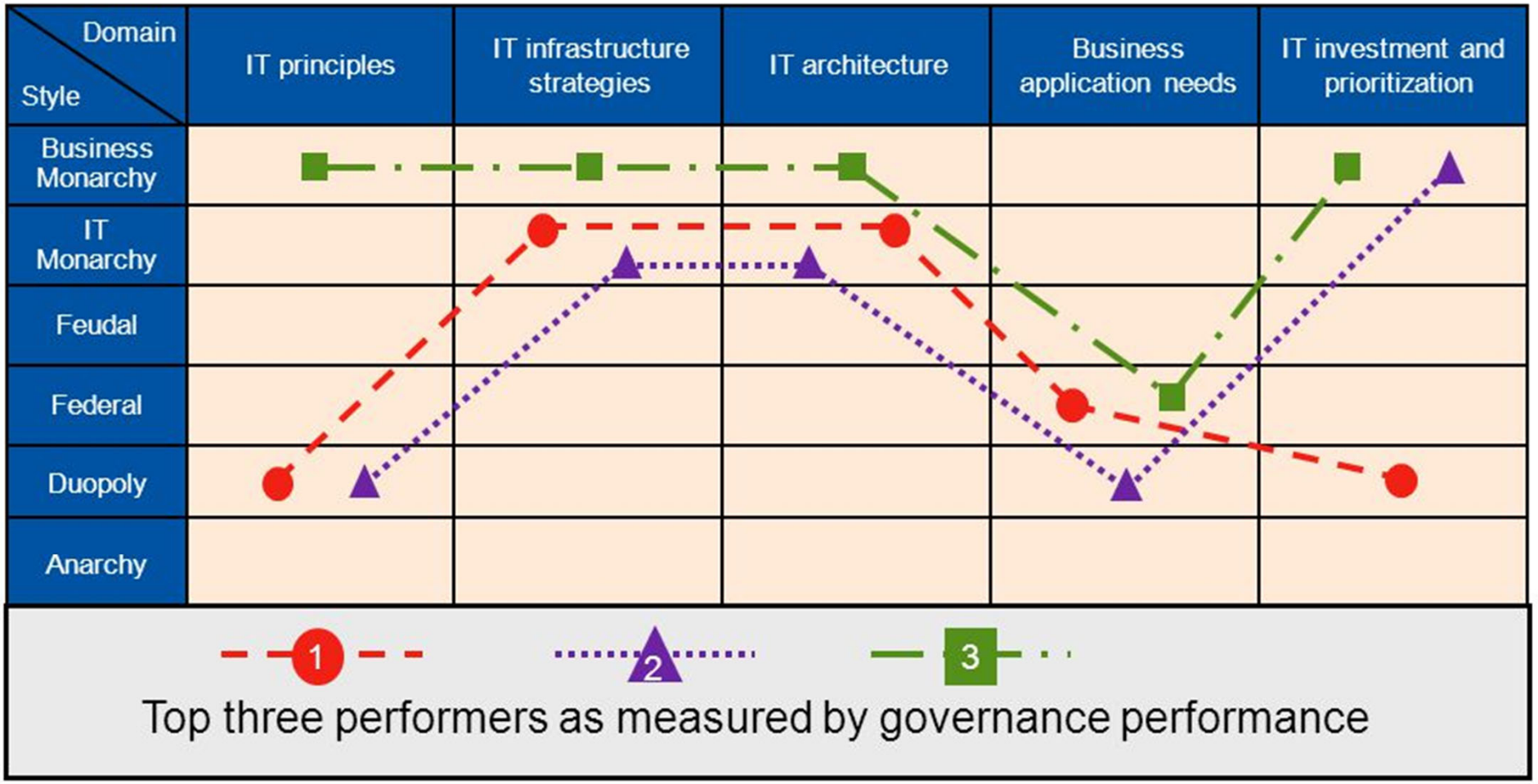
Example of UPS's IT Governance

IT Governance on One Page

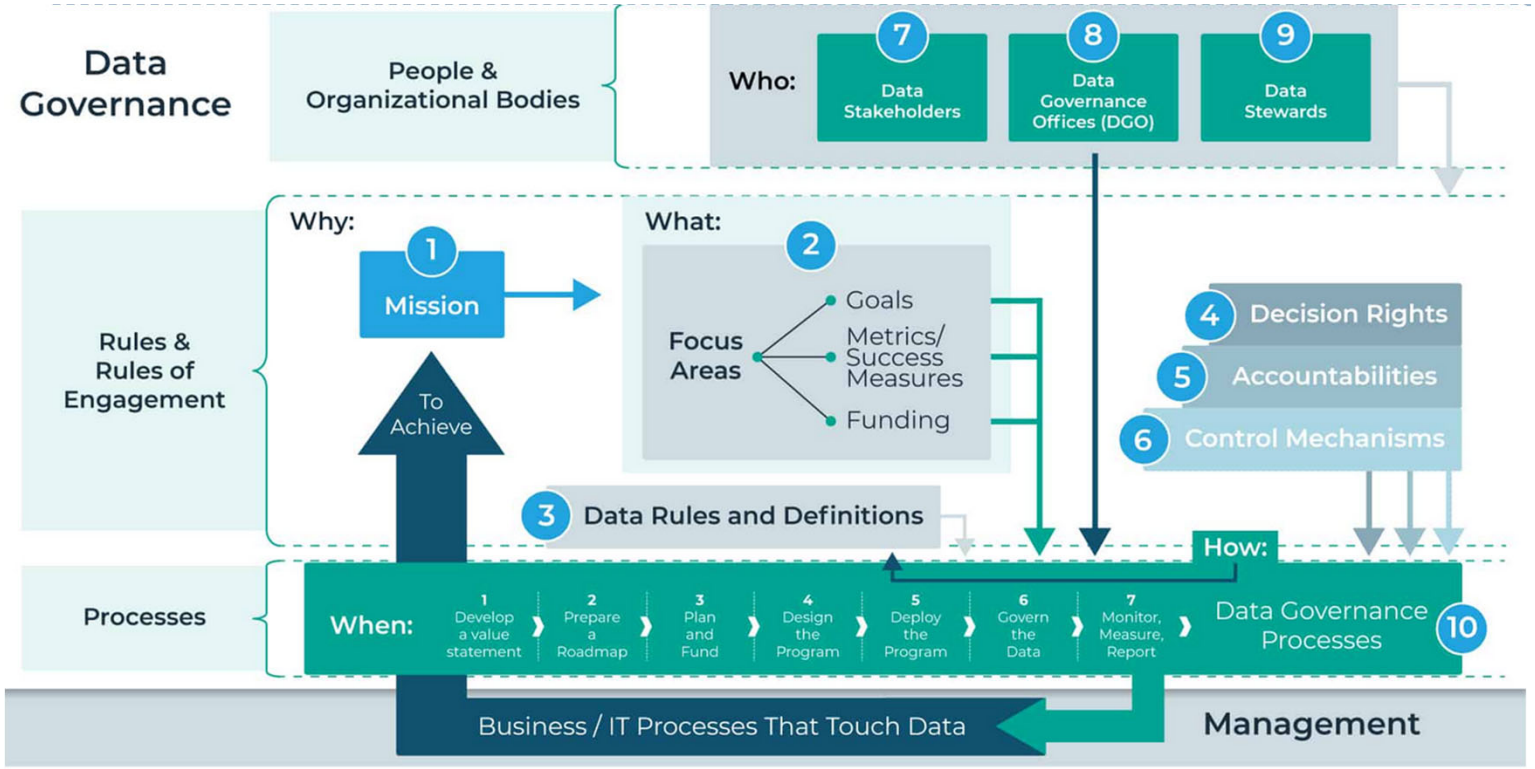
A matrix that juxtaposes the five IT decision domains against five of the six archetypal approaches creates, on a single page, a valuable tool for specifying, analyzing and communicating where IT decisions are made. UPS's governance is clear and relatively centralized: A subset of the senior management team takes responsibility for defining IT principles and IT investment; the CIO's team is held accountable for IT architecture and IT infrastructure; and business unit leaders and enterprisewide process managers are responsible for defining business application needs.

	Decision Domain				
Governance Archetype	IT Principles	IT Architecture	IT Infrastructure Strategies	Business Application Needs	IT Investment
Business Monarchy	X				X
IT Monarchy		X	X		
Federal				X	
IT Duopoly					
Feudal					

Business and IT executive collaboration mark high IT governance performers



Data Governance



Definition:

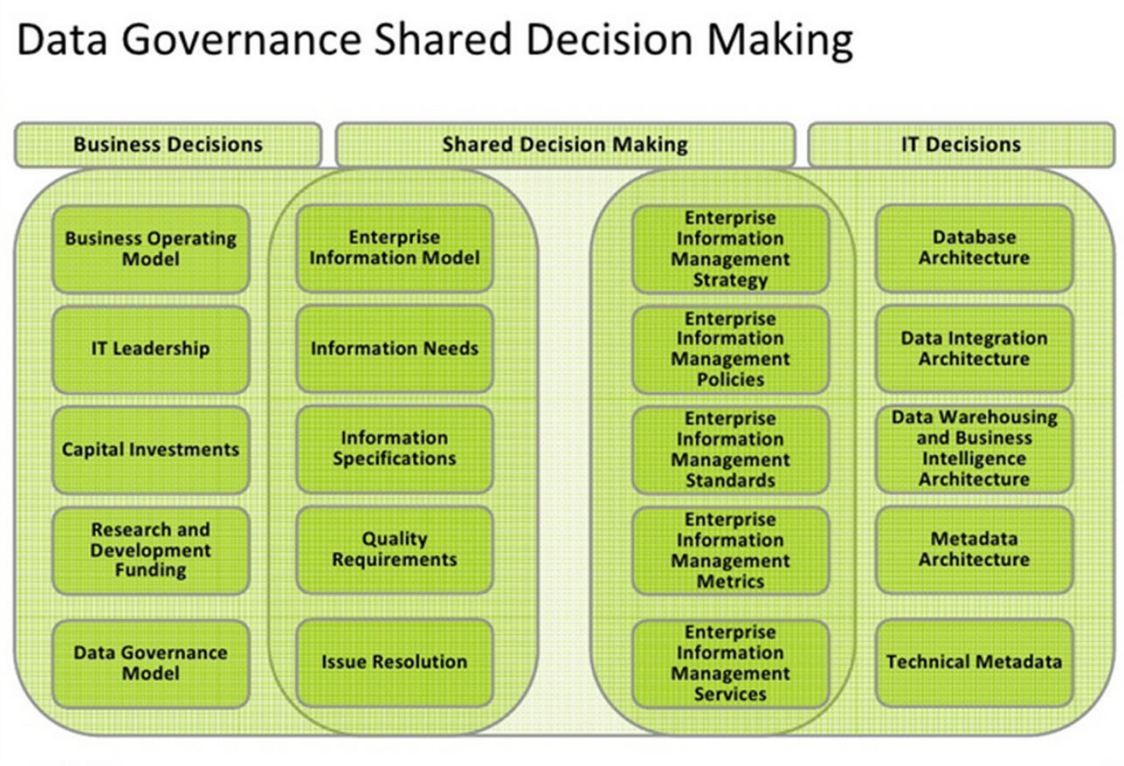
Data Governance is the exercise of decision making and authority for data-related matters.

It's a system of decision rights and accountabilities for information-related processes, executed according to agreed upon models which describe who can take what actions with what information and under what circumstaces, using what methods.

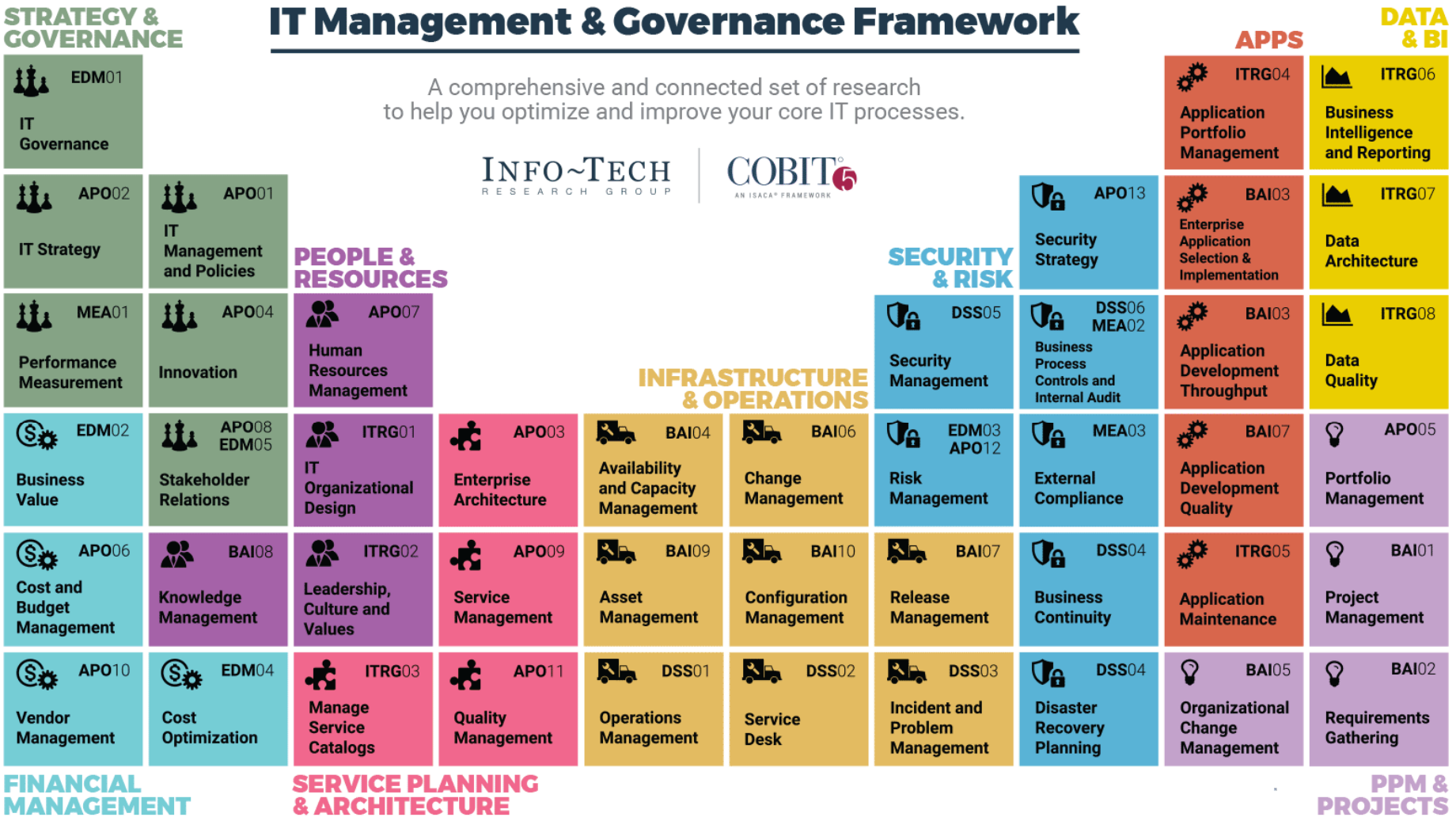
Processes for governing how data is used, and when, and by whom

1. Aligning Policies, Requirements & Controls
2. Establishing Decision Rights
3. Establishing Accountability
4. Performing Stewardship
5. Managing Change
6. Defining Data
7. Issue Resolution
8. Specifying Data Quality Requirements
9. Building Governance into Technology
10. Stakeholder Care and Support
11. Stakeholder Communications
12. Measuring and Reporting Value

Data Governance



COBIT (Control Objectives for Information Technologies)



Certified in the Governance of Enterprise IT®

An ISACA® Certification

CGEIT – Certified in the Governance of Enterprise IT – is the most widely accepted certification for an Information Systems Risk and Control professional.

This five days class room based training will primarily enable you to prepare for the CGEIT Examination and pass at the first appearance.

Achieve the key objectives of:

- Identify, analyze, treat and manage IS risk and how it relates to the overall organization. Design, implement, monitor & maintain the risk-based and effective IS Control of the Enterprise
- Achieve the Compliance with regulatory requirements

Course Objectives

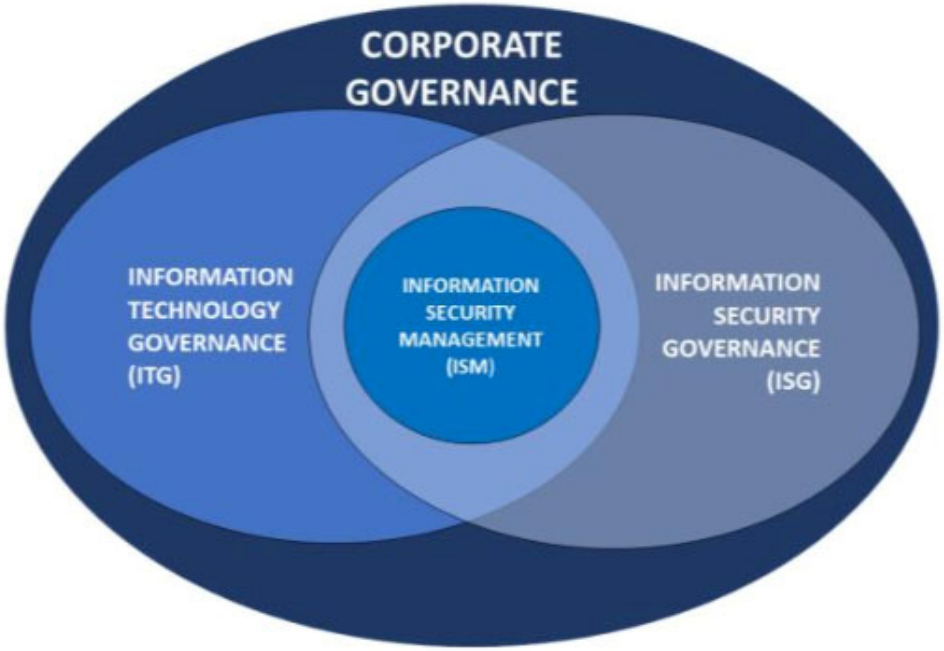
- How is the framework for the governance of enterprise IT defined, established, and managed in alignment with the mission, vision and values of the enterprise
- How the achievement of enterprise objectives ensure that IT enables and supports through the integration and alignment of IT strategic plans with enterprise strategic plans
- Ensure that IT-enabled investments are managed to deliver optimized business benefits and that benefit realization outcome and performance measures are established, evaluated and progress is reported to key stakeholders
- Ensure that an IT risk management framework exists to identify, analyse, mitigate, manage, monitor, and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework
- Ensure the optimization of IT resources including information, services, infrastructure and applications, and people, to support the achievement of enterprise objectives

https://www.isaca.org/credentialing/cgeit

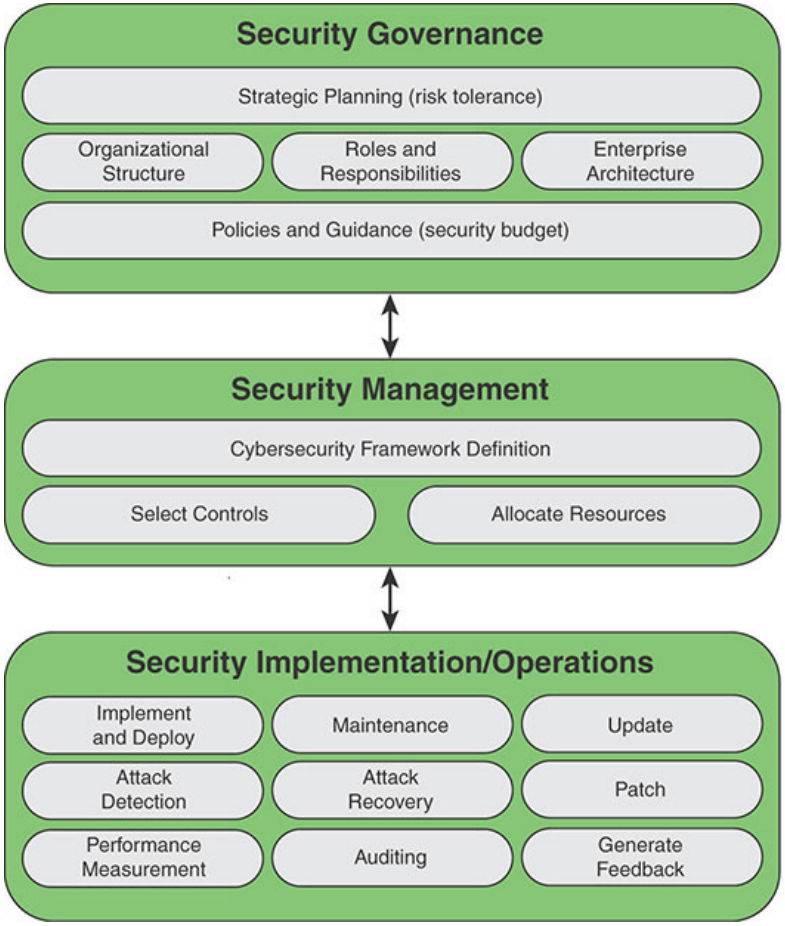
https://www.ntuclearninghub.com/en-gb/-/course/nicf-certified-in-the-governance-of-enterprise-it-cgeit-sf

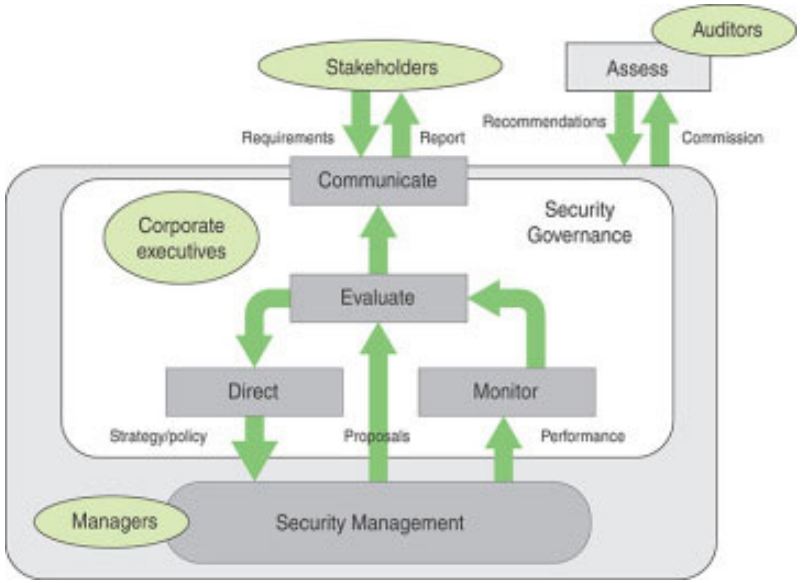
Information Security Governance (ISG)

- ISG contains a structured set of elements that are required to provide senior management with assurance that its major *objectives* are captured in the organization's security posture.
- After the elements have been put in place, management can rest assured that adequate and effective information security will protect the organization's most critical and important assets.



Information Security Governance (ISG)





CISM Certified Information Security Manager®

An ISACA® Certification

Build a Strategic Team

Prove you can manage information security programs and become a strategic asset to enterprise leadership.

CISM Overview | **Is CISM Right for You** | Why Hire a CISM

ISACA's Certified Information Security Manager (CISM) certification is for those with technical expertise and experience in IS/IT security and control and wants to make the move from team player to manager. CISM can add credibility and confidence to your interactions with internal and external stakeholders, peers and regulators.

42%
SALARY IN MANAGERIAL ROLES

70%
ON-THE-JOB PERFORMANCE IMPROVEMENT

ANSI
ANSI Accredited Program Personnel Certification
CISM ACCREDITED UNDER ISO/IEC 17024:2012

THE CISM DIFFERENCE

Whether you are seeking a new career opportunity or striving to grow within your current organization, a CISM certification proves your expertise in these work-related domains:

- INFORMATION SECURITY GOVERNANCE
- INFORMATION RISK MANAGEMENT
- INFORMATION SECURITY PROGRAM DEVELOPMENT & MANAGEMENT
- INFORMATION SECURITY INCIDENT MANAGEMENT

IT Portfolio Management (ITPM)

- Most CIOs face demand for projects that far outstrips their ability to deliver
  - exponentially increasing information requirements
  - reduced budgets and staff
- Responsibility of Project Management Office (PMO)

- "How do we maximize the business value from IT investments?"

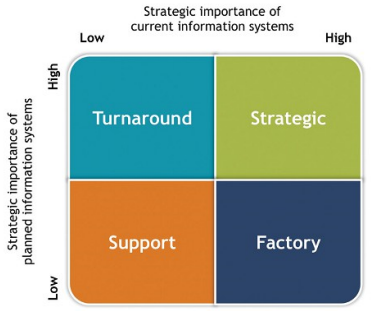
IT Portfolio Management

- ITPM is an approach to aligning, prioritizing, selecting, managing, and monitoring IT investments to:
  - improve returns
  - ensure optimum alignment with and contribution to the organization's goals
  - a core activity of IS governance
- Managing (existing and planned) IT as a portfolio of assets similar to a financial portfolio and striving to improve the portfolio performance by balancing (and regularly rebalancing) risk and return
- Portfolio management of *IT projects* - include software application projects, hardware assets, infrastructure, outsourcing contracts and software licenses, etc

Four broad classification of IT investments

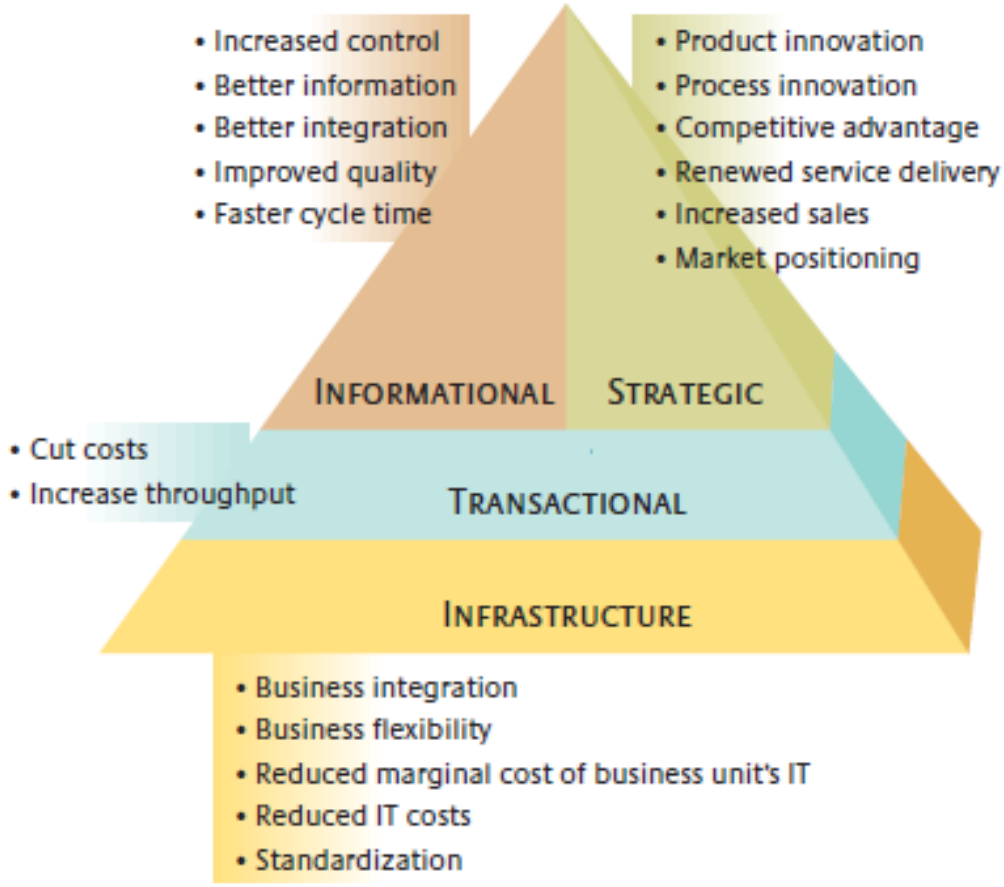
- Each type of investment represents a different IT asset class with its own unique risk-return profile

1. *Infrastructure investments* are the shared IT services used by multiple applications (such as, servers, networks, laptops, customer databases)
2. *Transactional investments* are used primarily to cut costs or increase throughput for the same cost (for e.g., a brokerage firm's trade processing system)
3. *Informational investments* provide information for purposes such as accounting, reporting, compliance, communication or analysis
4. *Strategic investments* are used to gain competitive advantage by supporting entry into new markets or by helping to develop new products, services or business processes
   - ATMs were a successful strategic IT initiative for the first banks that introduced them but they became transactional over time



Considering IT Investments as a Portfolio

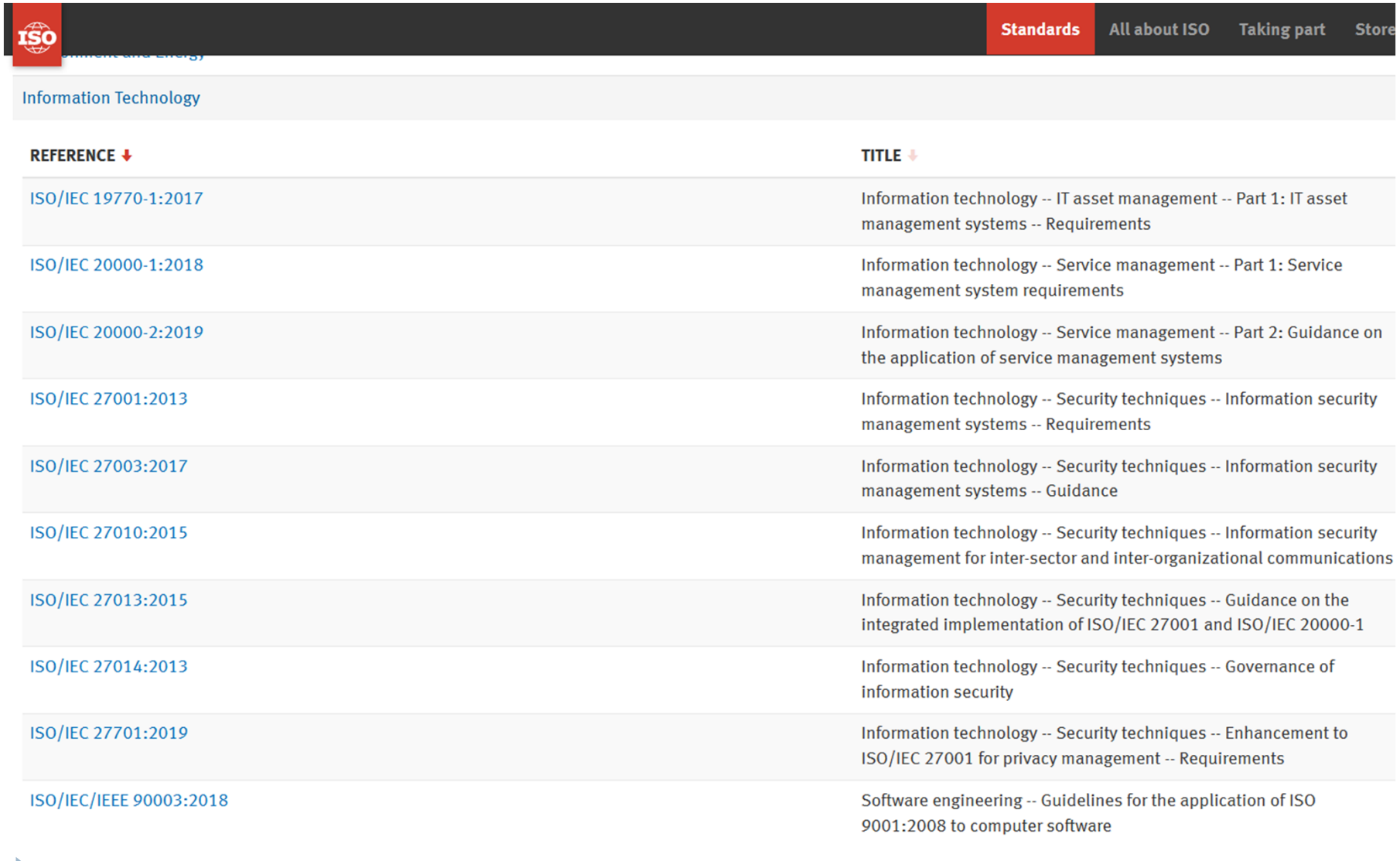
IT portfolio management is an increasingly common way to help management teams match IT investments to strategic objectives. Our research identified four broad classifications of IT investments: transactional, informational, strategic and infrastructure.



Extracting More Business Value from IT Portfolio

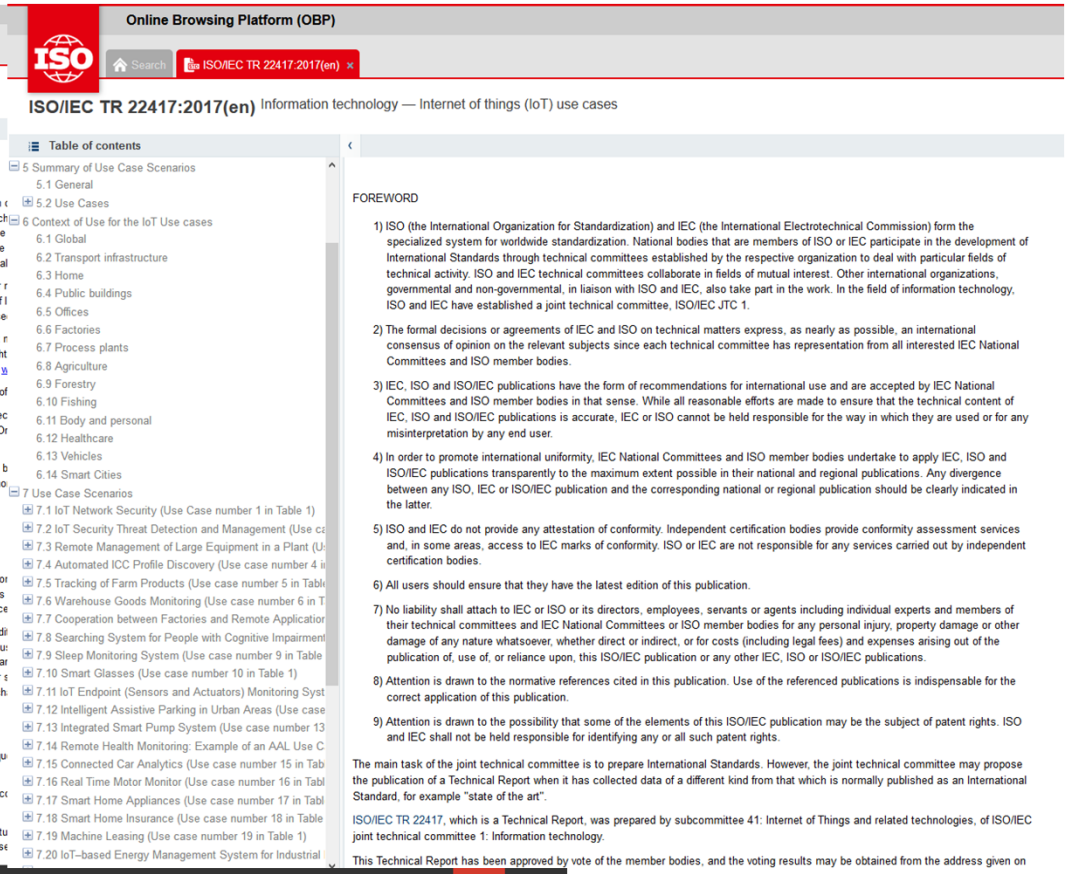
1. Identify the current and previous year's IT portfolios (using the portfolio categorization)
2. Understand IT asset class performance and benchmarks for your business
3. Balance the portfolio for alignment and risk-return profile — and ensure that the process is transparent
4. Re-weight portfolios annually and whenever major changes occur
5. Incorporate the IT portfolio approach into the IT governance framework
6. Learn from post-implementation reviews and formal training

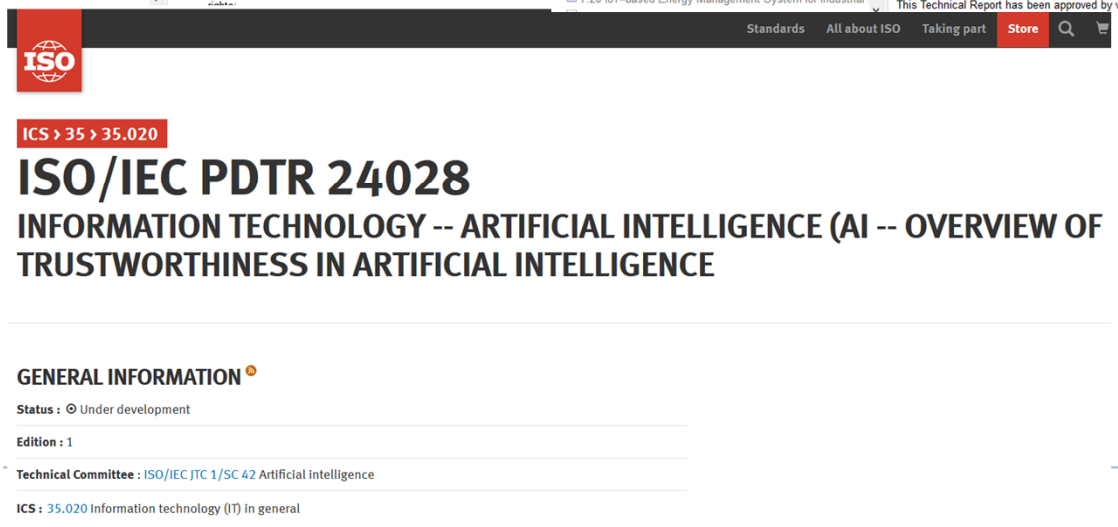
IT Standards (e.g., ISO - www.iso.org)



REFERENCE	TITLE
ISO/IEC 19770-1:2017	Information technology -- IT asset management -- Part 1: IT asset management systems -- Requirements
ISO/IEC 20000-1:2018	Information technology -- Service management -- Part 1: Service management system requirements
ISO/IEC 20000-2:2019	Information technology -- Service management -- Part 2: Guidance on the application of service management systems
ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27003:2017	Information technology -- Security techniques -- Information security management systems -- Guidance
ISO/IEC 27010:2015	Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
ISO/IEC 27013:2015	Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014:2013	Information technology -- Security techniques -- Governance of information security
ISO/IEC 27701:2019	Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements
ISO/IEC/IEEE 90003:2018	Software engineering -- Guidelines for the application of ISO 9001:2008 to computer software


Online Browsing Platform (OBP)
Search
ISO/IWA 27:2017(en)
ISO/IWA 27:2017(en) Guiding principles and framework for the sharing economy
Table of contents
Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Guiding principles — Platform operators and providers
4.1 General
4.2 Integrity
4.3 Transparency
4.4 Accountability
4.5 Accessibility and inclusion
4.6 Responsiveness
4.7 Health, safety and environment
4.8 Confidentiality, privacy and security
4.9 Capacity
4.10 Competence
4.11 Continual improvement
5 Sharing economy decision-making and action framework
5.1 General
5.2 Customers
5.3 Labour
5.4 Government
5.5 Environment
5.6 Broader economic, societal and community impacts and opportunities
6 Feedback, review and continual improvement
Annex A Operationalizing the principles
A.1 General
A.2 Aligning performance with purpose
A.3 Operating day-to-day
A.4 Keeping the system in good working order
A.5 Enhancing the system to improve its value
Annex B Guidance on handling comments and complaints
Annex C Guidance for platform operators
Annex D Guidance for providers
Annex E Guidance from the customer's perspective
Annex F Guidance for interested parties
Annex G International guidelines
G.1 General
G.2 ISO 10001, Quality management — Customer satisfaction — Guidelines for c
G.3 ISO 10002, Quality management — Customer satisfaction — Guidelines for c
G.4 ISO 10003, Quality management — Customer satisfaction — Guidelines for di
G.5 ISO 10008, Quality management — Customer satisfaction — Guidelines for b
Foreword
ISO (the International Organization for Standardization) is a worldwide federation
work of preparing International Standards is normally carried out through ISO tech
subject for which a technical committee has been established has the right to be
organizations, governmental and non-governmental, in liaison with ISO, also take
International Electrotechnical Commission (IEC) on all matters of electrotechnical
The procedures used to develop this document and those intended for its further r
Part 1. In particular the different approval criteria needed for the different types of
drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (se
Attention is drawn to the possibility that some of the elements of this document r
responsible for identifying any or all such patent rights. Details of any patent right
be in the Introduction and/or on the ISO list of patent declarations received (see w
Any trade name used in this document is information given for the convenience of
For an explanation on the voluntary nature of standards, the meaning of ISO spec
assessment, as well as information about ISO's adherence to the World Trade Or
Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.
International Workshop Agreement IWA 27 was approved at a workshop hosted b
with the CSA Group and the federal government's Innovation, Science and Econo
(OCA), held in Toronto, Canada, in March 2017.
Introduction
A combination of technological and other factors have enabled the sharing econor
with changing consumer behaviour are driving its growth. This document provides
the intention of making participation in the sharing economy a positive experience
The activities associated with the sharing economy in some ways challenge tradi
transactions for a fee or free, matching often-underused assets and skills with cu
managing impacts of planned and unforeseen events. Customers and providers ar
initially absent. Sharing economy participants often use reviews, customized for s
mutual ratings of providers and customers in addition to other trust-building mech
conformance.
The sharing economy presents both opportunities and challenges:
— customers can find improved prices, options and social interaction, but qu
validity of online reviews;
— providers can welcome flexible work arrangements and access to new inco
benefits, insurance, security and other economic and safety protections;
— platform providers can seek broader market access and economic opportu
legal requirements while assuring technological reliability, data integrity, se


Online Browsing Platform (OBP)
Search
ISO/IEC TR 22417:2017(en)
ISO/IEC TR 22417:2017(en) Information technology — Internet of things (IoT) use cases
Table of contents
5 Summary of Use Case Scenarios
5.1 General
5.2 Use Cases
6 Context of Use for the IoT Use cases
6.1 Global
6.2 Transport infrastructure
6.3 Home
6.4 Public buildings
6.5 Offices
6.6 Factories
6.7 Process plants
6.8 Agriculture
6.9 Forestry
6.10 Fishing
6.11 Body and personal
6.12 Healthcare
6.13 Vehicles
6.14 Smart Cities
7 Use Case Scenarios
7.1 IoT Network Security (Use Case number 1 in Table 1)
7.2 IoT Security Threat Detection and Management (Use ca
7.3 Remote Management of Large Equipment in a Plant (U
7.4 Automated ICC Profile Discovery (Use case number 4 i
7.5 Tracking of Farm Products (Use case number 5 in Tabl
7.6 Warehouse Goods Monitoring (Use case number 6 in T
7.7 Cooperation between Factories and Remote Applicatior
7.8 Searching System for People with Cognitive Impairment
7.9 Sleep Monitoring System (Use case number 9 in Table
7.10 Smart Glasses (Use case number 10 in Table 1)
7.11 IoT Endpoint (Sensors and Actuators) Monitoring Syst
7.12 Intelligent Assistive Parking in Urban Areas (Use case
7.13 Integrated Smart Pump System (Use case number 13
7.14 Remote Health Monitoring: Example of an AAL Use C
7.15 Connected Car Analytics (Use case number 15 in Tab
7.16 Real Time Motor Monitor (Use case number 16 in Tabl
7.17 Smart Home Appliances (Use case number 17 in Tabl
7.18 Smart Home Insurance (Use case number 18 in Table
7.19 Machine Leasing (Use case number 19 in Table 1)
7.20 IoT–based Energy Management System for Industrial
FOREWORD
1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.
2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.
3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.
8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.
The main task of the joint technical committee is to prepare International Standards. However, the joint technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".
ISO/IEC TR 22417, which is a Technical Report, was prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.
This Technical Report has been approved by vote of the member bodies, and the voting results may be obtained from the address given on


Standards
All about ISO
Taking part
Store
ICS > 35 > 35.020
ISO/IEC PDTR 24028
INFORMATION TECHNOLOGY -- ARTIFICIAL INTELLIGENCE (AI -- OVERVIEW OF TRUSTWORTHINESS IN ARTIFICIAL INTELLIGENCE
GENERAL INFORMATION
Status : Under development
Edition : 1
Technical Committee : ISO/IEC JTC 1/SC 42 Artificial intelligence
ICS : 35.020 Information technology (IT) in general

(IT) Service Management as a Practice

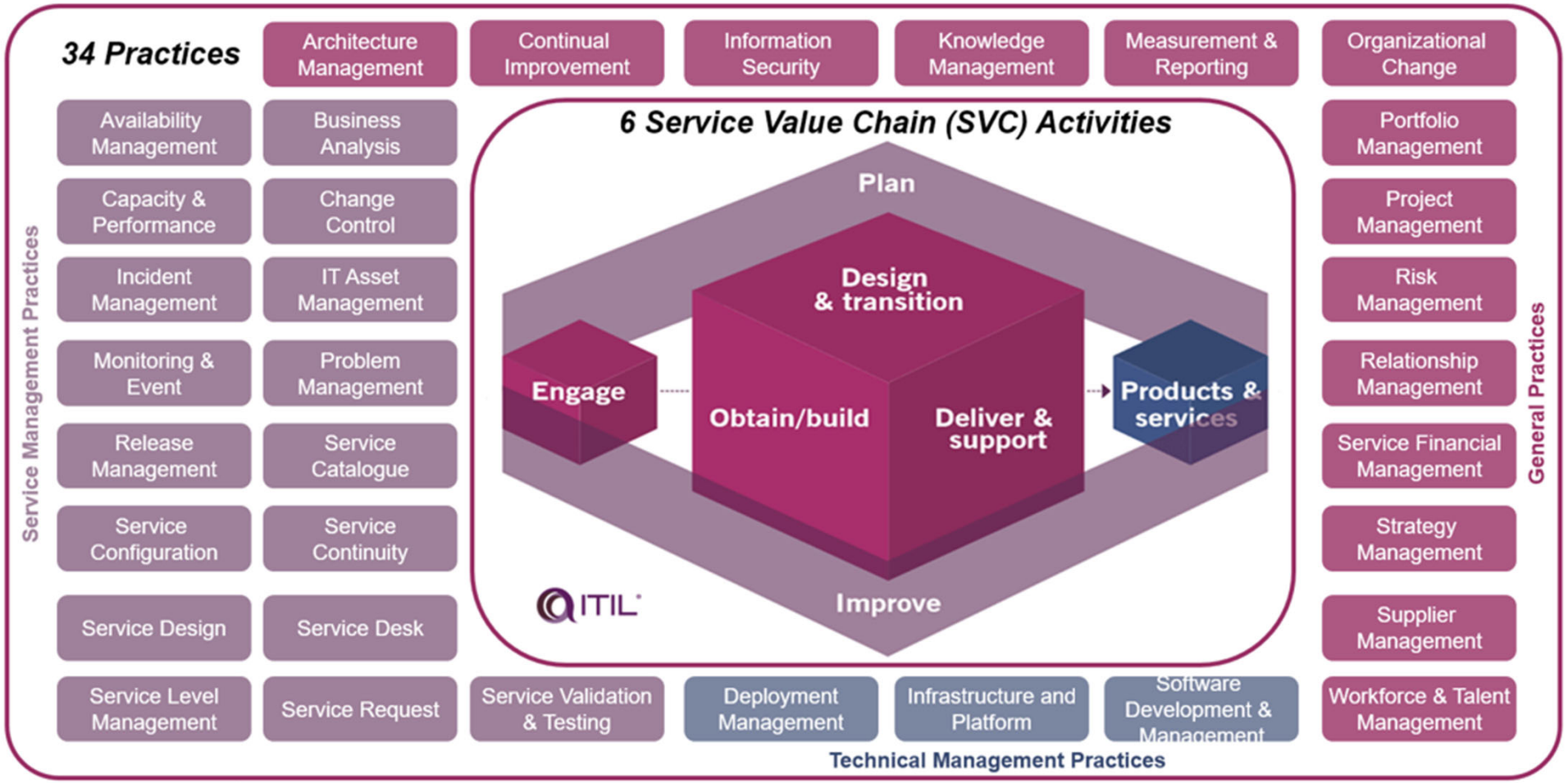
ITIL = IT Infrastructure Library

- Set of books giving guidance on the provision of quality IT services
- Best practices in delivery of IT services
- Not standards!
  - **ISO/IEC 20000** is the international standard for service management
    - https://www.iso.org/standard/70636.html
- Platform independent
- 4th version (2019)

§ *Service* is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks

§ *Service management* is a set of specialized organizational capabilities for providing value to customer in the form of service

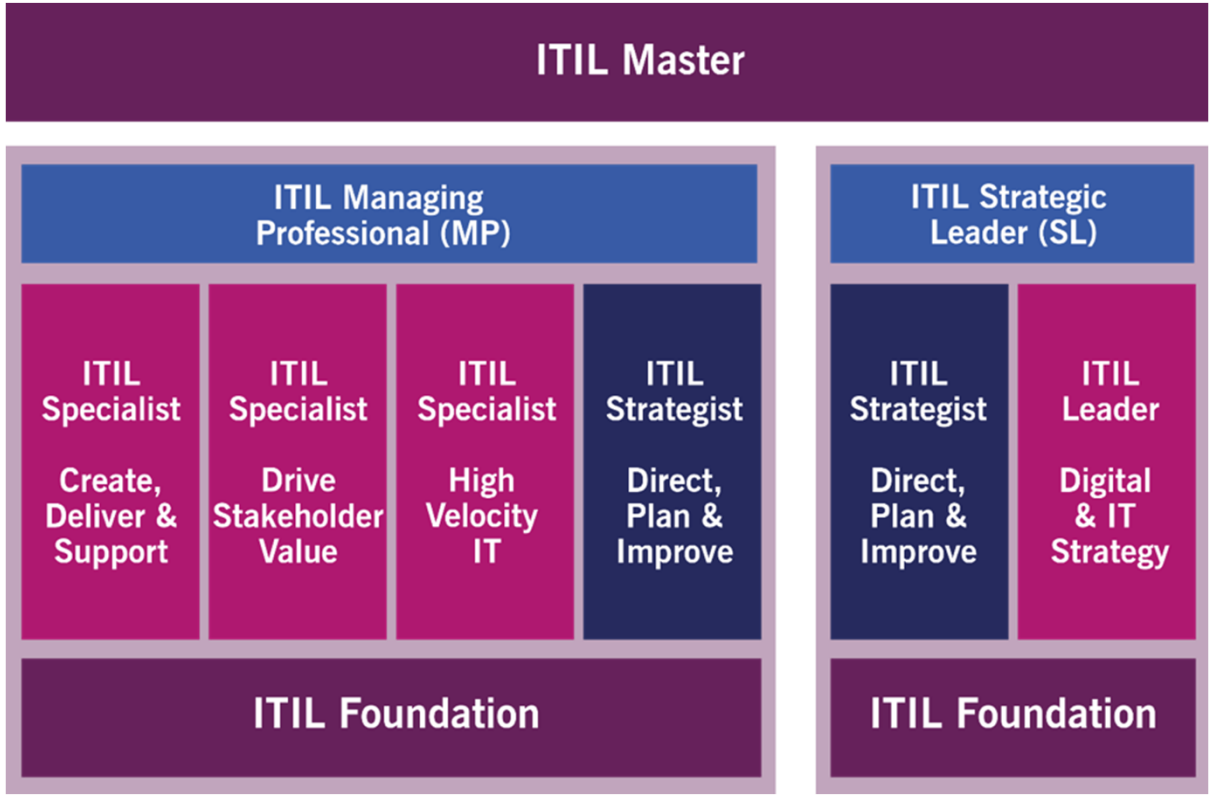
ITIL Version 4



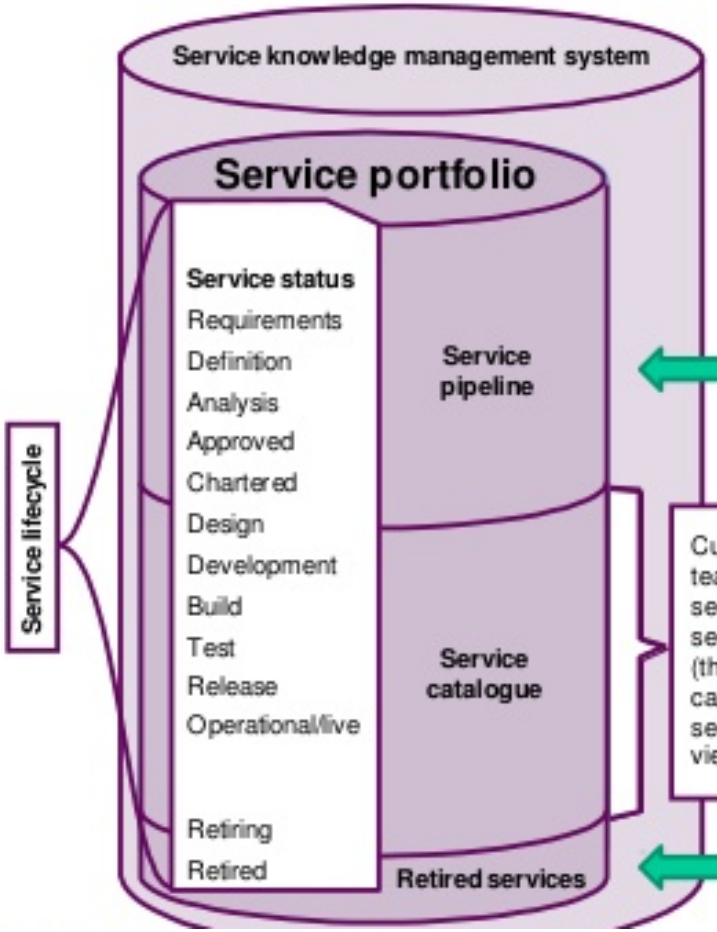
https://www.axelos.com/certifications/itil-certifications

IT Service Management Career Path

- ITIL Certifications



ITIL ® Service Portfolio



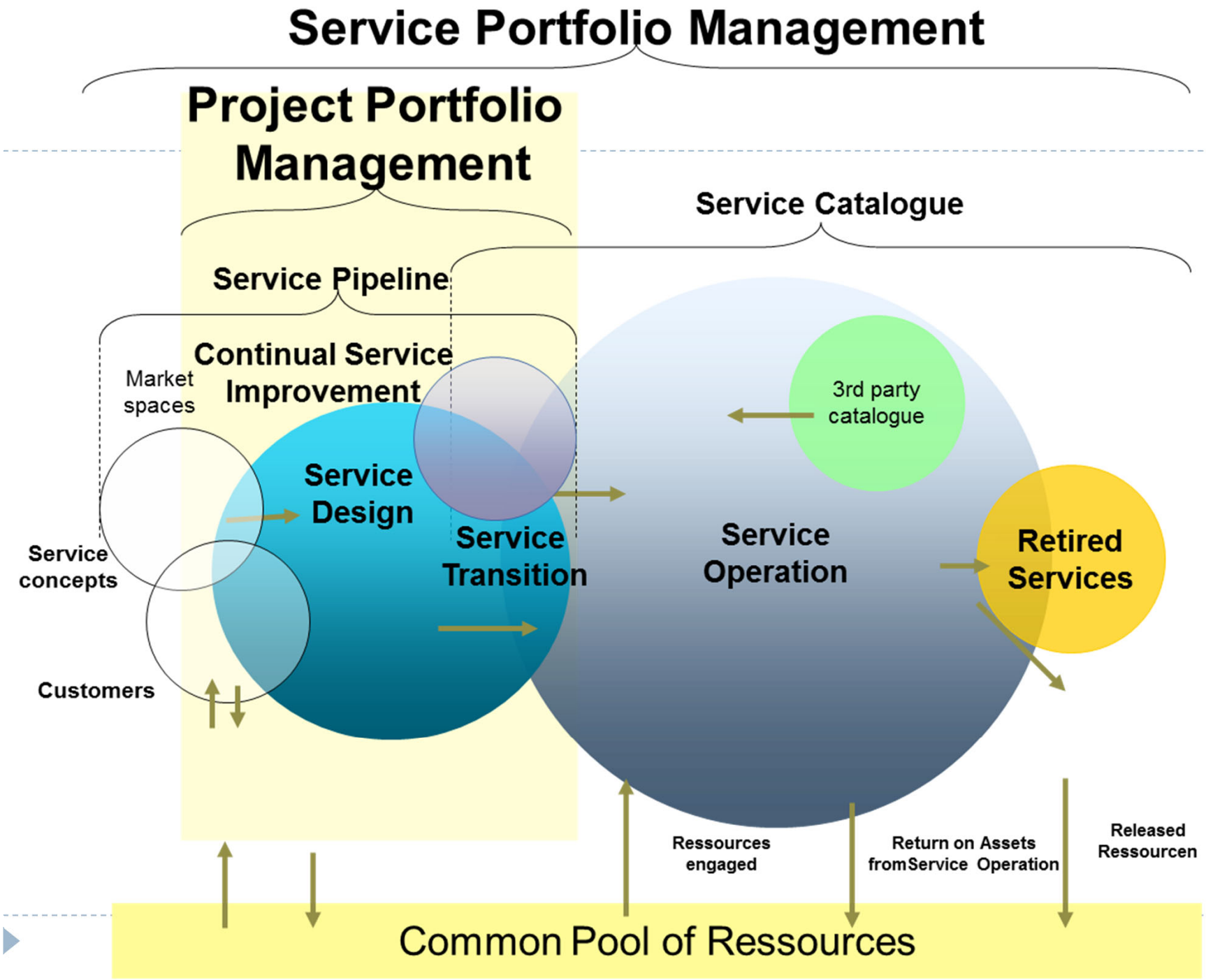
Service Strategy helps to plan and govern the implementation of **Service Portfolio** e.g.:

New IT services or enhancements **to add** to the Service Pipeline

Customer/support team viewable section of the service portfolio (the service catalogue, with selected fields viewable)

Existing IT services

IT services **to be retired**


Service Portfolio Management
Project Portfolio Management
Service Catalogue
Service Pipeline
Continual Service Improvement
Market spaces
Service concepts
Customers
Service Design
Service Transition
Service Operation
3rd party catalogue
Retired Services
Ressources engaged
Return on Assets fromService Operation
Released Ressourcen
Common Pool of Ressources

Traditional Model of IT Service Delivery

- Ownership model
- A company owns and operates its IT infrastructure
- Data are stored on storage devices (hard drives of PCs, or servers, or mainframe computers) owned by the company
- Application software are executed on the local PC or the server
- The IT department is responsible for smooth functioning of IT operations and delivery of IT services
- System upgrades are planned and executed by the IT department

Alternate Models of IT Service delivery

- Open Source Software (Free software)
- Cloud Computing (Rental Model)
- Outsourcing (Let the expert do it)

Open Source Software

- Open source software is software whose source code
  - is available for free download
  - can be modified to suit the user's need
- Examples:
  - Linux, Apache, MySQL, OpenOffice
- Use of OSS is a variation of the ownership model – you own the hardware and software, except the software is free

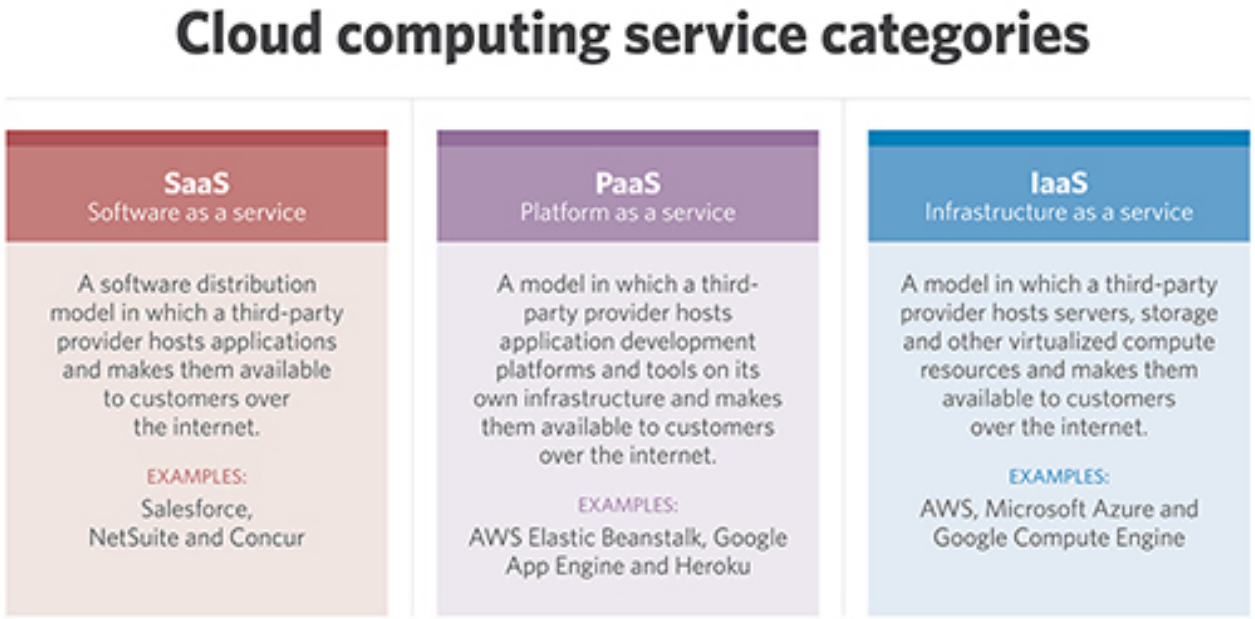
Open Source Software

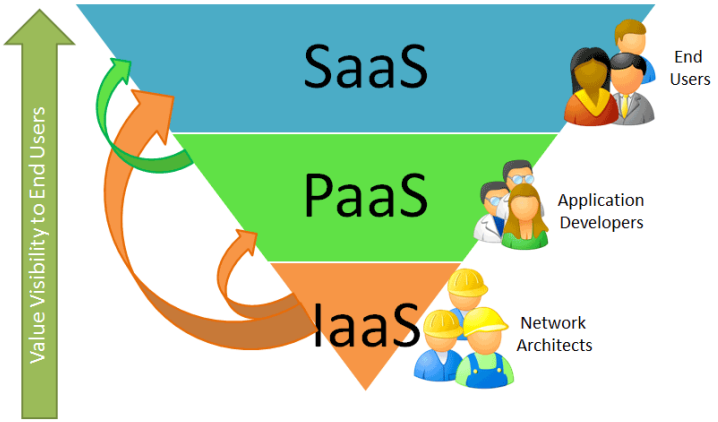
- Benefits
  - OSS can lower initial investment cost as there is no purchase cost for software
  - Total cost of ownership (TCO) can be lowered by relying on the developer community instead of paying an annual maintenance fee
- Cost
  - You are on your own to install and maintain the software
  - Lack of indemnification, in case of software failure – a key concern of some for-profit businesses
  - Third party maintenance cost add to TCO

Cloud Computing

- Provision of IT services using virtualized resources
  - "Green Computing"
- Appearance of "infinite" computing resources available on demand
- No upfront commitment of resource requirement
- Pay for use pricing structure

Cloud Service Models



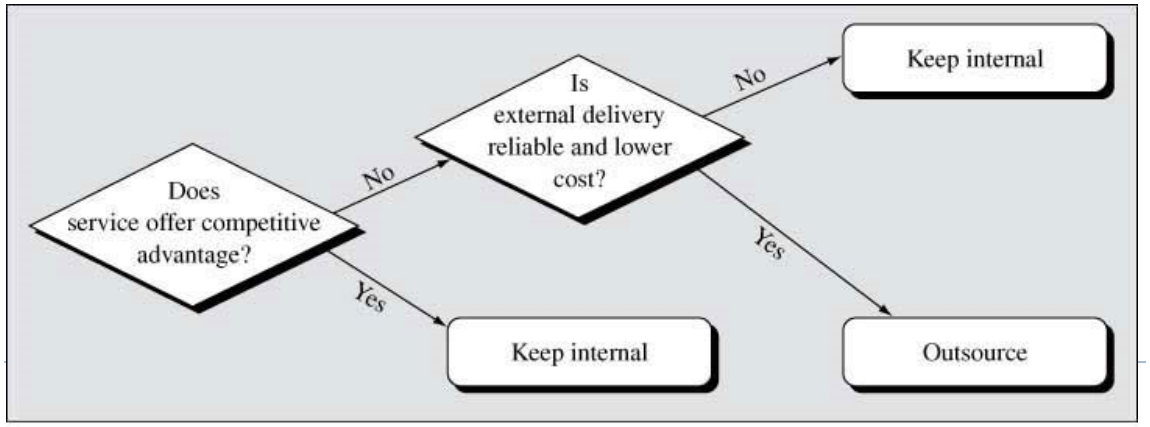


Benefits of the Rental Model (pay for use)

- Favorable cash flow, no upfront cost
- Reduced time to market – no need to set up IT infrastructure
- Lower risk
  - No need for capital investment in IT
  - Flexible demand lowers the risk of underestimating or overestimating IT service need
- No need to maintain and update the IT infrastructure
- No need to hire and retain skilled IT workers – most beneficial to SMEs
- 24x7 global access to IT services is readily available

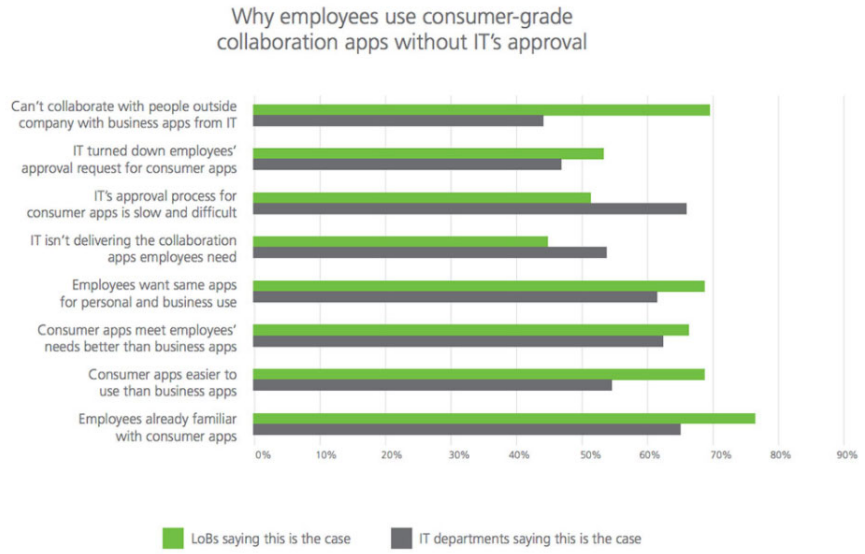
Internal Vs. External Service Delivery

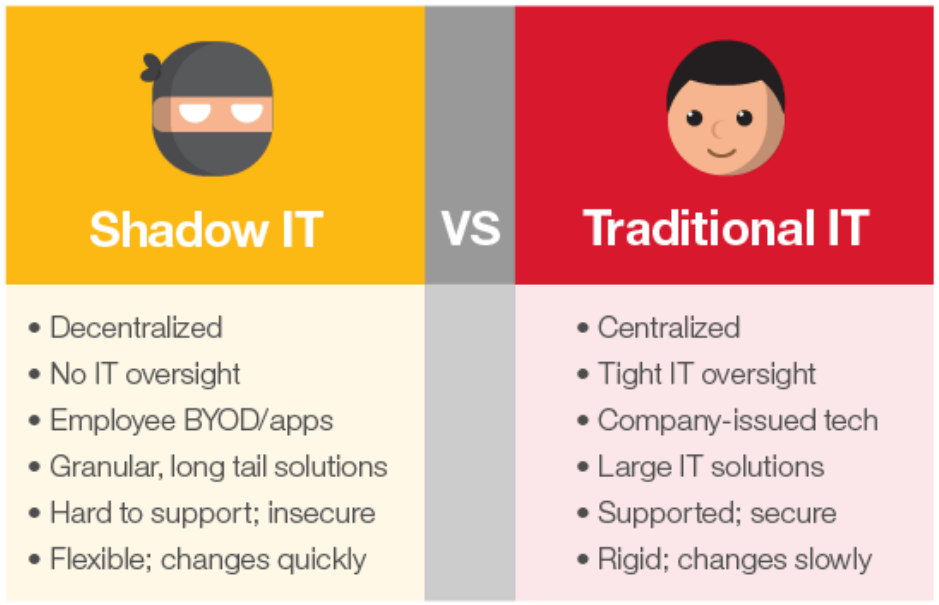
- Applications that provide competitive advantage to an organization – keep these in-house
- Commodity like services, such as email, word processing, etc. – may be rented/outsourced
  - Make sure that the service provider guarantees the desired level of service quality and reliability but charges a lower cost compared to in-house delivery
- The rental model is less risky compared to large scale outsourcing
- Partner relationship management is a critical success factor for the rental model

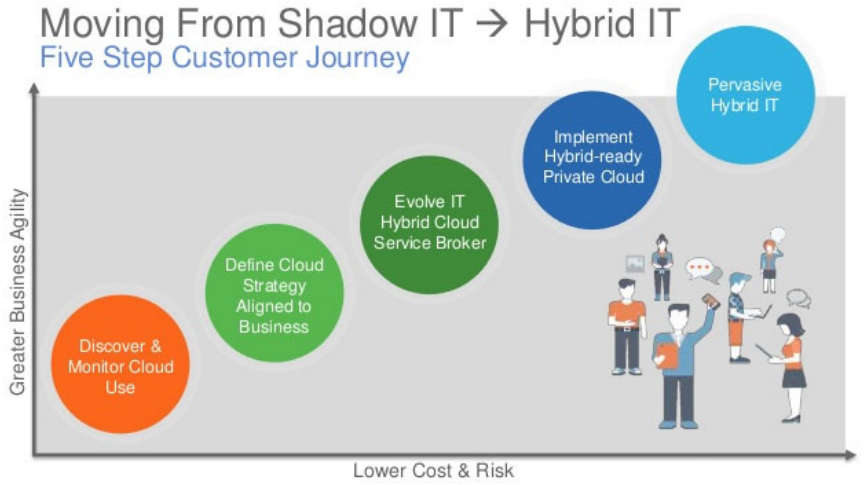


Managing *Shadow IT*

- Use of IT devices, software and services outside the ownership or control of IT organizations







Key Takeaways and Reflection Points from Lecture 4

- How to develop IS strategic plans?
- What is IS governance and why is it important to organizations' ROI and use of IT?
- How to apply IS governance/data governance/security governance frameworks to improve IT decision making?
- How to apply the principles of ITPM to manage IS investments and projects?
- What is ITIL? How do you incorporate ITIL guidelines in IS strategic plans?
- What are the different models of IT service delivery? How do you decide which is the most suitable model to adopt?