Information Systems Strategy and IT Governance ITC4212

Dr Nalaka Lankasena
Faculty of Technology
University of Sri Jayewardenepura

ITG Frameworks

Table of content

- ITG frameworks
  - COBIT
  - ITIL
  - ISO 17799

Information Technology Governance Framework

- **ITG framework** defines the ways and methods through which a**n organization can implement, manage, and monitor ITG within an organization**. It provides guidelines and measures to effectively utilize IT resources and processes within an organization.
- ITG frameworks have been introduced by various researchers and practitioners **to implement and improve the management of IT with the business needs of organizations**.
- ITG frameworks are increasingly being utilized in organizations around the world as their **impact on the performance of the organisation is significant**.
- ITG frameworks **not only assure conformance with regulations but also leverage the performance of organizations**.
- ITG helps **monitor and improve critical IT activities to increase business value and reduce business risk**.

ITG frameworks

- **COBIT** - Control Objectives for Information and Related Technologies
- **ITIL** - Information Technology Infrastructure Library
- **ISO 17999** - Information Technology – Code of Practice for Information Security Management (Introduced by The International Organization for Standardization)
- **ValIT** - Enterprise Value: Governance of IT Investments

Control Objectives for Information and Related Technologies (COBIT)

- COBIT is an IT governance framework introduced by the Information Systems Audit and Control Foundation as a tool for monitoring and managing IT activities
- COBIT is now maintained by the IT Governance Institute (ITGI)
- COBIT serves as an IT governance framework with **associating tools such as maturity models, critical success factors, key goal indicators and key performance indicators**.

..contd.. COBIT ..

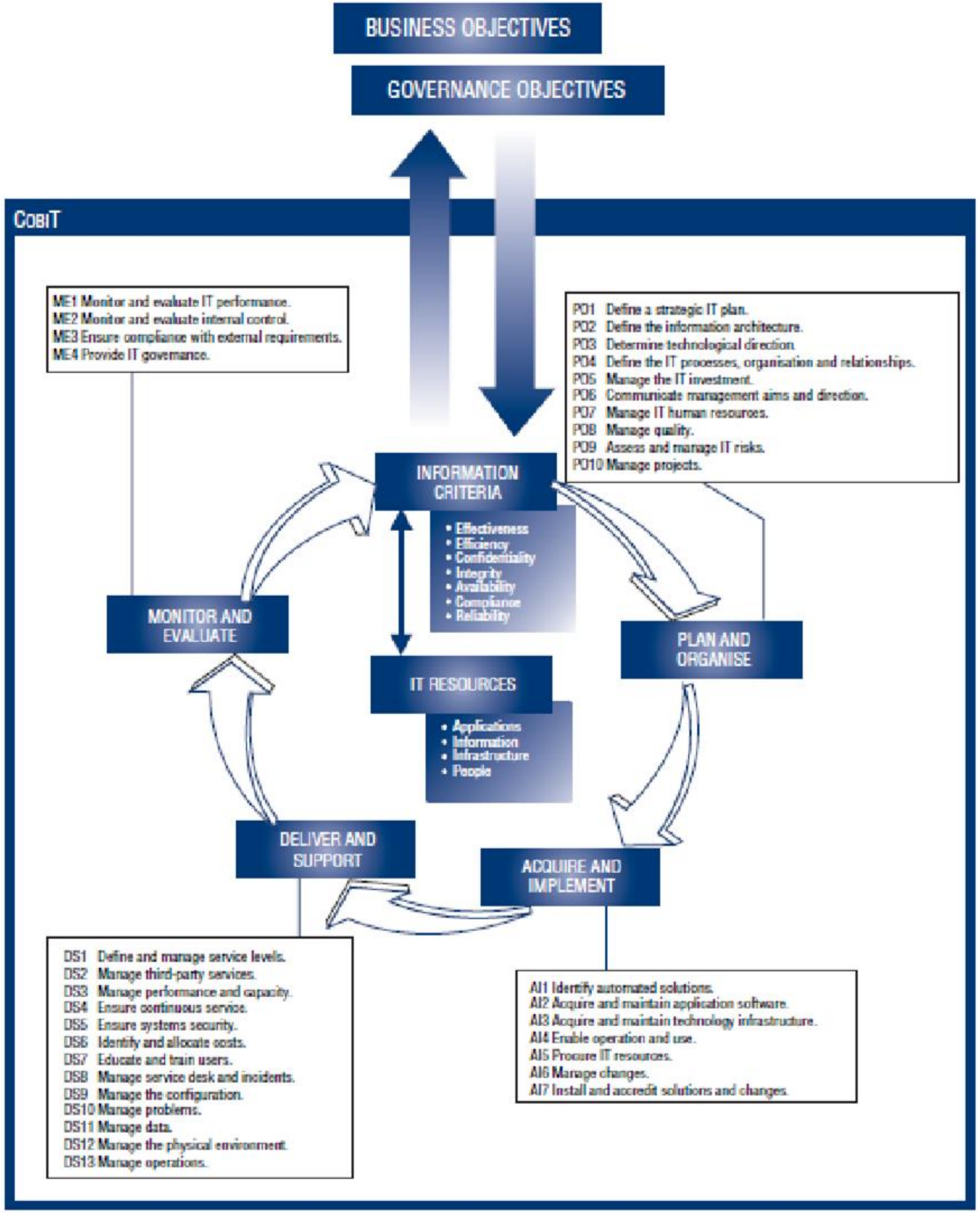
- The top management of every organisation needs to have confidence that they can **rely on IT and the investment made in IT provide positive returns**.
- COBIT has been introduced in order to provide a better understanding of **how to direct and manage an organization’s IT and the standard of good practices for benchmarking**.
- COBIT tells you what you should be doing.
- COBIT is a supporting toolset that allows: managers to bridge the gap between **control requirements, technical issues, and business risks**.

.. Contd. COBIT..

- COBIT framework has been introduced with a hierarchical structure i.e. processes and domains.
- COBIT consists of **318 detailed control objectives** and these have been organized into **four domains and 34 high-level control objectives** C**OBIT Framework subdivides IT into four domains**
  - **Planning and Organizing (PO)**
  - **Acquisition and Implementation (AI)**
  - **Delivery and Support (DS)**
  - **Monitoring and Evaluation (ME)**
- **34 high-level control objectives** are grouped into 4 main domains

Overall COBIT framework

34 high level control objectives are grouped into 4 main domains



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

COBIT frameworks domains and objectives

Planning & organizing (10)

- Define an IT strategic plan
- Define the information architecture
- Define technology direction
- Define the IT organization
- Manage the IT investment
- Communicate aims and direction
- Manage human resources
- Assesses risks
- Manage projects
- Manage quality

Acquisition & implementation (7)

- Identify solutions
- Acquire & maintain applications
- Acquire & maintenance infrastructure
- Develop & maintain procedures
- Install and accredit systems
- Manage changes
- Procure IT resources

Delivery & support (13)

- Define & manage service levels
- Manage third-party services
- Manage performance & capacity
- Ensure continuous service
- Ensure systems security
- Identify & allocate costs
- Educate & train users
- Assist & advise customers
- Manage the configuration
- Manage problems and incidents
- Manage data
- Manage facilties
- Manage operations

Monitoring (4)

- Monitor the processes
- Assess internal control adequacy
- Obtain independent assurance
- Provide for independent audit

Planning and organisation (PO)

- This domain covers **strategy and tactics used by IT to realize business objectives**
- How to **utilize IT to realize the vision of the organization** is to be planned with the required technology and human capital in the organization
- Provides direction to solution delivery
- Eleven subdomains have been identified for planning and organization.

Concerns:

- **Is IT and the business strategy aligned and is the usage of resources optimized?**
- **Does everyone in the organization understand the IT objectives and the risks?**
- **Are these properly managed?**

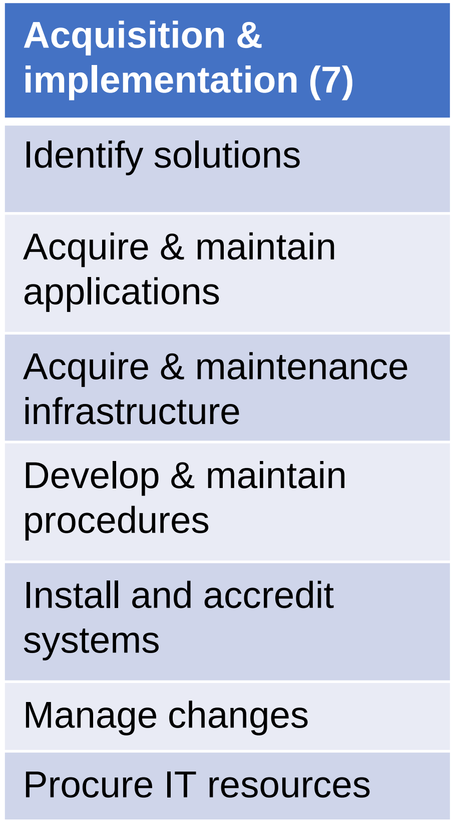
Planning & organizing
Define an IT strategic plan
Define the information architecture
Define technology direction
Define the IT organization
Manage the IT investment
Communicate aims and direction
Manage human resources
Assesses risks
Manage projects
Manage quality

Acquisition and implementation (AI)

- To realize the strategy, IT solutions need to identify, develop, or acquire as well as integrate into business processes.
- As depicted in the diagram seven subdomains have been identified for acquisition and implementation.
- In addition, the life cycle of existing systems through maintenance, enhancements, and retirements is also covered through this domain
- Provides the solutions and passes them to be turned into services

Concerns:

- **Will the new projects deliver solutions that meet business needs in time and within the budget**?



Acquisition & implementation (7)

- Identify solutions
- Acquire & maintain applications
- Acquire & maintenance infrastructure
- Develop & maintain procedures
- Install and accredit systems
- Manage changes
- Procure IT resources

Delivery and Support (DS)

- This domain is to cover the delivery of required services to its stakeholders which range from service, support, performance, security and training.
- 13 sub domains are available to cover the aspects of delivery and support

Concerns

- Are **IT costs optimized** and are **employees using IT efficiently and safely**?
- **Are security measures such as confidentiality, integrity, and availability in place?**

Delivery & support (13)
Define & manage service levels
Manage third-party services
Manage performance & capacity
Ensure continuous service
Ensure systems security
Identify & allocate costs
Educate & train users
Assist & advise customers
Manage the configuration
Manage problems and incidents
Manage data
Manage facilities
Manage operations

Monitoring and Evaluation (ME)

- All IT processes are to **be regularly assessed** for their quality and compliance with control requirements.
- The monitoring domain consists of four sub-domains and addresses the organization’s control processes.
- In addition, assurance is provided through internal or external audits or obtained from alternative sources.

Monitoring
Monitor the processes
Assess internal control adequacy
Obtain independent assurance
Provide for independent audit

Concerns

- **Is IT performance being measured to detect problems before it is too late**?
- **Are risks, control, compliance, and performance being measured and reported?**

Metrics of COBIT

KPIs should be like markers in medicine — a doctor gage your health using a set of indicators that measure the key elements of your health like blood pressure, cholesterol, and body mass index, among others. KPIs should do the same for companies. They should help you make better-informed decisions and get you an idea of how healthy you are or how well a company is doing.

- COBIT uses two types of metrics
- **Outcome measures**
  - Key goal indicators (KGIs)
- What is measured here?
  - Is the information needed available all the time to support the business needs?
  - Are integrity and confidentiality risks absent?
  - Is the information and resources reliable?

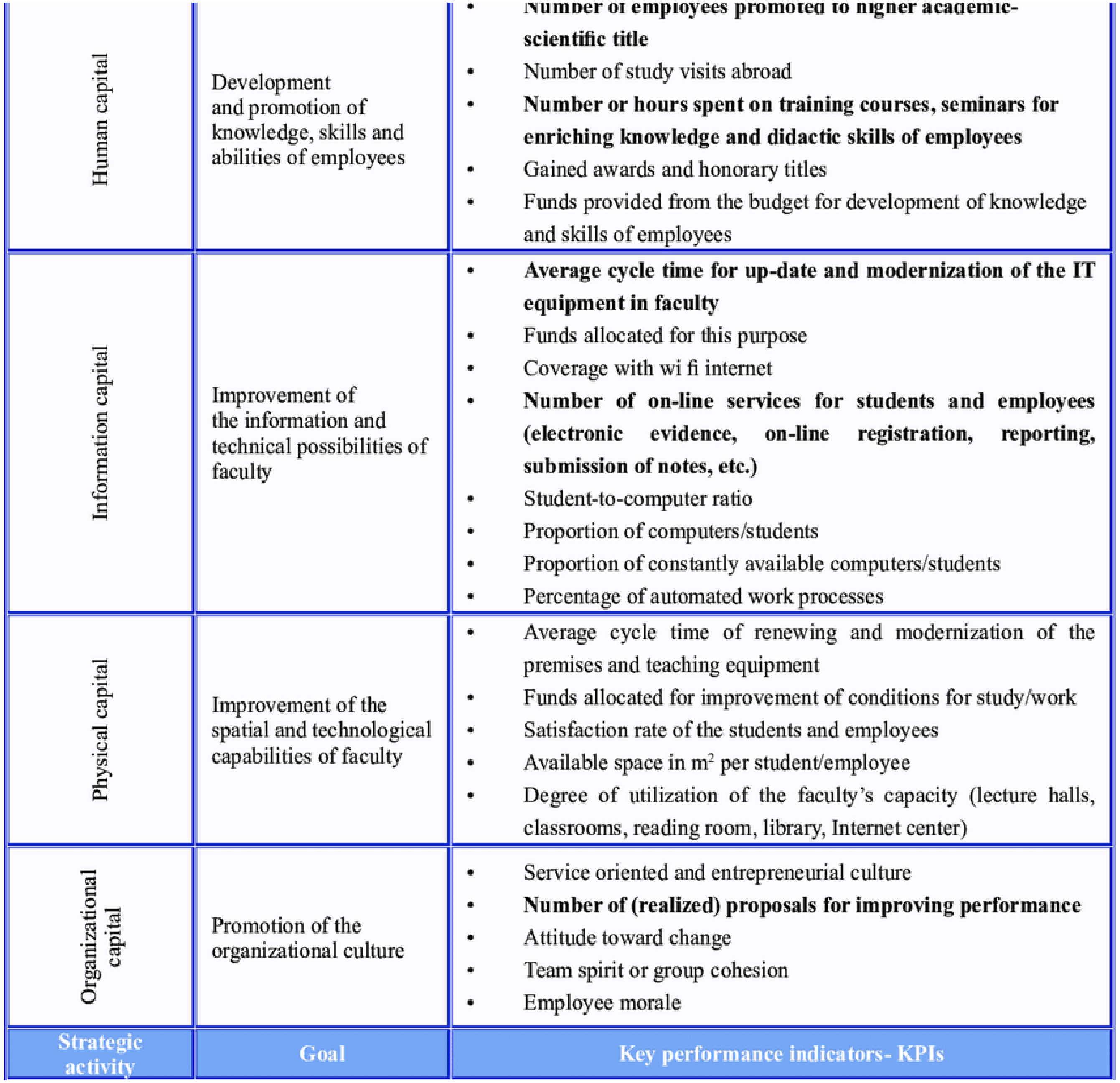
Key Performance Indicators

- Performance indicators, or key performance indicators (KPIs), indicate whether goals are likely to be met.

Example: Sales Target

- Measure the number of sales over a specific time period and compare it to a future target and past performance to motivate your sales team.

Discuss?



Human capital	Development and promotion of knowledge, skills and abilities of employees	• **Number of employees promoted to higher academic-scientific title** • Number of study visits abroad • **Number or hours spent on training courses, seminars for enriching knowledge and didactic skills of employees** • Gained awards and honorary titles • Funds provided from the budget for development of knowledge and skills of employees
Information capital	Improvement of the information and technical possibilities of faculty	• **Average cycle time for up-date and modernization of the IT equipment in faculty** • Funds allocated for this purpose • Coverage with wi fi internet • **Number of on-line services for students and employees (electronic evidence, on-line registration, reporting, submission of notes, etc.)** • Student-to-computer ratio • Proportion of computers/students • Proportion of constantly available computers/students • Percentage of automated work processes
Physical capital	Improvement of the spatial and technological capabilities of faculty	• Average cycle time of renewing and modernization of the premises and teaching equipment • Funds allocated for improvement of conditions for study/work • Satisfaction rate of the students and employees • Available space in m^2 per student/employee • Degree of utilization of the faculty's capacity (lecture halls, classrooms, reading room, library, Internet center)
Organizational capital	Promotion of the organizational culture	• Service oriented and entrepreneurial culture • **Number of (realized) proposals for improving performance** • Attitude toward change • Team spirit or group cohesion • Employee morale
Strategic activity	**Goal**	**Key performance indicators- KPIs**
]

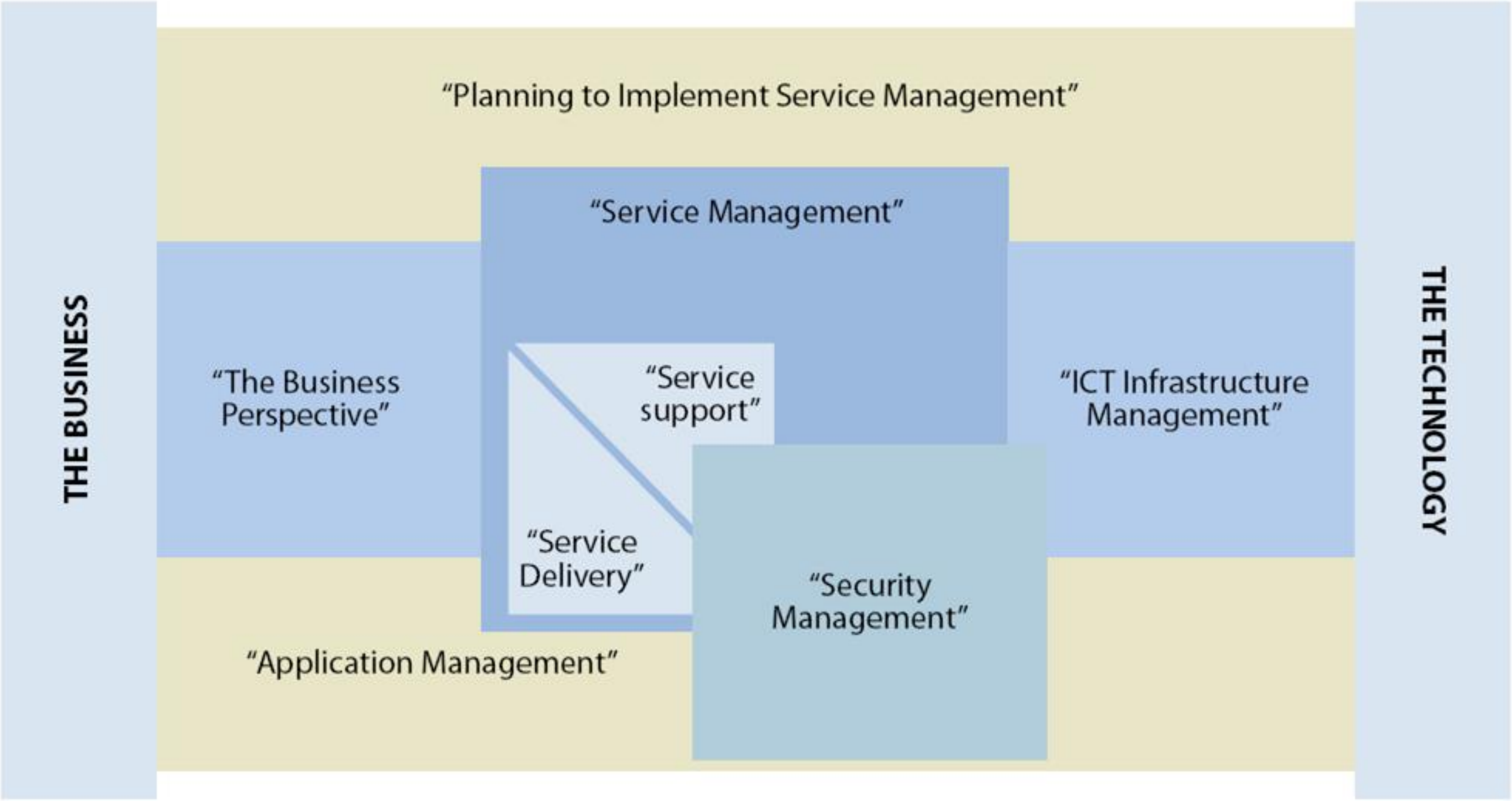
Information Technology Infrastructure Library (ITIL)

- ITIL was initially developed and published by the British Office of Government Commerce (OGC) to promote **efficient and effective use of IT resources** within the British government.
- In 2000, it was revised in conjunction with the British Standards Institute (BSI) and incorporated within BS15000.
- **ITIL is a series of eight books which provides practices for IT service management and delivery.**
- The strength of this framework lies in **service delivery and management**.

ITIL ..

- ITIL framework **does not cover the entire scope of IT governance and aspects of all decision-making** relevant to management.
    - Though this framework traditionally provides little support for strategic IT concerns, however, it receives massive support from all over the world.
- ITIL is a process-oriented framework and focuses on introducing best practices for respective organizations.
- ITIL does not document how to do things but tells you what can and should be doing. It shares with us what other people found to be the best way to approach IT as a service provider

Eight ITIL Books



..contd.. Eight ITIL Books

Planning to implement service management

- This book deals with how to start ITIL in an organisation.
- It provides necessary steps for organizations to identify how it would benefit by the processes of ITIL.
- This book is helpful to identify organization's strengths and weaknesses, current maturity level of service management within the organisation.

The business perspective

This book is to draw attention to align the organisation overall business with the architecture and the processes of ICT.

This book provides best practices in IT service management.

Software asset management

- Software asset management explains **how to manage the entire infrastructure and processes for effective management, control, and protection of software** asset within the organisation.
- This includes the **management of software throughout all the stages of the life cycle**.

Service support

- This book is **to ensure that the customer has access to relevant services to support their business requirements.**
- It includes services such as configuration management, and other support management including incident, problem, change, and release management.

Service delivery

- This book is to **cover the specific business requirements of business users through IT.**
- It includes processes such as service level management, availability management, capacity management, financial management for IT services, and continuity management.

Security management

- This book is to look at the **IT security to all stakeholders** from the service provider perspective.
- It needs to identify the relationship between security management and the IT security officer and to provide necessary security for the entire organisation from the IT perspective.

ICT infrastructure management

- This book covers all aspects of i**nfrastructure management, including design and planning processes, deployment processes, operation processes and technical support processes**.

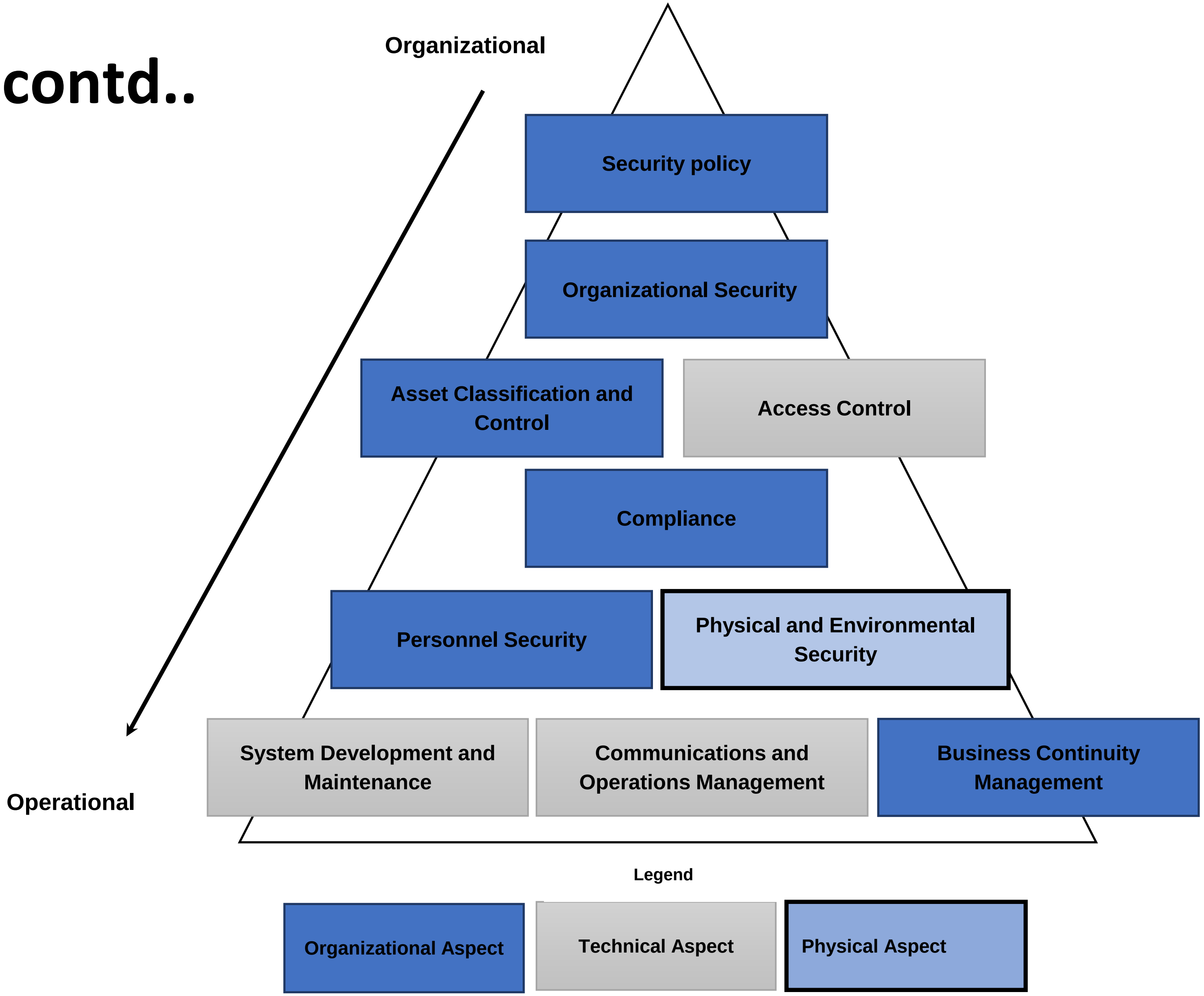
Application management

- This book is to address **application management from the initial requirement identification to all the stages of the application management life cycle**

ISO 17799 ..contd..

- The International Organization for Standardization has introduced a major governance framework ISO 17799, titled “Information Technology – Code of Practice for Information Security Management.
- It provides a framework **to ensure legal compliance and business continuity.**
- This 17799 is based on the British Standard 7799, and it is intended to **create an effective IT security plan for the organization**
- The framework has developed based on **ten domains,** and implementation perspectives vary from organizational to operational. The ten domains are depicted in the Figure.

..contd..
ISO 17799 ..contd..


Organizational
Security policy
Organizational Security
Asset Classification and Control
Access Control
Compliance
Personnel Security
Physical and Environmental Security
System Development and Maintenance
Communications and Operations Management
Business Continuity Management
Operational
Legend
Organizational Aspect
Technical Aspect
Physical Aspect

COBIT vs ITIL

- ITIL was designed as **a service management framework** to help you understand h**ow you support processes, & how you deliver services**
- **COBIT was designed as an IT governance model,** particularly and initially with the **audit in mind to give you control objectives and control practices** on how that process should behave
- The difference between the two is, COBIT tells you what you should be doing, while ITIL tells you how you should be doing it
- Put them together, and you have a very powerful model of what you need to be doing and how to do it.
- **None of these frameworks is in competition with each other. In fact, it is best if they are used together.**

Use of combination of frameworks

- ISO 17799 outlines security controls, but does not focus on how to integrate them into business processes – ITIL focuses on IT processes/services, not on security – COBIT focuses on controls and metrics, not as much on security So, a combination of all three is usually the best approach.
    - COBIT can be used to determine if the company's needs (including security) are being properly supported by IT. ISO 17799 can be used to determine and improve upon the company's security position. And ITIL can be used to improve IT processes & services to meet the company's goals (including security).

Q&A
Questions
Answers