IT Governance – Frameworks and Techniques to get you started or over the hump.

Track: Business Services

Presenter: Mark Thomas

AN INTERFACE TECHNICAL TRAINING LEARNING CONFERENCE

Agenda

- **Introduction & Purpose**
- *IT Governance Evolution and Description*
- *IT Governance Components*
- *Key Methodologies and Frameworks*
- *Closing and Questions*

Synopsis

Too many frameworks, too little time. The IT governance space is full of frameworks, standards and bodies of knowledge. What are these frameworks and what do they mean to IT? This discussion explores some of the most common IT Frameworks, Bodies of Knowledge, and standards and explains how and when they are applicable in an IT organization and pros and cons of each.

Introduction and Purpose

The purpose of today's presentation is to offer you a snapshot of the governance and compliance landscape surrounding Information Technology. When we leave here today, you should understand:

- The size and complexity of the growing external pressures IT organizations are facing in the governance and compliance arenas.
- The fundamentals of IT governance.
- Current methodologies and frameworks that are growing in applicability and popularity in the market today.

Agenda

- *Introduction & Purpose*
- **IT Governance Evolution and Description**
- *IT Governance Components*
- *Key Methodologies and Frameworks*
- *Closing and Questions*

Today’s IT Challenges

- Keeping IT Running
- Value/Costs
- Mastering Complexity
- Aligning IT with Business
- Regulatory Compliance
- Security
- Resources

From itgi.org

Trends

According to a recent article by Compliance 360 on CIO.com, the following is a list of 2011 predictions in the area of Governance, Risk, and Compliance.

- Boards of Directors Returning to Risk Management.
- Measuring the Effectiveness of Compliance Programs.
- Increasing Focus on Third-Party Risk Management.
- Convergence of Compliance and Audit as Integrated Processes.
- Continued Emergence of GRC in the Cloud.

CIO.com: "Major Trends in governance, risk management and compliance for 2011," March 4, 2011

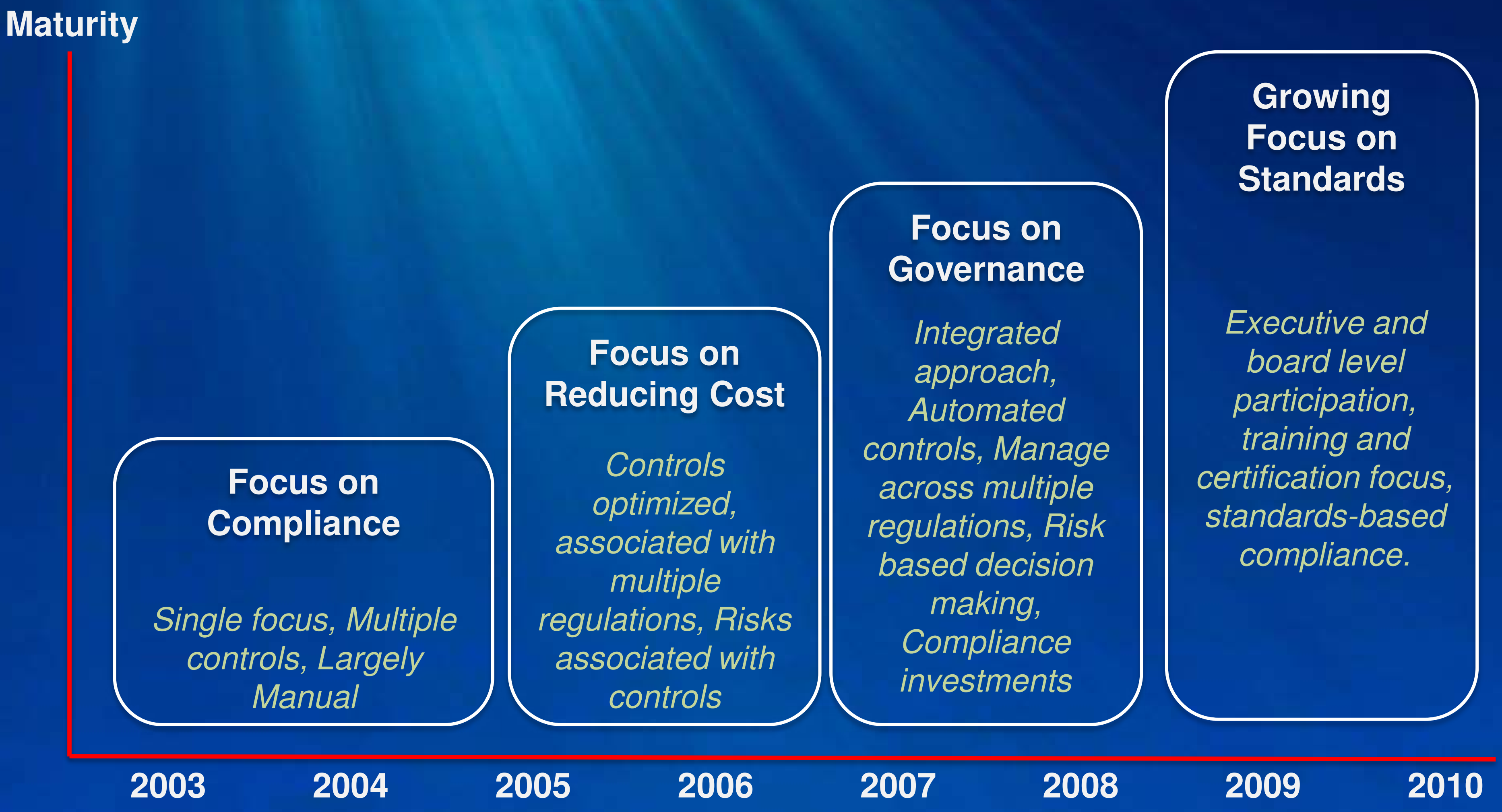
Responsibilities

"IT Governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that enterprise IT sustains the organization's strategies and objectives."

- Integrate and institutionalize good practices.
- Take full advantage of information.
- Satisfy quality, fiduciary and security requirements.
- Optimize resources.
- Balance risk versus return.

Reference: IT Governance Institute, COBIT 4.1

Evolution



Focus on Compliance

Single focus, Multiple controls, Largely Manual

Focus on Reducing Cost

Controls optimized, associated with multiple regulations, Risks associated with controls

Focus on Governance

Integrated approach, Automated controls, Manage across multiple regulations, Risk based decision making, Compliance investments

Growing Focus on Standards

Executive and board level participation, training and certification focus, standards-based compliance.

Agenda

Introduction & Purpose

IT Governance Evolution and Description

IT Governance Components

Key Methodologies and Frameworks

Closing and Questions

Focus Areas and Principles

IT Governance is grouped into the following five focus areas: Strategic Alignment, Value Delivery, Risk Management, Resource Management, and Performance Measurement.

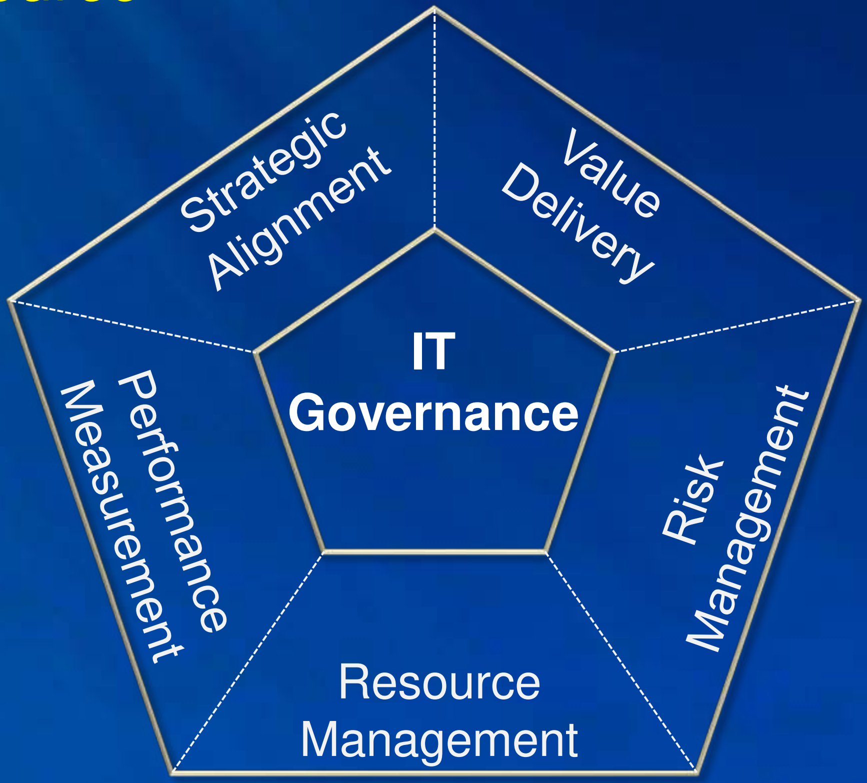
Principles:

Direct and Control

Responsibility

Accountability

Activities



The need for frameworks

Effective IT Governance needs a control framework. The following are requirements for a control framework.

- The need for sharper business focus driven by business needs.
- A common language with a standardized process model, objectives, and tools suitable for any type or size of organization.
- A sound framework for ensuring IT compliance with applicable regulatory and security requirements.
- A reliable and useful source based on best practices which are generally accepted in the industry.

Reference: IT Governance Institute, COBIT 4.1

Agenda

- *Introduction & Purpose*
- *IT Governance Evolution and Description*
- *IT Governance Components*
- **Key Methodologies and Frameworks**
- *Closing and Questions*

Applicable Frameworks

Although there are several methodologies and frameworks competing for the attention of IT leadership, the following are some of the most popular and applicable today.

- *Service Management*: ITIL, MOF
- *IT Controls and Compliance*: COBIT
- *Enterprise Architecture*: TOGAF
- *Project/Portfolio Management*: PMBOK, PRINCE2, Agile PM, BABOK, VAL IT
- *International Standards*: ISO38500, ISO20000, ISO27000
- *Application/Software Development*: SWEBOK, SDLC, Agile
- *Process & Quality Management*: BPM-CBOK, Six Sigma, CMMI

Service Management

IT Infrastructure Library (ITIL)

Microsoft Operations Framework (MOF)

IT Infrastructure Library (ITIL)

ITIL is the most widely accepted approach to IT service management in the world which provides a cohesive set of best practice guidance drawn from public and private sectors.

- Developed by the United Kingdom's Office of Government Commerce (OGC) and has become a world-wide de facto standard in Service Management.
- The Guidance, documented in a set of five books, describes an integrated, process based, best practice framework for managing IT services.
- Currently these books are the only comprehensive, non-proprietary, publicly available guidance for IT Service Management.

ITIL

The ITIL framework identifies all applicable processes, roles, and functions required to effectively deliver services to customers.

Services

A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of costs and risks.

Email

Processes

A coordinated set of activities combining and implementing resources and capabilities in order to produce an outcome which creates value.

Incident Management

Roles

A set of connected behaviors or actions that are performed by a person, team or group for a specific outcome.

Incident Manager

Functions

Units of organization specialized to perform certain types of work and are responsible for certain outcomes.

Service Desk

MOF

MOF provides comprehensive technical guidance for achieving mission-critical production system reliability, availability, supportability, and manageability for solutions and services built on Microsoft's products and technologies.

- Comprises a complete IT service lifecycle that organizes and describes all activities and processes required to manage an IT service.
- Uses question-based guidance to help 1) Determine what your organization needs now, and 2) Keep your IT organization running efficiently and effectively in the future.
- Integrates best practices of Microsoft Solutions Framework.

IT Controls and Compliance

Control Objectives for Information and Related Technology (COBIT)

COBIT

Developed by the IT Governance Institute and ISACA, COBIT is a governance and control framework that focuses on "what needs to be achieved" rather than "how to achieve it."

- Develop, publicize and promote an internationally accepted control framework for business managers, IT, and assurance professionals.
- Resulted in the creation of a growing family of publications and products designed to assist in the implementation of effective IT governance throughout an enterprise.

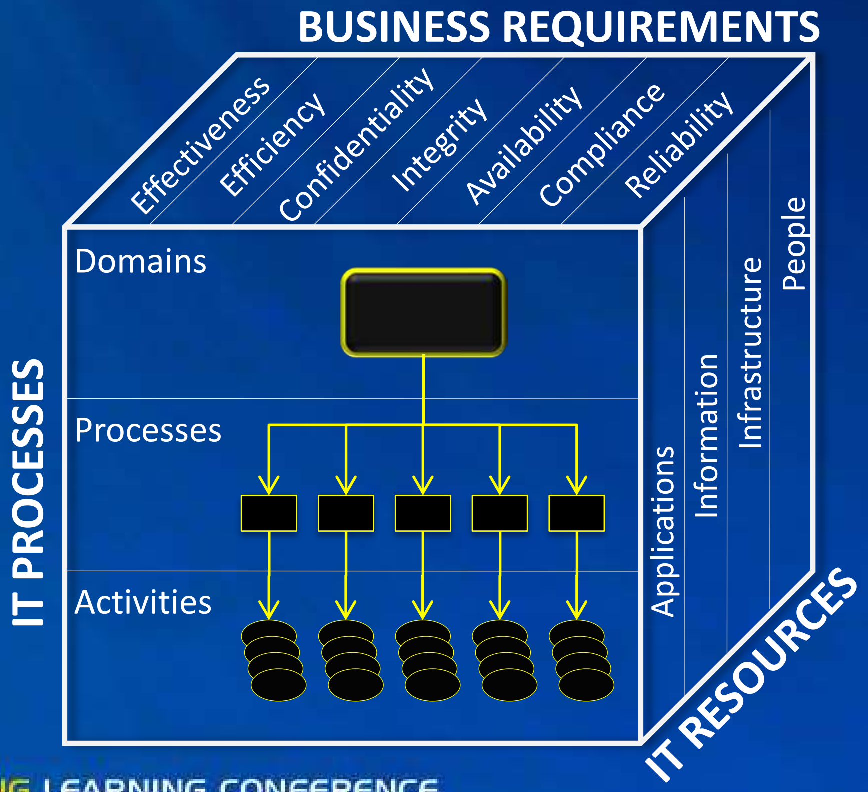
Reference: IT Governance Institute, COBIT 4.1

COBIT

Three key components that assist organizations organize processes and deliver the information that the business needs to achieve its objectives is illustrated in the "COBIT Cube."

IT Processes are grouped into four domains and 34 processes with each process consisting of activities, tasks and Control Objectives.

Control practices convert the control objectives into detailed practices on "how" and "why" the business should adhere to the practices.



Reference: IT Governance Institute, COBIT 4.1

Enterprise Architecture

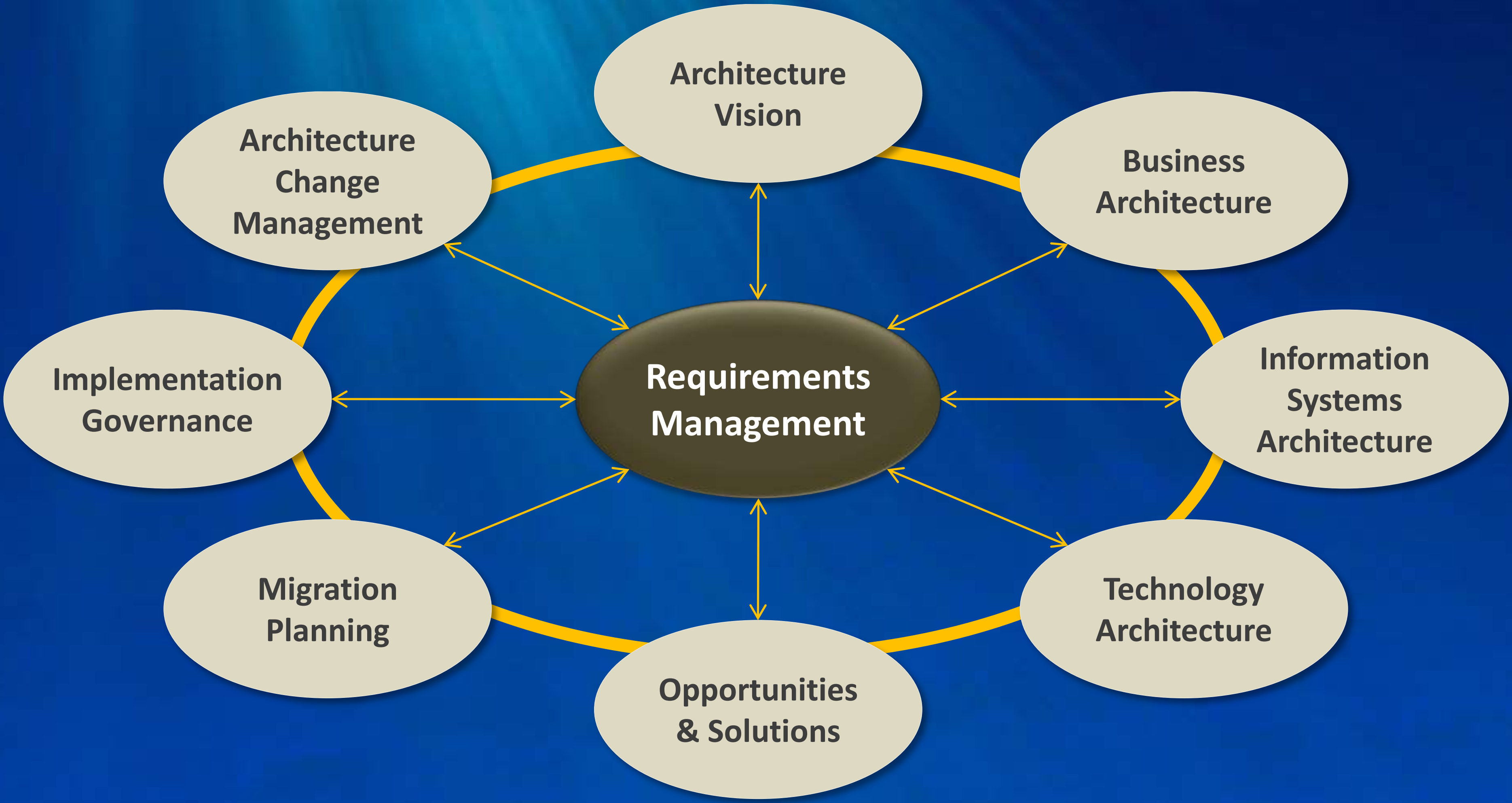
The Open Group Architecture Framework (TOGAF)

TOGAF

TOGAF is a method and set of supporting tools for designing, developing and evaluating an enterprise architecture. The framework consists of four parts:

- *PART I (Introduction)*: Key concepts behind enterprise architecture and the TOGAF approach.
- *PART II (Architecture Development Method)*: Step-by-step approach to developing an enterprise architecture.
- *PART III (Enterprise Continuum)*: Virtual repository of architecture assets.
- *PART IV (Resources)*: Tools and techniques available for use in applying TOGAF.

TOGAF


Architecture Vision
Business Architecture
Information Systems Architecture
Technology Architecture
Opportunities & Solutions
Migration Planning
Implementation Governance
Architecture Change Management
Requirements Management

Project and Portfolio Management

- Project Management Body of Knowledge (PMBOK)
- Projects in Controlled Environments (PRINCE2)
- Agile Project Management
- Business Analysis Body of Knowledge (BABOK)
- VAL IT

Project Management

PMBOK

The Project Management Body of Knowledge, developed by PMI is an internationally recognized standard that provides PM fundamentals for a wide range of projects and industries and promotes a common vocabulary and framework.

PRINCE2

Projects In Controlled Environments 2 is a de-facto standard in the UK and practiced worldwide, PRINCE2 is a process-based approach providing an easily tailored and scalable project management methodology for the management of all types of projects.

AGILE PM

Agile methods for project management processes espouses a lightweight set of activities used to manage the acquisition and development of software. These include requirements, design, coding, and testing based on a minimal set of activities.

BABOK

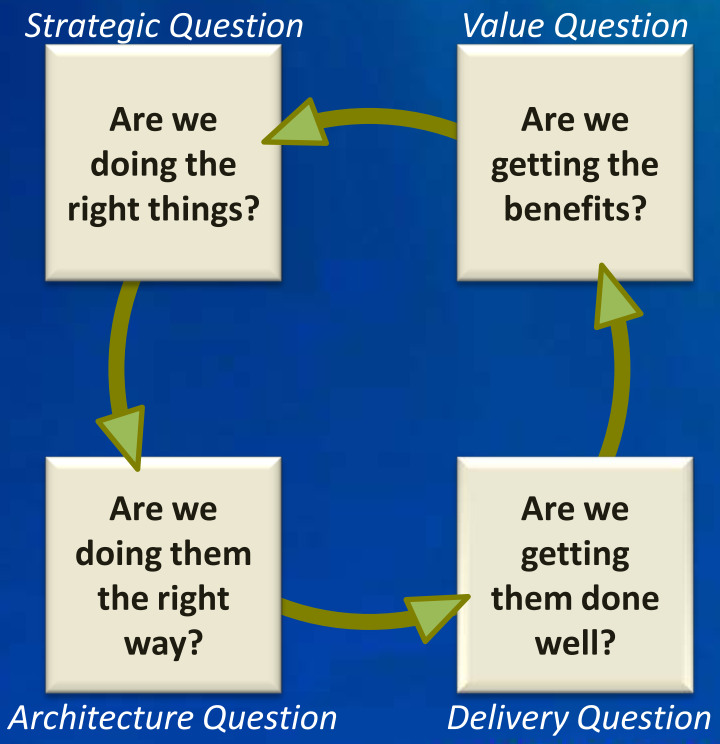
The Business Analysis Body of Knowledge (BABOK) is the collection of knowledge within the profession of Business Analysis and reflects current generally accepted practices.

- Maintained by the IIBA (International Institute of Business Analysis), a professional association in the growing field of Business Analysis.
- Describes areas of knowledge, their activities and the tasks and skills necessary to be effective in their execution.
- Provides the basis for the Certified Business Analysis Professional™ (CBAP®) Certification.

Reference: IIBA, Business Analysis Body of Knowledge (BABOK®), V2.0

VAL IT

Val IT focuses on the value delivery dimension that supports processes related to the evaluation and selection of investments and realized benefits of their delivery.



Strategic Question
Are we doing the right things?
Value Question
Are we getting the benefits?
Are we doing them the right way?
Architecture Question
Are we getting them done well?
Delivery Question

- Applied to management processes including value governance, portfolio management, and investment management.
- Maximizes the quality of business cases for IT-enabled business investments.

Reference: IT Governance Institute, COBIT 4.1

International Standards

- ISO 38500
- ISO 20000
- ISO 27000

ISO 38500

This standard provides guiding principles for organizational directors on governing the acceptable use of IT. It is applicable to organizations with all sizes of IT departments.

- Corporate governance of information technology.
- Establish standard principles for the effective, efficient and acceptable use of IT.
- Provide stakeholders the confidence in the corporate governance of IT provided the standard is followed.

Reference: ISO/IEC 38500: 2008

ISO 38500

The following principles within ISO 38500 articulate six preferred behaviors to guide decision making, referring to what should happen as opposed to prescribing details of how, when, or by whom.

Principle 1: Responsibility

Principle 2: Strategy

Principle 3: Acquisition

Principle 4: Performance

Principle 5: Conformance

Principle 6: Human Behavior

Reference: ISO/IEC 38500: 2008

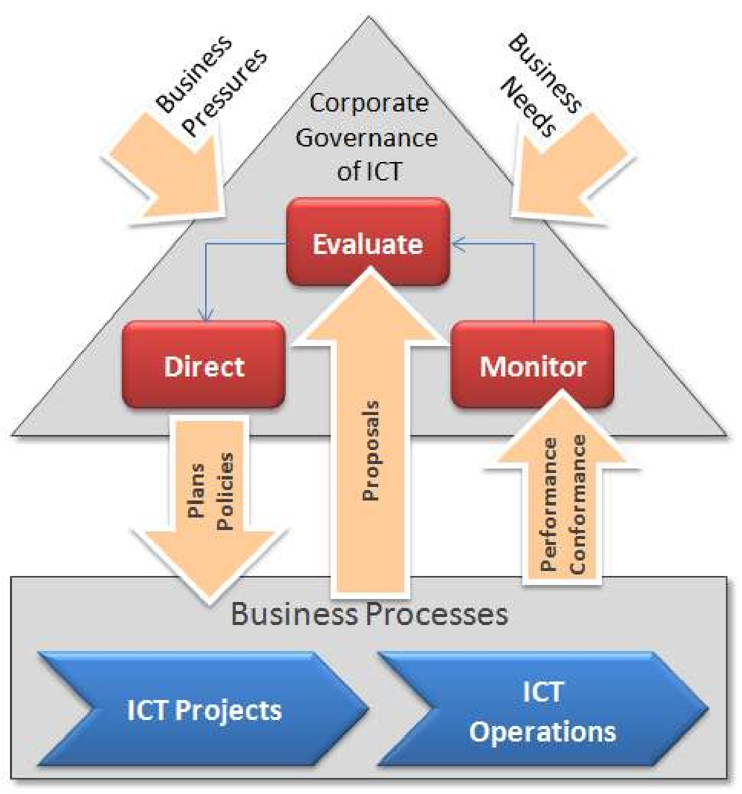
ISO 38500

Within the standard, each of the six principles is further defined using the cycle of Evaluate – Direct – Monitor.

Evaluate the current and future use of IT.

Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.

Monitor conformance to policies, and performance against the plans.



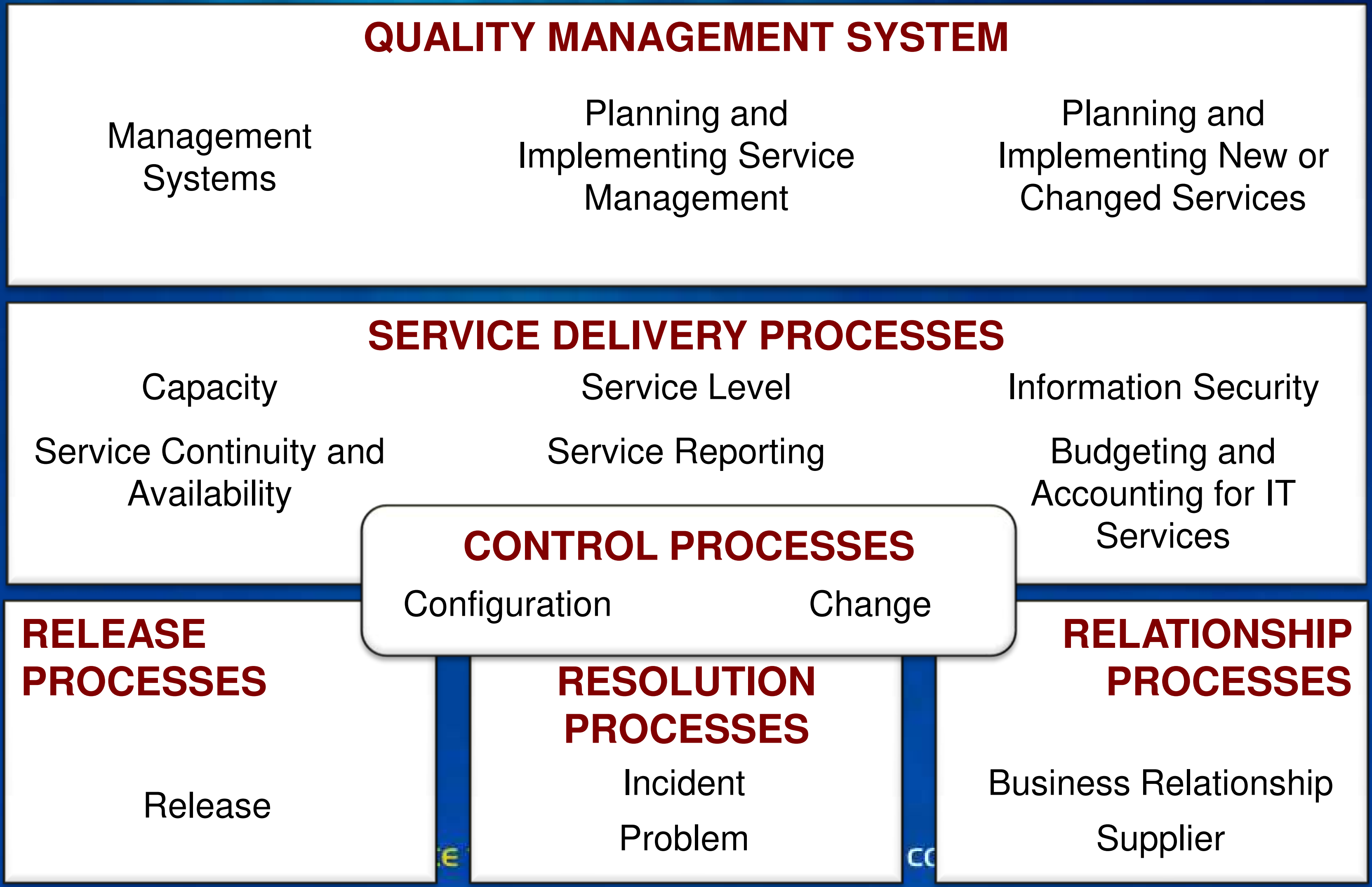
Reference: ISO/IEC 38500: 2008

ISO 20000

ISO 20000 is an international standard that promotes an integrated process approach to delivering IT Services.

- In 2000, the British Standards Institute developed the requirements for the delivery of IT services called BS 15000.
- In late 2005, the International Standards Organization (ISO) accepted BS 15000 as a new international standard called ISO 20000.
- Provides a common standard for any enterprise offering IT services – and a common terminology.
- It does not assess the quality of a service or product, it does certify effective processes.

ISO 20000



QUALITY MANAGEMENT SYSTEM

Management Systems

Planning and Implementing Service Management

Planning and Implementing New or Changed Services

SERVICE DELIVERY PROCESSES

Capacity

Service Level

Information Security

Service Continuity and Availability

Service Reporting

Budgeting and Accounting for IT Services

CONTROL PROCESSES

Configuration

Change

RELEASE PROCESSES

Release

RESOLUTION PROCESSES

Incident

Problem

RELATIONSHIP PROCESSES

Business Relationship

Supplier

ISO 27000

The ISO 27000 series provides best practices and requirements on Information Security. This code of practice replaces the formerly numbered 17799.

ISO 27000 Series

ISO 27001
The specification for an information security management system (ISMS).

ISO 27002
The code of practice for information security outlining potential controls and control mechanisms.

ISO27003
This will be the official number of a new standard with guidance for implementing an ISMS.

ISO 27004
Information security system management measurement and metrics.

ISO 27005
Methodology independent ISO standard for information security risk management.

ISO27006
Guidelines for the accreditation of organizations offering ISMS certification.

Application and Software Development

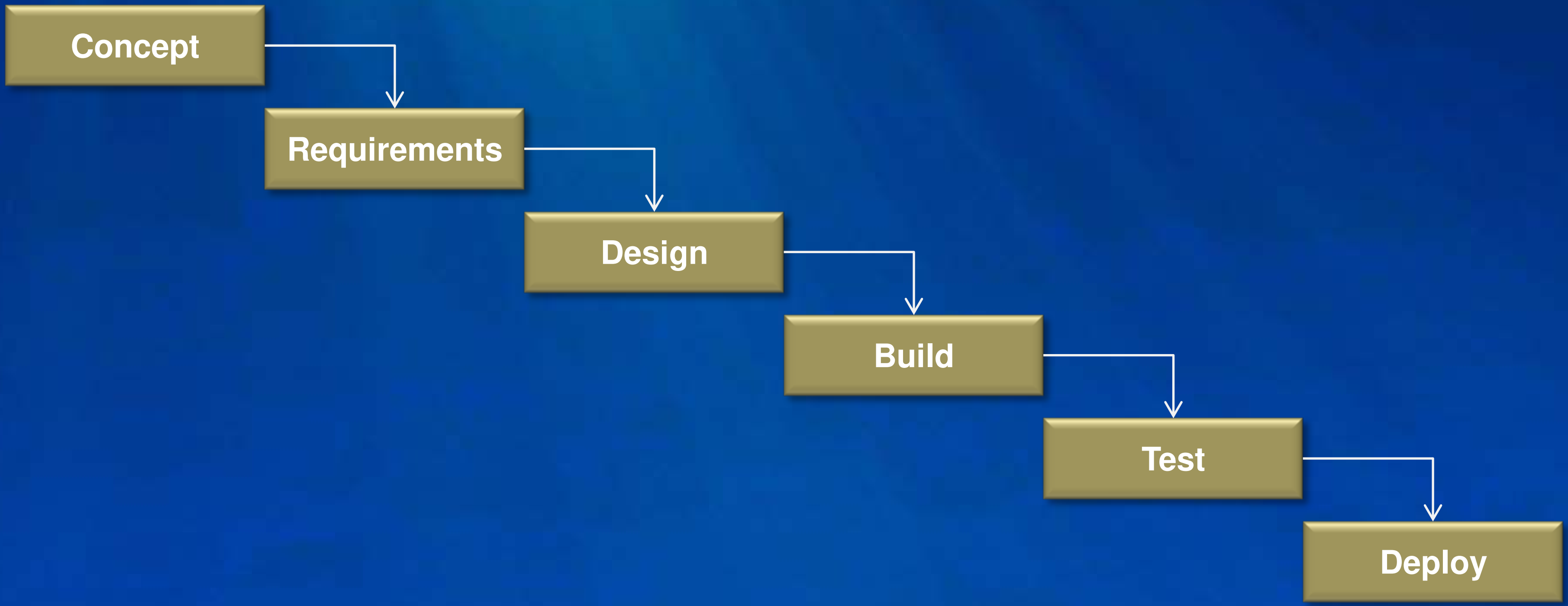
System Development Lifecycle (SDLC)

Software Engineering Body of Knowledge (SWEBOK)

Agile

SDLC

The SDLC, often called the "Waterfall" approach, is a development framework for describing the phases involved in developing business and information systems.



SWEBOK

Software Engineering Body of Knowledge -- motivates the fundamental organization of the Guide into 10 knowledge areas:

```
ion = data
 = dataSource
getConnection()
connection.create
tSQL = "SELECT *
statement.execute
Set.next()) {
```

- Software requirements
- Software design
- Software construction
- Software testing
- Software maintenance
- Software configuration management
- Software engineering management
- Software engineering process
- Software engineering tools and methods
- Software quality

AGILE

In 2001, seventeen software developers met to discuss lightweight development methods. From this meeting, they published the following Agile Manifesto:

- We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:
    - ***Individuals and interactions*** *over processes and tools*
    - ***Working software*** *over comprehensive documentation*
    - ***Customer collaboration*** *over contract negotiation*
    - ***Responding to change*** *over following a plan*
- That is, while there is value in the items on the right, we value the items on the left more.

AGILE

The twelve principles underlie the Agile Manifesto, including:

- Customer satisfaction by rapid delivery of useful software
- Welcome changing requirements, even late in development
- Working software is delivered frequently (weeks rather than months)
- Working software is the principal measure of progress
- Sustainable development, able to maintain a constant pace
- Close, daily co-operation between business people and developers
- Face-to-face conversation is the best form of communication (co-location)
- Projects are built around motivated individuals, who should be trusted
- Continuous attention to technical excellence and good design
- Simplicity
- Self-organizing teams
- Regular adaptation to changing circumstances

Process and Quality Management

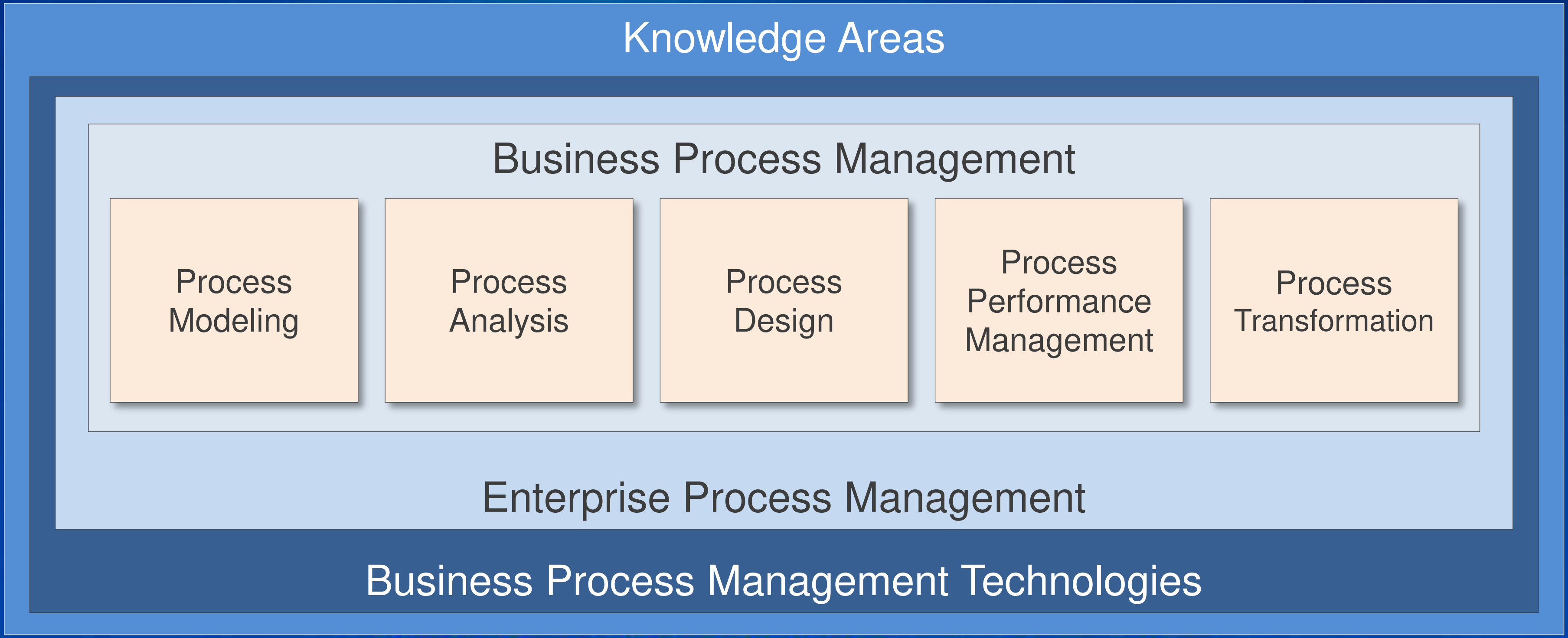
Business Process Management Common Body of Knowledge (BPM-CBOK)

Six Sigma

Capability Maturity Model Integrated (CMMI)

BPM-CBOK

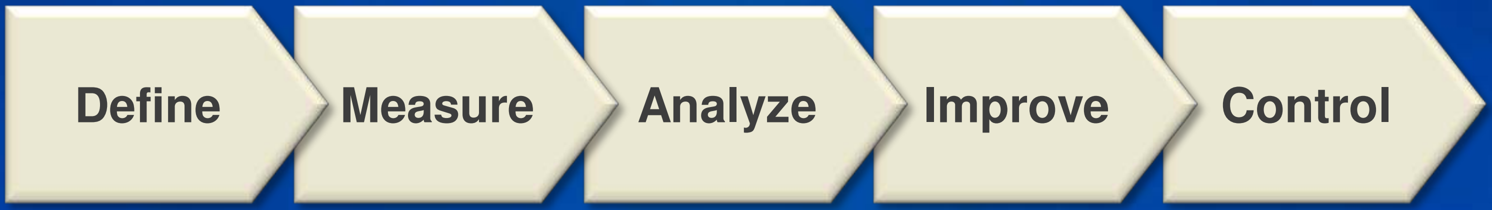
The BPM-CBOK is produced by the Association of Business Process Management Professionals. Its purpose is to provide Knowledge Areas in process management and improvement.


Knowledge Areas
Business Process Management
Process Modeling
Process Analysis
Process Design
Process Performance Management
Process Transformation
Enterprise Process Management
Business Process Management Technologies

Six Sigma

Six Sigma is a quality framework that focuses on reducing costs and increases customer satisfaction by reducing waste in processes that deliver services to customers.

- Six Sigma is about data and facts.
- The central idea is that if you can measure defects in a process, you can systematically eliminate them.
- The elementary Six Sigma methodology was developed, tested, and proven at Motorola in the early 1980s.



Define

Measure

Analyze

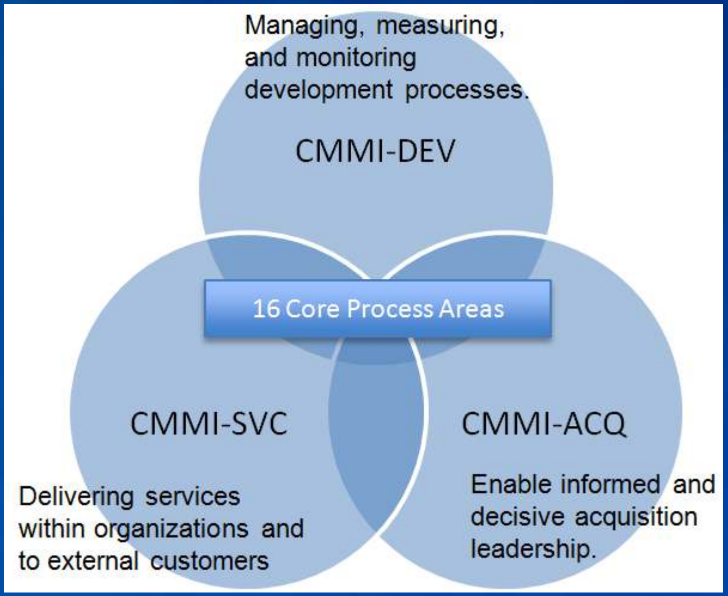
Improve

Control

CMMI

CMMI, developed by the Software Engineering Institute, is a process improvement approach that can be used across a project, a division, or an entire organization and provides a point of reference for appraising current processes.

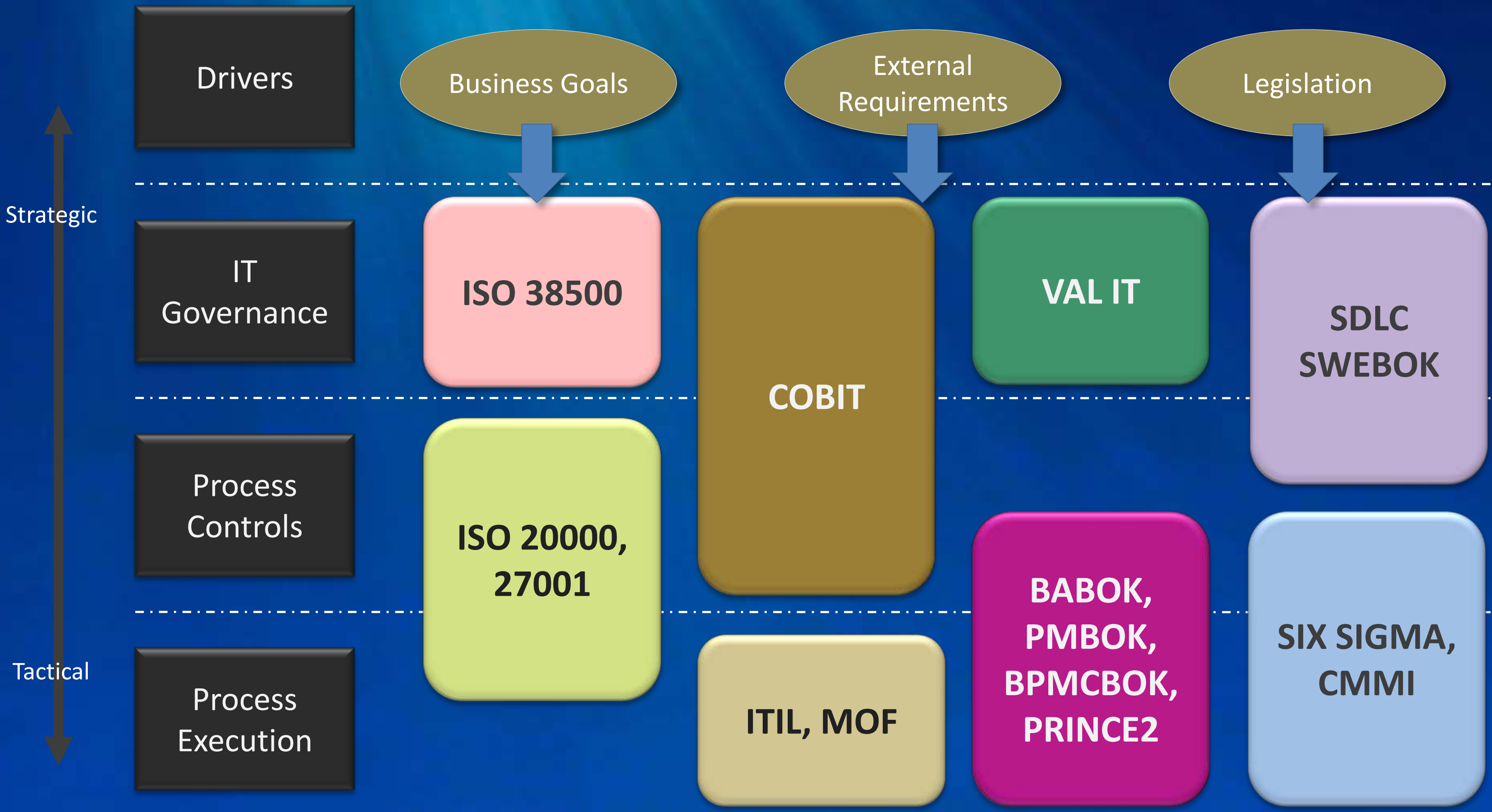
- Structures and organizes the components used in generating models, training materials, and appraisal methods.
- Organized into groupings called constellations, which facilitate construction of approved models.


Managing, measuring, and monitoring development processes.
CMMI-DEV
16 Core Process Areas
CMMI-SVC
CMMI-ACQ
Delivering services within organizations and to external customers
Enable informed and decisive acquisition leadership.

Agenda

- *Introduction & Purpose*
- *IT Governance Evolution and Description*
- *IT Governance Components*
- *Key Methodologies and Frameworks*
- **Closing and Questions**

Putting them together



Strategic

Tactical

Drivers

Business Goals

External Requirements

Legislation

IT Governance

ISO 38500

COBIT

VAL IT

SDLC SWEBOK

Process Controls

ISO 20000, 27001

Process Execution

ITIL, MOF

BABOK, PMBOK, BPMCBOK, PRINCE2

SIX SIGMA, CMMI

Thank you.