IT Governance Frameworks

Bill Pankey
Tunitas Group

Reality Check

• CGEIT domain task requirements necessitate
  – Some knowledge about:
    • COBIT, Val IT
    • the scope, objective and benefits of:
      – IT practices, standards and frameworks, such as ITIL, CMMI, PRINCE2, PMBOK, TOGAF, ISO 17799/27000 series, and the IT Balanced Scorecard
      – of continuous process improvement, such as Six Sigma, Total Quality Management and the Balanced Scorecard
  ‡ but not, Detailed knowledge or expertise
    • Internals of the framework
    • Ability to implement or manage the use of
Reality Check 2

Framework domain tasks emphasize skills that enable an organization to operate holistically—one mission, one vision, one strategy, one set of priorities

- Drive the establishment of IT governance for the enterprise that: considers the values, philosophy, management style, IT awareness, organizational structure, standards and policies.

- Establish specialized governance structures, such as an enterprise investment committee, a resource forecasting process, an ERM ...

- Ensure that appropriate roles, responsibilities and accountabilities are defined, assigned and enforced for information requirements, data and system ownership, IT processes, and benefits and value realization.

Reality Check 3

Domain tasks emphasize use of frameworks to provide assurance that:

- IT governance framework enables the enterprise to achieve optimal value

- IT conforms with external requirements; contractual terms; organizational policies; plans and procedures; generally accepted practices; and the effective and efficient practice of IT

- IT governance monitoring (considering cost/benefits analyses of controls, return on investment for continuous monitoring, etc.), an approach to track all IT governance issues and remedial actions to closure, and a lessons-learned process.

Successful IT governance requires the means and methods of managing and coordinating across departments and IT boundaries.
Today’s Agenda

• Organizational factors in framework adoption
  – How an organization operates is important
    • Drivers for IT Governance initiative
    • Preference for type of ‘governance’ structures

• Frameworks Survey
  – How each framework defines
    • Area of application
    • Appropriate roles, responsibilities, accountabilities and ownership
    • [IT] processes, the benefits and value realized from them

ORGANIZATIONAL FACTORS
Sentinel Events

As likely or not, new IT governance program will be driven by one or more adverse events:

- Poor Performance
  - Poor return on IT investments
  - Program Failures
  - Compliance / security issues
  - User dissatisfaction
  - Rigid infrastructure

- Auditor recommendation
  - Process failures
  - Risks not identified or not addressed
  - Skills not being refreshed
  - Change too difficult

![Linked Business Goals to IT Goals](image)

Linked, in turn, to COBIT control objectives
Poor Cultural Patterns to Overcome

- Going it alone-IT culture of self governance
  - fails to reach out to business or get input and buy in to IT directions and strategies
- Failure to recognize business units have alternatives
  - unresponsive IT will drive business units to outsourced solutions
- Cult of personality
  - a few dominate or derail planning and decision making
- Many silos of IT activity
  - failure to use strategy as an aligning force; failure to communicate or measure
- Historical rather than future based planning
  - failure to take a risk management perspective in defining new budgets and programs
- Too many “strategies” or frequent strategy changes
  - failure to measure progress, communicate strategy, ensure key initiatives are tied to strategy

Key Questions for IT Governance

- What drives the governance initiative?
  - Financials--Growth, profit, return on assets
  - Non-financials—Reputation, culture, market place
- Who will decide?
  - Board
  - Sr. Executives
  - Business Units
  - IT Management

Governance values interdisciplinary decision making—not a strict hierarchical top down approach

- What is the level of Corporate & IT Maturity
  - Evolutionary / revolutionary change
  - Control vs autonomy
  - Large scale vs intimate
Actors

• Board & Sr. Executives
  – Proxy for stakeholders
  – Accountable for the production of value | delivery of service
  – Duty to protect corporate asset
• the Business
  – Managers of the production and delivery of customer value
• Technology
  – Supports the Business with appropriate information & IT related services

How decisions are made

1. Characteristic decision patterns reflect the various importance of the different actors in making decisions
2. Enterprise may adopt different patterns for different decisions
3. Different patterns work better or worse in different companies and for different decisions
4. No a priori preference for one pattern over another, although industry results may recommend one pattern over another
Decision Structures (aka, patterns, archetypes)*

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Input &amp; Decision Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Monarchy</td>
<td>Group of senior business executives (CXO) acting individually or in committees. Precludes IT executives acting independently</td>
</tr>
<tr>
<td>IT Monarchy</td>
<td>Group of IT executives acting independently or in committees</td>
</tr>
<tr>
<td>Feudal</td>
<td>Business units leaders or key process owners</td>
</tr>
<tr>
<td>Federal</td>
<td>Sr. Executives and business unit leaders</td>
</tr>
<tr>
<td>IT Duopoly</td>
<td>IT executives and one other group (business unit leader, process owner, or Sr. executives)</td>
</tr>
<tr>
<td>Anarchy</td>
<td>Each individual user</td>
</tr>
</tbody>
</table>

*Wiell & Ross, IT Governance

A Typical Decision Pattern

<table>
<thead>
<tr>
<th>A Profile characterizes the firm’s IT governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles</td>
</tr>
<tr>
<td>Input</td>
</tr>
<tr>
<td>Business Monarchy</td>
</tr>
<tr>
<td>IT Monarchy</td>
</tr>
<tr>
<td>Feudal</td>
</tr>
<tr>
<td>Federal</td>
</tr>
<tr>
<td>IT Duopoly</td>
</tr>
<tr>
<td>Anarchy</td>
</tr>
</tbody>
</table>
### Academic Research:*

#### Characteristics of the Best | Worst Governance

| Significant positive (+) & negative (0) correlation with governance quality |
|---|---|---|---|---|---|
| Principles | Architecture | Infrastructure | Application | Priorities |
| Business Monarchy | | | | |
| IT Monarchy | | | | |
| Feudal | | | 0 | |
| Federal | + 0 0 0 + 0 | |
| IT Duopoly | 0 + 0 | + 0 | |
| Anarchy | | | | |

*MIT Center for Information Systems Research

### Academic Research:*

#### Characteristics of Top Financial Performers

| Patterns most used by firms with high ROA(return of assets), growth, or profit |
|---|---|---|---|---|---|
| Principles | Architecture | Infrastructure | Application | Priorities |
| Business Monarchy | Profit Growth | Profit | Profit | Growth | Profit Growth |
| IT Monarchy | | ✓ | Profit | Growth |
| Feudal | | | | |
| Federal | | | Profit | ✓ |
| IT Duopoly | ROA | ROA | ROA | ROA | ROA |
| Anarchy | | | | |

*MIT Center for Information Systems Research

kB1

---

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in SF-ISACA’s 2011 CGEIT Preparation Class. No other use is permitted without express written authorization.
“Board Briefing”
ISACA Identified Structures

<table>
<thead>
<tr>
<th>Business dominance</th>
<th>profit oriented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles</td>
<td>Architecture</td>
</tr>
<tr>
<td>Input</td>
<td>Decision</td>
</tr>
</tbody>
</table>

IT Strategy Committee (Business Monarchy) | x |
IT Steering Committee (Business Monarchy) | x | x | x | x |
Technology Council (IT Monarchy) | x | x | x |
IT Architectural Review Board (IT Monarchy) | x | x |

What is an IT Framework?
Calder-Moir Framework of Frameworks (ISO 38500)
COBIT
ITIL
ISO17799
ISO 900x

FRAMEWORKS

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in SF-ISACA’s 2011 CGEIT Preparation Class. No other use is permitted without express written authorization.
What is a framework?

Frameworks in Software Engineering*

A framework, in computer programming, is an abstraction in which common code providing generic functionality can be selectively overridden or specialized by user code providing specific functionality. Frameworks are a special case of software libraries in that they are reusable abstractions of code wrapped in a well-defined Application programming interface (API), yet they contain some key distinguishing features that separate them from normal libraries.

Software frameworks have these distinguishing features that separate them from libraries or normal user applications:

- **inversion of control** - In a framework, unlike in libraries or normal user applications, the overall program's flow of control is dictated by the framework.
- **default behavior** - A framework has a default behavior. This default behavior must actually be some useful behavior and not a series of no-ops.
- **extensibility** - A framework can be extended by the user usually by selective overriding or specialized by user code providing specific functionality.
- **non-modifiable** framework code - The framework code, in general, is not allowed to be modified. Users can extend the framework, but not modify its code.

* Wikipedia: Software Framework

Frameworks concept applied to IT

A framework is a way of organizing activity to include:

- Task definition (library functions)
- Workflow (program flow)
- Roles and responsibilities (library functions)
- Default behavior
- Standards & ‘Principles’ (non-modifiable code)
- Extensibility

A Framework communicates management’s expectation as to how management tasks will be completed.
What is a Governance Framework?

Way of organizing the component activities of IT governance

- Strategy, tactics, objectives, controls, metrics, assessments, audit, communication, accountabilities

As implemented, a Governance Frameworks can be **good or bad**.

Standard Tests:

**Existence**
- Well defined in corporate policy and procedure
- Active participation of accountable parties

**Completeness**
- Adequately cover governance objectives of alignment, value delivery, risk & resource management, performance measurement

**Efficiency**
- Minimum controls suitable for objective
- Appropriate reuse of process inputs / outputs
- Support industry best practice
- Readily comprehended by relevant parties

**Effectiveness**
- Accomplish the governance objectives of IT value creation and preservation

---

IT Governance LifeCycle

1. Board / Executive Awareness
   - Recognition
   - Board Questions
   - IT Governance Charter

2. Establish IT Governance Framework(s)
   - Select
   - Adapt
   - Integrate
   - Implement
   - Use
   - Improve

3. Monitor Performance
ISO38500: Framework Roles

Board: direct, evaluate, monitor IT to support the businesses

Executives: Manage activities to deliver 'end to end' process

Select
Adapt
Integrate

IT Practitioners: design, assess, control & deliver IT support for business

Implement
Use
Improve

Calder-Moir IT Governance LifeCycle

1. Develop strategy
2. Address Risk \ set constraints
3. Architecture & Plans
4. Make changes / implement
5. Verification
6. Operate
### Framework Scope (1)

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Governance</td>
<td>Focus on how to manage information, information and communication technology efficiently and effectively</td>
<td>COBIT, ValIT</td>
</tr>
<tr>
<td>Service Management</td>
<td>How to perform and organize IT management, such as service delivery &amp; support</td>
<td>ITIL, Generic Framework</td>
</tr>
<tr>
<td>Quality Management</td>
<td>Quality standards applied to IT domains</td>
<td>ISO 9000, ISO 20000,</td>
</tr>
<tr>
<td>Quality Improvement</td>
<td>Improvement of processes or performance</td>
<td>IT BSC, CMM, Six-Sigma</td>
</tr>
<tr>
<td>Project Management</td>
<td>Portfolio, program &amp; project management</td>
<td>PMBOK, MSP, PRINCE2</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Identifying &amp; managing risk</td>
<td>ISO 2700x, RiskIT, OCTAVE, FIRM, AS/NZ 4360</td>
</tr>
</tbody>
</table>
IT Frameworks

Overlapping Content w/ varying purpose / specificity

COSO

COBIT

ISO 17799

ITIL

ISO 9000

WHAT

HOW

Breath of Application

Framework Specificity

For example, varying levels of security guidance
Some Governance Frameworks

- **Topics**
  - Framework Concepts & Organization
    - Calder-Moir / ISO 38500
  - Survey
    - Strategy: Balanced Scorecard
    - Risk & Compliance: COSO | COBIT | ISO 2700x | PCIDSS
    - Architecture & Plans: TOGAF | Zachman
    - Implement & Manage Change: PMBOK | PRINCE2 | COBIT
    - Verify: Balanced Scorecard, Zachman
    - Operate: ITIL | ISO 9000 | Six-Sigma

How ISACA Positions COBIT

COBIT is the application of COSO to IT
COBIT Supports Multiple Audiences

- **Management**
  - Help govern, direct, manage and monitor IT activities
  - *Are we doing the right things*
- **IT & Business Users**
  - Implement **better managed** IT solutions
- **Auditors / Consultants**
  - Substantiate opinions & advice on internal controls

How COBIT Helps Governance Process

- **Provide Direction**
  - COBIT links IT & business goals
  - SET OBJECTIVES
  - *IT business alignment*
  - *IT enables business & mgmt benefits*
  - *IT resources used responsibly*
  - *IT risks are managed appropriately*

- **Measure Performance**
  - IT ACTIVITIES
  - *Increase automation*
  - *Decrease Cost*
  - *Manage Risk*

- **COMPARE**
  - COBIT KGIs and KPIs enable measurement
  - COBIT process & maturity models focus on IT capability

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in SF-ISACA’s 2011 CGEIT Preparation Class. No other use is permitted without express written authorization.
**COBIT Support for Governance Objectives**

<table>
<thead>
<tr>
<th>COBIT Feature</th>
<th>Governance Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business &amp; IT KGI</td>
<td>Align IT strategy w/ business goals</td>
</tr>
<tr>
<td></td>
<td>Cascade strategy down into organization</td>
</tr>
<tr>
<td></td>
<td>Set up functions that facilitate strategy implementation</td>
</tr>
<tr>
<td>COBIT Framework</td>
<td>Adopt control &amp; governance framework</td>
</tr>
<tr>
<td></td>
<td>Provide IT infrastructure that facilitates creation &amp; sharing of business information</td>
</tr>
<tr>
<td></td>
<td>Embed responsibility for risk management</td>
</tr>
<tr>
<td>IT Processes Mgmt Guidelines KPI CMM</td>
<td>Focus on important IT processes and core competence</td>
</tr>
<tr>
<td></td>
<td>Measure performance</td>
</tr>
<tr>
<td></td>
<td>Identified areas where improvement needed</td>
</tr>
<tr>
<td></td>
<td>Appreciate consequences of incorrect or no action</td>
</tr>
</tbody>
</table>

**COBIT Framework**

- Business
  - Requirements
  - Information
- IT Processes
  - Audited with
  - Measured by
- Control Outcome Tests
- Control Objectives
  - Audited with
  - Implemented with
- Key Performance Indicators
- Key Goal Indicators
- Maturity Models
- Control Design Tests
- Control Practices

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in SF-ISACA’s 2011 CGEIT Preparation Class. No other use is permitted without express written authorization.
Digression

What is ‘process’?

- **Organized set of activities**
  - a. Produce specific results / outcome
  - b. Responds to specific events (triggers)
  - c. Has identified ‘customer’ receiving the benefit of the process *(ITIL perspective)*
  - d. Performance is measurable
- **Defined roles *(COBIT Perspective)***
  - Process **Owner**, responsible for results
  - Process **Manager**, responsible for ‘realization and structure’; report to PO
  - Process **Operatives**, responsible for specific process activities, report to PM

---

Process Control

Measurement & Control is an essential aspect of COBIT ‘process’
COBIT Framework: Requirements Cascade

Business Requirements => Process Definition => Resource Management

- Business requirements are specified in terms of the following information properties:
  - Effectiveness
  - Efficiency
  - Confidentiality
  - Integrity
  - Availability
  - Compliance
  - Reliability

Information requirements cascade to requirements for IT
Information Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Requirements for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectiveness</td>
<td>Information being relevant and pertinent to business process delivered in a timely, correct, consistent and reliable manner</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Most productive and economical use of resources</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Protection from unauthorized disclosure</td>
</tr>
<tr>
<td>Integrity</td>
<td>Accuracy and completeness of information</td>
</tr>
<tr>
<td>Availability</td>
<td>Being available when required by the business process. Safeguarding resources and capability.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Conformance with laws, regulations and contractual requirements</td>
</tr>
<tr>
<td>Reliability</td>
<td>Provisioning of appropriate information to management to operate in exercise fiduciary &amp; governance responsibilities.</td>
</tr>
</tbody>
</table>

COBIT OUTPUT

- List of the required IT processes
  - Each associated a high level ‘objective’
  - Catalog is intended to be ‘complete’
- ‘Best Practice’ Process definition
  - Detailed sequence of activity
  - Affected information properties
  - Resource utilization
  - Process inputs and outputs
  - Goals and metrics
  - Roles
  - Competency
Process Catalogue
Domains => Processes => Activities

Domains
- Plan & Organize
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate

“Natural” grouping of processes

Series of processes supporting domain goals

Processes
- 1. IT Performance
- 2. Internal Control
- 3. Regulatory Compliance
- 4. IT Governance

Activities / Tasks

Actions needed to achieve measurable result. Activities have lifecycles.Tasks are discrete

Other Frameworks Complement COBIT

Figure 10—High-level Mapping of Guidance to CoIT Domains

<table>
<thead>
<tr>
<th>Framework</th>
<th>PO</th>
<th>AI</th>
<th>DS</th>
<th>ME</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSO</td>
<td>+</td>
<td>+</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ITIL</td>
<td>0</td>
<td>0</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>ISO/IEC 17799</td>
<td>0</td>
<td>+</td>
<td>+</td>
<td>0</td>
</tr>
<tr>
<td>FIPS PUB 200</td>
<td>0</td>
<td>+</td>
<td>+</td>
<td>0</td>
</tr>
<tr>
<td>ISO/IEC 13335</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>ISO/IEC 15408</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>PRINCE2</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>PMBOK</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>TickIT</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>CMMI</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>TOGAF 8.1</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IT BPM</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>NIST 800-14</td>
<td>0</td>
<td>+</td>
<td>+</td>
<td>0</td>
</tr>
</tbody>
</table>

(+): Frequently addressed
(o): Moderately addressed
(+): Not or rarely addressed

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in SF-ISACA’s 2011 CGEIT Preparation Class. No other use is permitted without express written authorization.
Governance Frameworks

- **Topics**
  - Framework Concepts & Organization
    - COSO Cube
  - Survey
    - COBIT
    - COSO ERM | ISO 2700x | M_O_R | OCTAVE | ISO3100
    - ITIL
    - ISO 9000 | Six-Sigma
    - Balanced Scorecard | TOGAF | Zachman
    - CMMI
    - PMBOK | PRINCE2

---

ISO 2700x Infosec Framework

Table 1.1 ISO 27000 Family

<table>
<thead>
<tr>
<th>ISO/IEC</th>
<th>Standard Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27001</td>
<td>Information Security Management System requirements (specification)</td>
</tr>
<tr>
<td>27002</td>
<td>Code of practice for information security; management</td>
</tr>
<tr>
<td>27003</td>
<td>(Pending) Implementation guidance</td>
</tr>
<tr>
<td>27004</td>
<td>(Pending) Metric and measurement</td>
</tr>
<tr>
<td>27005</td>
<td>(Pending) Risk management</td>
</tr>
</tbody>
</table>

- ISMS monitoring and review guidelines
- ISMS internal auditing
- ISMS continual improvements
Digression: Security Framework Related Issues for CGEIT Study

- Knowledge of details has not been on the test
- Know the difference between a Code of Practice and a Certification Standard
- Security Standards Lead other disciplines in the rigor and approach of available standards – contrast with project management
- Know why standards are important in the context of governance
  - In some cases, they offer certification
  - In all cases they offer widely accepted language and methods for a particular discipline
  - In the case of ISO, integration with other standards and a holistic approach

Some Governance Frameworks

- Topics
  - Framework Concepts & Organization
    - Calder-Moir / ISO 38500
  - Survey
    - Strategy: Balanced Scorecard
    - Risk & Compliance: COSO | COBIT | ISO 2700x | PCIDSS
    - Architecture & Plans: TOGAF | Zachman
    - Implement & Manage Change: PMBOK | PRINCE2 | COBIT
    - Verify: Balanced Scorecard, Zachman
    - Operate: ITIL | ISO 9000 | Six-Sigma
TOGAF Four Architecture Domains

- **The Open Group Architecture Framework (TOGAF)**
  - framework for enterprise architecture
  - a comprehensive approach to the design, planning, implementation, and governance of an enterprise information architecture

- TOGAF is based on four **architecture domains**:
  - **Business architecture** or business process architecture: which defines the business strategy, governance, organization, and key business processes of the organization
  - **Applications architecture** which provides a blueprint for the individual application systems to be deployed, the interactions between the application systems, and their relationships to the core business processes of the organization
  - **Data architecture** which describes the structure of an organization's logical and physical data assets and the associated data management resources
  - **Infrastructure or Technical architecture or Technology architecture** which describes the hardware, software and network infrastructure needed to support the deployment of core, mission-critical applications

TOGAF Framework

The **architecture framework** is a toolset or set of tools which can be used for developing a broad range of different architectures. It

- describe a method for defining an information system in terms of a set of building blocks
- show how the building blocks fit together
- contain a set of tools
- provide a common vocabulary
- include a list of recommended standards
- include a list of compliant products that can be used to implement the building blocks
TOGAF Architecture Development Method

- The Architecture Development Method (ADM) is applied to develop an enterprise architecture which will meet the business and information technology needs of an organization. It may be tailored to the organization’s needs and is then employed to manage the execution of architecture planning activities.

- The process is iterative and cyclic. Each step checks with Requirements. Phase C involves some combination of both Data Architecture and Applications Architecture. Additional clarity can be added between steps B. and C. in order to provide a complete information architecture.

- Performance engineering working practices are applied to the Requirements phase, and to the Business Architecture, Information System Architecture, and Technology architecture phases. Within Information System Architecture, it is applied to both the Data Architecture and Application Architecture.
Some Governance Frameworks

• **Topics**
  – **Framework Concepts & Organization**
    • Calder-Moir / ISO 38500
  – **Survey**
    • Strategy: Balanced Scorecard
    • Risk & Compliance: COSO | COBIT | ISO 2700x | PCIDSS
    • Architecture & Plans: TOGAF | Zachman
    • **Implement & Manage Change:** PMBOK | PRINCE2 | COBIT
    • Verify: Balanced Scorecard, Zachman
    • Operate: ITIL | ISO 9000 | Six-Sigma

---

PMBOK

**General ‘project management’ book of knowledge**

– Maintained by Project Management Institute (PMI)
  • Basis of PMP certification

• **Plan centric approach to project management**
  • E.g., management of ‘project risk’ occurs as an artifact of the development, maintenance and monitoring of a ‘project risk management plan’
  • E.g., same-same ‘quality management’, quality management plan
Standardized Project Phases

- **Initiation**
  - Feasibility, scoping & project charter
- **Planning**
  - Project Management Plan to manage numerous subordinate plans
- **Plan Execution**
  - Deliver on plan
  - Request and implement changes to plan
- **Monitoring & Controlling Plans**
  - Approval of change requests
  - Update plan
  - Status reports & forecasts
- **Closing**
  - Verification, delivery and signoff

PMBOK Best Practices

Defines inputs, tools and techniques and outputs for 9 project management areas
- Integration Management
- Scope management
- Time Management
- Cost Management
- Quality Management
- Human Resource Management
- Communications Management
- Risk Management
- Procurement Resource Management

All PMBOK maps to a single COBIT process, PO10 | Manage Projects
Some Governance Frameworks

- **Topics**
  - Framework Concepts & Organization
    - Calder-Moir / ISO 38500
  - Survey
    - Strategy: Balanced Scorecard
    - Risk & Compliance: COSO | COBIT | ISO 2700x | PCIDSS
    - Architecture & Plans: TOGAF | Zachman
    - Implement & Manage Change: PMBOK | PRINCE2 | COBIT
    - Verify: Balanced Scorecard, Zachman
    - Operate: ITIL | ISO 9000 | Six-Sigma

IT Infra-Structure Library (ITIL)

- Standardization of IT service delivery

- Derived from effort within British Government (1980’s) to standardize management of ‘services’
  - “service” is the means of delivery of value whereby customers get desired outcomes w/o having ownership of certain costs or risks
- Published as series of books dealing with different aspects of IT management
- Currently at Version 3
- Certification of organizations and practitioners

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in SF-ISACA’s 2011 CGEIT Preparation Class. No other use is permitted without express written authorization.
Service LifeCycle

- ITIL v3 organized around the concept of a service lifecycle

ITIL v3 Core Books
ITIL Guidance

- For each phase, defines:
  - Key Principles
  - Key Documents
  - Required processes
    - Targets (process outcomes | deliverables | metrics)
    - Roles and Responsibilities
    - Artifacts (policy | SOP | ‘documentation’)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Management processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Strategy</td>
<td>Strategy Generation</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td>Financial Management</td>
</tr>
<tr>
<td>Service Design</td>
<td>Service Catalog Management</td>
</tr>
<tr>
<td></td>
<td>Service Level Management</td>
</tr>
<tr>
<td></td>
<td>Supplier Management</td>
</tr>
<tr>
<td></td>
<td>Capacity Management</td>
</tr>
<tr>
<td></td>
<td>Info Security Management</td>
</tr>
<tr>
<td></td>
<td>Service Continuity Management</td>
</tr>
<tr>
<td>Service Transition</td>
<td>Release &amp; Deployment Management</td>
</tr>
<tr>
<td></td>
<td>Change Management</td>
</tr>
<tr>
<td></td>
<td>Knowledge Management</td>
</tr>
<tr>
<td></td>
<td>Asset &amp; Configuration Management</td>
</tr>
<tr>
<td></td>
<td>Service Validation &amp; Testing Management</td>
</tr>
<tr>
<td>Service Operation</td>
<td>Request Fulfillment</td>
</tr>
<tr>
<td></td>
<td>Access Management</td>
</tr>
<tr>
<td></td>
<td>Event Management</td>
</tr>
<tr>
<td></td>
<td>Functions (Service Desk Mgmt</td>
</tr>
<tr>
<td>CSI</td>
<td>7 Step Improvement</td>
</tr>
<tr>
<td></td>
<td>Service Reporting</td>
</tr>
</tbody>
</table>
ISO 900x

Standard for Quality Management Systems (QMS)

- Supports demonstration that a production process is ‘controlled’
  - Prevention of errors / fault
  - Assure quality to customers
- 3 Core Sections applicable to all areas
  - ISO 9000: QMS – Fundamentals and Vocabulary
  - ISO 9001: QMS – Requirements
    - Basis for ‘ISO 9000’ certification
  - ISO 9004: QMS – Guidelines for Performance Improvement

ISO 9003: QMS – Software Engineering

ISO 9000 Evolution: Emphasis on ‘Process’

http://www.praxiom.com/principles.htm

- ISO 9000: 2000 version emphasis on evidence of compliance with documented procedures
  - Tyranny of the ISO bureaucracy
- ISO 9000: 2004 version emphasis on process management
  - “documented system” vs. “system of documents”
  - Continual process improvement based on customer satisfaction
- ISO 9000: 2005
- ISO 9000: 2008 expands QMS to includes outsourced processes
ISO 9000 Generic Processes

- Management of resources
- Product Quality
- Maintenance of Quality Records
- Continual Improvement

ISO 9000 Best Practice Topics

http://tinyurl.com/cgeit-ISO9000

Eight QMS Principles:
- Correct implementation
- Customer focus
- Leadership
- Involvement of people, e.g.
  - People understanding the importance of their contribution and role in the organization.
  - People identifying constraints to their performance.
  - People accepting ownership of problems and their responsibility for solving them.
  - People evaluating their performance against their personal goals and objectives.
  - People actively seeking opportunities to enhance their competence, knowledge and experience.
  - People freely sharing knowledge and experience.
  - People openly discussing problems and issues
- Process approach
- Continual improvement
- Factual approach
- Supplier relationships
  - Mutual benefit
ISACA Resource: IT Governance Roundtables

governance challenges & trends; frameworks; value; staffing

Obtain from isaca.org ‘downloads’ page

Next Week:
VALUE MANAGEMENT