

# Foundations of IT Governance

## March 30, 2010

Bill Pankey  
Tunitas Group



2

## Notices

### Disclaimer

- No endorsement by ISACA International
- Materials have been developed by instructors
- No insider knowledge .... *No special access to CGEIT exam materials*

### ISACA's CGEIT Review Manual 2010

- Includes material not in CGEIT Primary References
- Organized by CGEIT task / knowledge statements
- Similar in quality and 'denseness' to CISA Study Guide
  - Requires multiple readings for complete comprehension

### Class wiki



3

## Required Knowledge\*

### Rationale for IT governance

- \* Define the requirements and objectives for, and drive the establishment of, IT governance in an enterprise.

### How IT governance is implemented

- \* Establish appropriate management governance structures
- \* Ensure that appropriate roles, responsibilities, accountabilities are established and enforced for information requirements, data and system ownership, IT processes, and benefits and value realization
- \* Ensure that an IT governance framework exists ...based on a comprehensive and repeatable IT process and control model .

### Barriers to implementing governance

- \* Continuously market, communicate and reinforce the need and value of IT governance across the enterprise



\* From CGEIT Job Practice (Frameworks domain)

4

## WHAT IS IT GOVERNANCE?




5

## Corporate Governance Defined

Procedures and processes according to which an organization is directed and controlled (OECD)

- The corporate governance structure specifies the distribution of rights and responsibilities among the different participants in the organization – such as the board, managers, shareholders and other stakeholders – and lays down the rules and procedures for decision-making.

Framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in the firm's relationship with its all stakeholders




6

## Governance is a Board Responsibility

**Principles of Corporate Governance: “responsibilities of boards” (OECD)**

- *Reviewing and guiding corporate strategy, major plans of action, risk policy*
  - **Strategic alignment**
  - **Risk management**} CGEIT domains
- *approving annual budgets and business plans; setting performance objectives*
  - **Resource management**
  - **Value delivery**} CGEIT domains
- *monitoring implementation and corporate performance*
  - **Performance measurement**} CGEIT domain



## IT governance implements Corporate Governance

Boards promulgate structures to exercise control over all aspects of a corporation

- Finance, personnel, strategic planning, ... IT

*So why would ...*

Effective IT governance require specialized treatment?

- High value but Intangible character of information assets
- Pervasiveness: infecting all aspects of the business
- Implementation cycles longer than typical business planning periods
- Highly technical aspects
- Ephemeral / indirect value of IT
- ... <exercise for candidates>

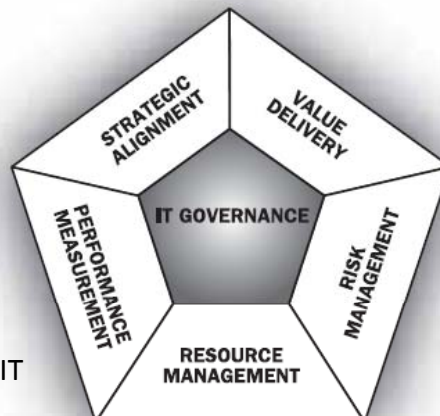


7

## ISACA's Answer: CGEIT Pentagon

- Provide strategic direction
- Ensure achieved objectives
- Appropriately manage risk
- Responsible resource use
- Recognize problems early

more than COBIT, ValIT, RiskIT



8

9

## Who drives IT governance?

IT governance in isolation risks being dysfunctional

1. Business planning cycles are shorter than technology implementation cycles
  - IT engineering must understand / accept / internalize the reality of changing business requirements.
    - Exemplar: Motorola's Iridium project
2. "IT service mentality" is inconsistent with ideas of the business' compliance with "IT" polices
  - IT may control the use of 'systems' but it cannot control the use of information contained within them.
3. .... <exercise for candidates>



10

## Something is wrong here!

"Governance processes are designed to help companies use limited resources wisely. However, several Fortune 500 CIOs recently told me that *business units* in their companies *have used the recession as an excuse to circumvent virtually all [IT] governance*. Projects have bypassed the executive steering committee, skipped the priority-setting process, and headed toward implementation with flimsy business cases and incomplete project plans. When IT protests, the business units claim that they needed to fast-track the projects in order to respond to competitive threats. In fact, they have ceded ground to their competitors by avoiding virtually all disciplines necessary for project success."

Bart Perkins, Dec 21, 2009, Computer World

*Resistance: Is IT governance the enemy of innovation?*



11

## WHAT IS THE RATIONALE FOR IT GOVERNANCE?



12

## Enron, WorldCom, Tyco ....GE ...

Fraudulent financial reporting in the late '90s focused regulatory attention on need for stronger corporate governance, accountability

- Sarbanes-Oxley
- Basel II

*Even good companies affected by weak or ineffective controls over financial reporting*



13

## Applied to IT?

Colossal IT failures lead to significant losses at otherwise successful companies

- Cedar Sinai (a hospital): decommissions \$70M CPOE application 1 day after mandating its use by all Cedar's practitioners.
- Green Giant (a frozen food processor): trucks 40 railroad car loads of fresh produce to land fill every day for a month due to failures to adequately implement SAP system
- Heartland (a bankcard transaction processor): \$30M+ in direct costs, significant loss of business and collapse of stock value due to single information security failure.

.... Name your 3 or 300 examples ... <exercise for candidates>

Pervasive IT failures indicate the need for greater control over IT investments and operations (?)



14

## Why is IT Governance Important?

*Stated in the negative*

Ineffective IT governance is a root cause for:

- Lost opportunities
- Damaged reputation
- Failure to meet deadlines, cost overruns, quality issues
- Negative impact on core processes due to poor quality IT services
- Failure of IT initiatives to bring innovation or promised benefits

Remains to be shown that specific governance program will avoid or correct



15

*however,*

## Governance must do more than “Prevent”

*Risk of overemphasis of loss prevention at the expense of value creation*

*Psychologically, losses are feared more than gains sought .... but vague or theoretical threats are easily discounted*


Goal of the firm is to **produce long term value for stakeholders**  
Create & maintain lasting competitive position

- Product innovation
- Customer relationships
- Operational efficiency

} Value disciplines

Control typically focused on loss prevention (avoiding the bad stuff)

- Cost reduction
- Risk mitigation



16

## Challenge of Value Creation

Value = quality / price

Effective IT governance proves itself by producing more business value from IT investments

- Same goods & services at lower price
  - cost reduction: resource management
- Higher quality goods & services
  - Customers / business define quality




17

Academic Research\*

## Benefits of Good IT Governance

- ☀ Greater return on assets & profitability
- Quicker to recognize new business opportunity
- Increased mission orientation: IT spending more focused on strategic objectives
- More accountability: IT decision making distributed to those responsible for outcomes
- Reduced IT cost

☀ Management efficiency: Better use of limited executive bandwidth

 Serving IT Governance Professionals  
San Francisco Chapter      \*MIT Center for Information Systems Research

18

## ISACA's Broad View of IT Governance\*


IT Governance's dual focus

- performance / results
  - Financial and non-financial
  - Current and future
- risk management
  - Asset preservation
  - Regulatory compliance

vs. say, COSO (& SOX) focus on risk management

- Integrity of financial statements
- Compliance with laws / regulation

\* IT Governance Institute

 Serving IT Governance Professionals  
San Francisco Chapter

19

## Goals of IT Governance (short answer)

**Put in place the structure & mechanisms to ensure that the enterprise:**

1. Makes the right IT investments in the right way (i.e., gets value)
2. Uses information 'responsibly' (i.e., manages risk)



20

## Anticipated by-Products IT Governance

### Value maximization

- Inventory of IT aspects that are strategic to the enterprise
- An opportunistic IT strategy
- Assurance of proper execution of the IT strategy
- Assurance that costs of non-strategic IT activities are minimized

### Risk minimization

- Assurance that information risks appropriately managed



## ISACA: What is IT Governance (1)

*Governance Requirements justify*

### **Formal mechanism for stakeholder control over IT**

- Defined by its accomplishments:
  - Receipt of appropriate value from IT
    - Making the 'right' IT investments
      - "Alignment"
      - "Value Delivery"
    - Maximizing the business benefit from those investments
      - "Performance measurement"
      - "Resource management"
  - Prevention of IT misuse
    - Avoid damage to company assets or reputation
      - "Risk management"



## ISACA: What is IT Governance? (2)

*Governance Requirements justify*

### **Special case of enterprise governance applied to information and IT**

- *Arrangement between governing body and management that provides the structure through which:*
  - Overall objectives are set
    - "strategic alignment"
  - Means of obtaining the objectives are outlined
    - "resource management"
    - "risk management"
    - "value delivery"
  - Performance monitoring is described
    - "performance management"



23

## HOW IS IT GOVERNANCE IMPLEMENTED?



24

## Components of IT Governance

- Critical decisions
- Actors & Decision structures
- Alignment Processes
- Risk Management Processes
- Communication
- Feedback
- Best Practices



25

## Caveat

Few absolutes | no 'one size fits all'

Many factors determine what governance mechanism will be effective for a given firm, e.g.:

- Company size and business complexity
- Value discipline
  - Product innovation
  - Customer intimacy
  - Operational excellence
- Technology maturity
- Company maturity {workforce, customers, business model, etc}
- Profit | not for profit | government
- Company's IT history

ISACA understates the importance of company factors

e.g. No segregation of RACI charts for governance factors. Perhaps more prescriptive than is warranted



26

## The Critical Decisions

### **IT Principles (IT strategy)**

- How IT will be used to accomplish business objectives?

### **IT Architecture**

- How will data, applications and infrastructure be organized to support desired level of business and technical standardization?

### **IT Infrastructure**

- What shared IT capability is required to support the business?

### **Business Application Needs**

- What are the IT investments needed to directly generate business value? How should the need for innovation be balanced with standardization requirements?

### **Investment Priorities**

- How to align investment portfolio with strategic priorities?



27

## The Critical Decisions & CGEIT Domains

**Performance Measurement**

**IT Principles (IT strategy)**

- How IT will be used to accomplish business objectives?

**Alignment**

**Architecture**

- How will data, applications and infrastructure be organized to support desired level of business and technical standardization?

**Resource Management**

**Infrastructure**

- What shared IT capability is required to support the business?

**Business Application Needs**

- What are the IT investments needed to directly generate value?

**Value Delivery**

**Investment Priorities**

- How to align investment portfolio with strategic priorities?

**ISACA**  
Serving IT Governance Professionals  
San Francisco Chapter

28

## 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
  - Support the business with appropriate information & IT related services

**ISACA**  
Serving IT Governance Professionals  
San Francisco Chapter

29

## Decision Structures

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



30

## Decision Structures (aka, patterns, archetypes)\*

| Pattern           | Input & Decision Rights  |
|-------------------|--|
| Business Monarchy | Group of senior business executives (CXO) acting individually or in committees. Precludes IT executives acting independently |
| IT Monarchy       | Group of IT executives acting independently or in committees   |
| Feudal            | Business units leaders or key process owners   |
| Federal           | Sr. Executives and business unit leaders  process owners and possibly IT executives.   |
| IT Duopoly        | IT executives and one other group (business unit leader, process owner, or Sr. executives)                                   |
| Anarchy           | Each individual user   |

\* Wiell & Ross, IT Governance




31

## Patterns applied to Critical Decisions

A Profile characterizes the firm's IT governance

|                   | Principles |          | Architecture |          | Infrastructure |          | Application |          | Priorities |          |
|-------------------|------------|----------|--------------|----------|----------------|----------|-------------|----------|------------|----------|
|                   | Input      | Decision | Input        | Decision | Input          | Decision | Input       | Decision | Input      | Decision |
| Business Monarchy |            | x        |              |          | x              |          |             |          |            | x        |
| IT Monarchy       |            |          | x            | x        | x              | x        |             |          |            |          |
| Feudal            |            | x        | x            |          |                |          | x           |          |            |          |
| Federal           | x          |          |              |          |                |          |             | x        | x          |          |
| IT Duopoly        |            |          |              |          |                |          |             |          |            |          |
| Anarchy           |            |          |              |          |                |          |             |          |            |          |




32

## Academic Research:\*

### Characteristics of the Best | Worst Governance

Significant positive (+) & negative (0) correlation with governance quality

|                   | Principles |          | Architecture |          | Infrastructure |          | Application |          | Priorities |          |
|-------------------|------------|----------|--------------|----------|----------------|----------|-------------|----------|------------|----------|
|                   | Input      | Decision | Input        | Decision | Input          | Decision | Input       | Decision | Input      | Decision |
| Business Monarchy |            |          |              |          |                |          |             |          |            |          |
| IT Monarchy       |            |          |              |          |                |          |             |          |            |          |
| Feudal            |            |          |              |          |                |          |             | 0        |            |          |
| Federal           | +          | 0        |              | 0        |                | 0        | +           |          |            | 0        |
| IT Duopoly        | 0          | +        |              |          |                |          | 0           |          |            | +        |
| Anarchy           |            |          |              |          |                |          |             |          |            |          |



\*MIT Center for Information Systems Research

33


## 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 |          |
|-------------------|------------|----------|--------------|----------|----------------|----------|-------------|----------|------------|----------|
|                   | Decision   | Decision | Decision     | Decision | Decision       | Decision | Decision    | Decision | Decision   | Decision |
| Business Monarchy | Profit     | Growth   | Profit       | Profit   | Profit         | Profit   | Growth      | Profit   | Growth     | Profit   |
| IT Monarchy       |            |          |              |          | Profit         |          |             |          |            |          |
| Feudal            |            |          |              |          |                |          |             |          | Growth     |          |
| Federal           |            |          |              |          |                |          | Profit      |          |            |          |
| IT Duopoly        | ROA        |          | ROA          |          | ROA            |          | ROA         |          | ROA        | ROA      |
| Anarchy           |            |          |              |          |                |          |             |          |            |          |

Most common patterns for all firms



\*MIT Center for Information Systems Research


34

## “Board Briefing”:

### ISACA Identified Structures

Business dominance | profit oriented

|  | Principles |          | Architecture |          | Infrastructure |          | Application |          | Priorities |          |
|--|------------|----------|--------------|----------|----------------|----------|-------------|----------|------------|----------|
|  | Input      | Decision | Input        | Decision | Input          | Decision | Input       | Decision | Input      | Decision |
| IT Strategy Committee<br>(Business Monarchy)   |            | x        |              |          |                |          |             |          |            |          |
| IT Steering Committee<br>(Business Monarchy)   |            |          |              | x        |                | x        |             | x        |            | x        |
| Technology Council<br>(IT Monarchy)            |            |          | x            |          | x              |          | x           |          |            |          |
| IT Architectural Review<br>Board (IT Monarchy) |            |          | x            |          | x              |          |             |          |            |          |




35

## Board Briefing:\*

### ISACA Identified Structures

| Committees recommended by ISACA           |            |              |                |             |            |
|---|------------|--------------|----------------|-------------|------------|
|   | Principles | Architecture | Infrastructure | Application | Priorities |
|   | Input      | Decision     | Input          | Decision    | Input      |
| IT Strategy Committee (Business Monarchy) | X          |              |                |             |            |
| IT Steering Committee                     |            |              |                |             |            |
| Technology Council                        |            |              |                |             |            |
| IT Architectural Review Board             |            |              |                |             |            |




\*MIT Center for Information Systems Research

36

## Alignment Processes

- IT investment approval process
  - Ensure that IT investments generate significant return relative to other investment
- Architectural exception processes
  - Support for learning about unique business needs
- Service level agreements
  - Articulate available IT services, costs & alternatives. Product of business & IT negotiation
- Chargeback
  - Gives business units visibility into costs of shared infrastructure
- Project tracking
  - Alert executives to potential problems in execution
- Formal tracking of business value
  - Support for learning about the value of IT enabled initiatives



37

## Risk Management Processes\*

- Internal control environment
- Event identification
- Risk assessment
- Risk response
- Risk communication
- Control activities
- Monitoring



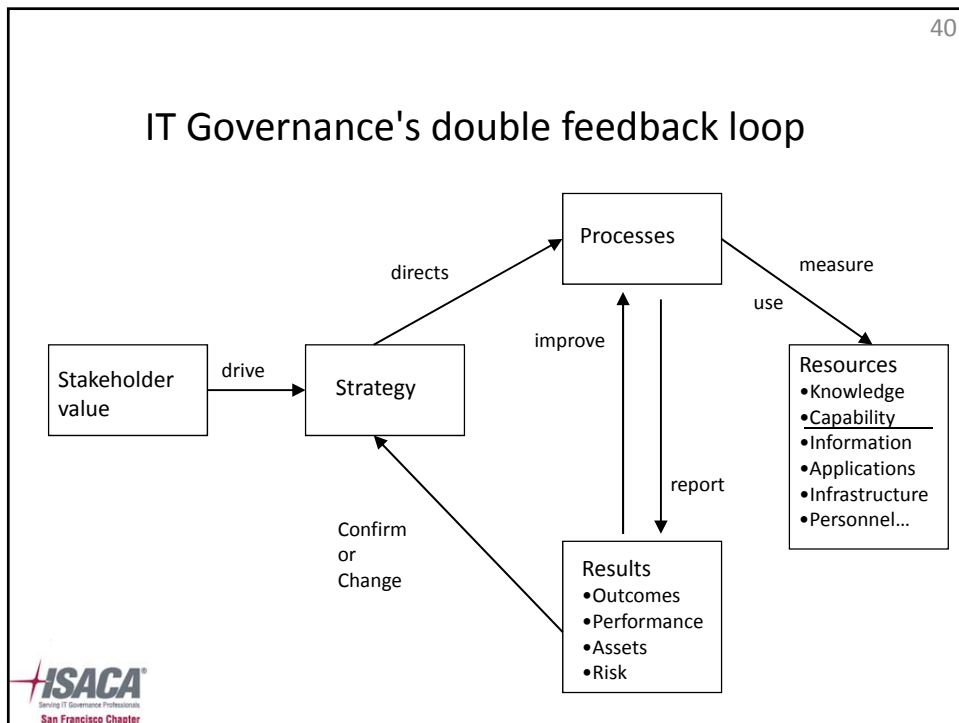
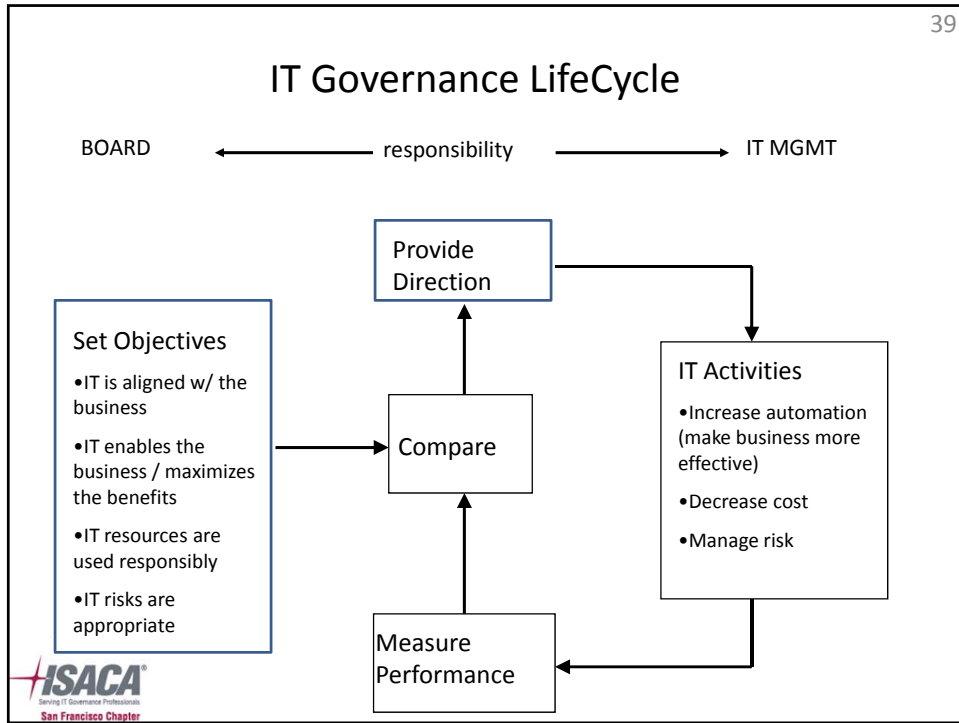
\* COSO ERM (enterprise risk management)

38

## Communication

- Senior management announcements
  - Clarify priorities | demonstrate commitment
- Policy Statements
  - Defines the 'control environment'
- Scorecards
  - Typically tied to compensation; incent behaviors and goals
- Formal committees
  - Make lower level decisions | carry out higher level ones
- Office of CIO or IT governance
  - Advocacy, ownership and 'organizational home'
- Working w/ nonconformists
  - Personal visits to inform or persuade | "architectural social workers rather than architectural police"
- Intranet Portals
  - Educate workforce around IT governance process





## Best Practice

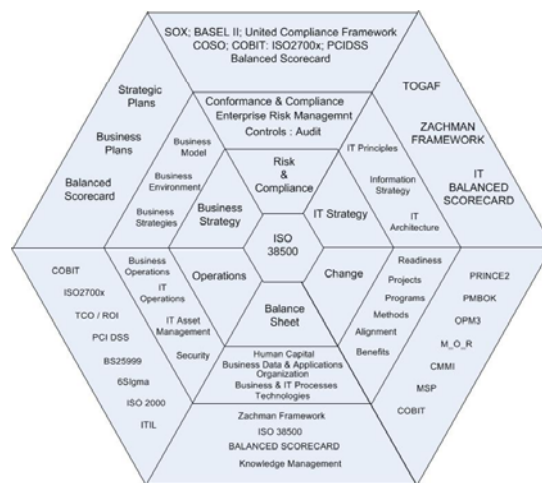
At practice level, successful companies will adopt industry leading IT management practices

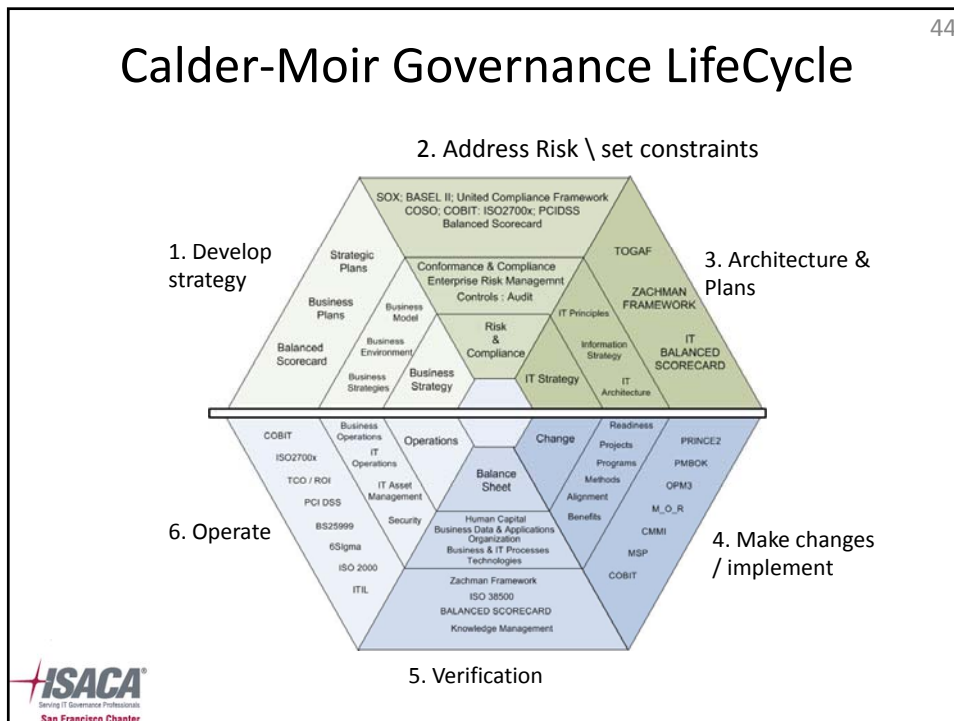
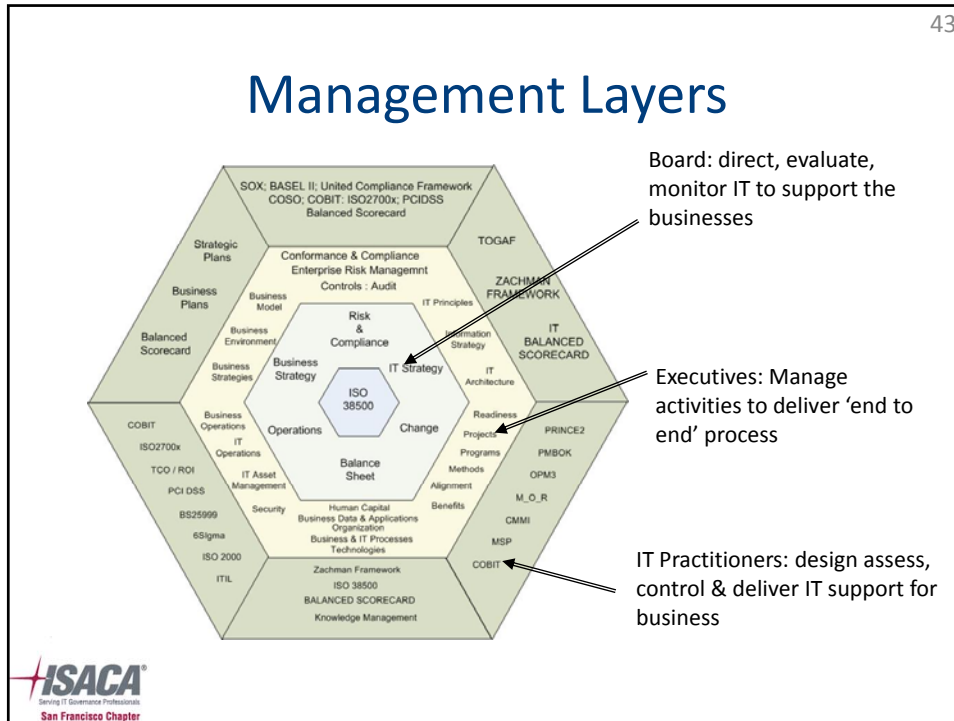
- Utilize best practice frameworks for:
  - Architecture
  - Service management
  - Project planning
  - Information security management
  - System Development
- ...
- COBIT and other IT frameworks cross referenced to such best practice

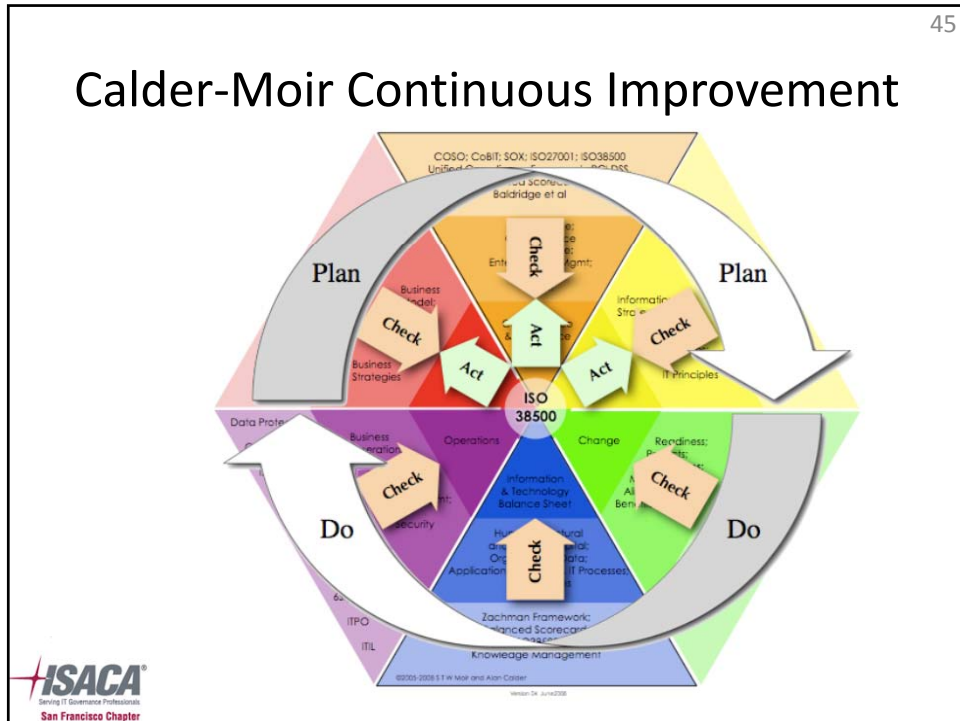
Calder-Moir (ISO 38500) organizes IT lifecycles with explicit references to numerous best practice frameworks



## Calder-Moir Framework of Frameworks ISO 38500







46

## Final Questions

# NEXT WEEK: STRATEGIC ALIGNMENT

ISACA  
Serving IT Governance Professionals  
San Francisco Chapter