IT Governance Deep Dive

Steve Romero, IT Governance

Romero Consulting

Consulting

Governance, Risk & Compliance – G21/G22

Governance defined

gov·er·nance noun (ˈgə-vər-nən(t)s)

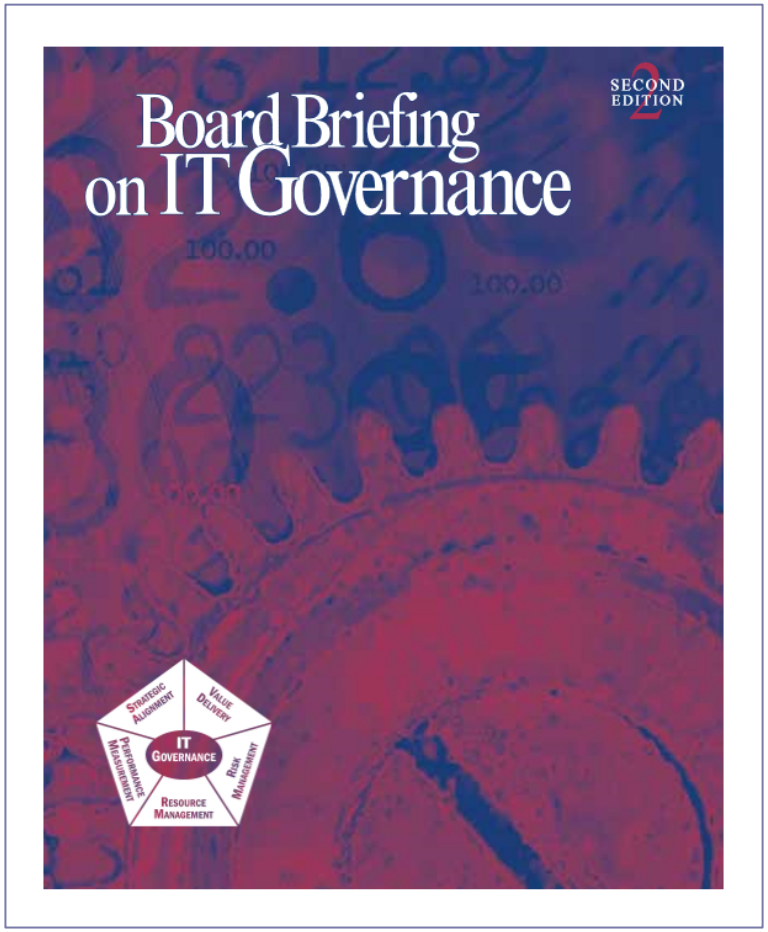
: the way that a city, company, etc., is controlled by the people who run it

Corporate governance defined

The structure and the relationships which determine corporate direction and performance.

- The board of directors is typically central to corporate governance – accountable to shareholders
- Participants include: management, employees, customers, suppliers, and creditors
- Depends on the legal, regulatory, and culture of the community

ITGI – First IT governance guidance



IT Governance defined

~1998~ "The responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives."

IT Governance – more definitions

"The system by which the current and future use of IT is directed and controlled. Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization."

Today's ITGI Definition: "A governance system enables multiple stakeholders in an enterprise to have an organised say in evaluating conditions and options, setting direction and monitoring performance against enterprise objectives. Setting and maintaining the appropriate governance approach is the responsibility of the board of directors or equivalent body."

IT Governance – even more definitions

"The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals."

"A decision-making framework for IT investments that is designed to maximize the return of benefits while managing risk to acceptable levels."

IT Governance – another definition

"Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives."

IT Governance definition

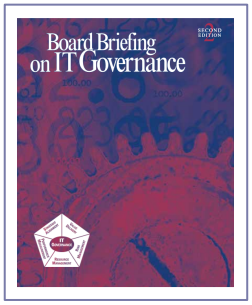
Depends who you ask, or, when you asked

ITGI


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

Comprehensive approach to IT governance

~1998~

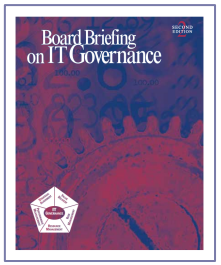


IT governance concepts

Useful as a reference booklet or as a tool for educating top management, and comes complete with checklists and tools to help management initiate and sustain an effective IT governance program.

Table of Contents

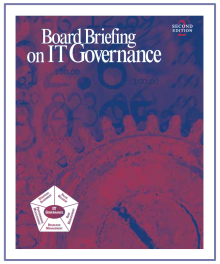
IT Governance Principles



The principles of ITG – according to ITGI, 1998

- Ensure IT is aligned with the business – focus on aligning with the business and collaborative solutions
- Ensure IT delivers value to the business – concentrating on optimizing expenses and proving the value of IT
- Ensure IT risk is managed – addressing the safeguard of IT assets, disaster recovery and continuity of operations
- Ensure IT resources are managed – realizing the optimal investment in, and proper management of, critical IT resources
- Ensure IT performance is managed – tracking and monitoring strategy implementation, project success, resource usage, process performance and service delivery

ITG Principle Definitions



- Strategic alignment — Achieving the goals and strategies of an enterprise through the coherent undertaking of activities by the different governance structures or management levels within an enterprise. A culture of business and IT partnership should be developed, supported by IT's interest in and understanding of the business, and sharing of technology-related issues and opportunities.
- Value delivery — Creating new value for the enterprise through IT, maintaining and increasing value derived from existing IT investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. The basic principles of IT value are delivery of fit-for-purpose services and solutions on time and within budget, and generating the financial and non-financial benefits that were intended.
- Risk management — IT risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT risk consists of IT-related events that could potentially impact the business. While value delivery focuses on the creation of value, risk management focuses on the preservation of value.
- Resource management — Ensuring that the right capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource management ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. It recognizes the importance of people, in addition to hardware and software, and, therefore, focuses on providing training, promoting retention and ensuring competence of key IT personnel.
- Performance measurement — Tracking the achievement of the objectives of the enterprise's IT-related services and solutions and compliance with specific external requirements. Without establishing and monitoring performance measures, it is unlikely that the previous focus areas will achieve their desired outcomes. It provides a link back to the other focus areas by monitoring that the required direction is being followed and creates the opportunity to take timely corrective measures, if needed.

ITGI - IT Governance Framework

Provide Direction

Set Objectives

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT-related risks are managed appropriately

Compare

IT Activities

- Increase automation (make the business effective)
- Decrease cost (make the enterprise efficient)
- Manage risks (security, reliability and compliance

Measure Performance

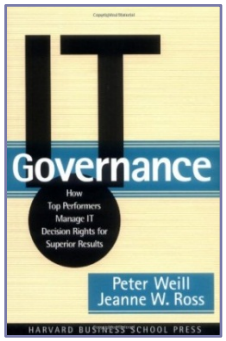
MIT CISR


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

MIT CISR view of IT governance

Massachusetts Institute of Technology Center for Information Research, Sloan School of Management

- MIT CISR has been asking and answering the same question for 38 years: How do enterprises realize the most value from their investment in technology?
- Peter Weill, Chairman of MIT CISR: "If I was to choose one factor that most contributed to the success of IT, it is IT Governance."
- Firms with superior IT Governance had more than 20% higher profits over those that did not
- "Specifying the decision rights and accountability framework to encourage desirable behavior in using IT."

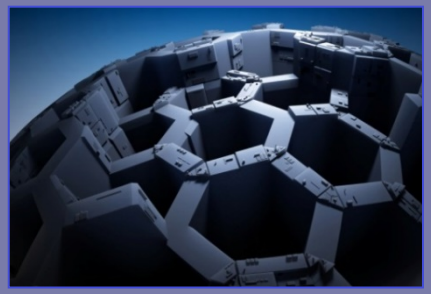


2004

Every organization addresses five key IT governance decisions

IT Principles for Digitization Decisions
Clarifying the Role for IT

Enterprise Architecture Decisions



IT Infrastructure Decisions

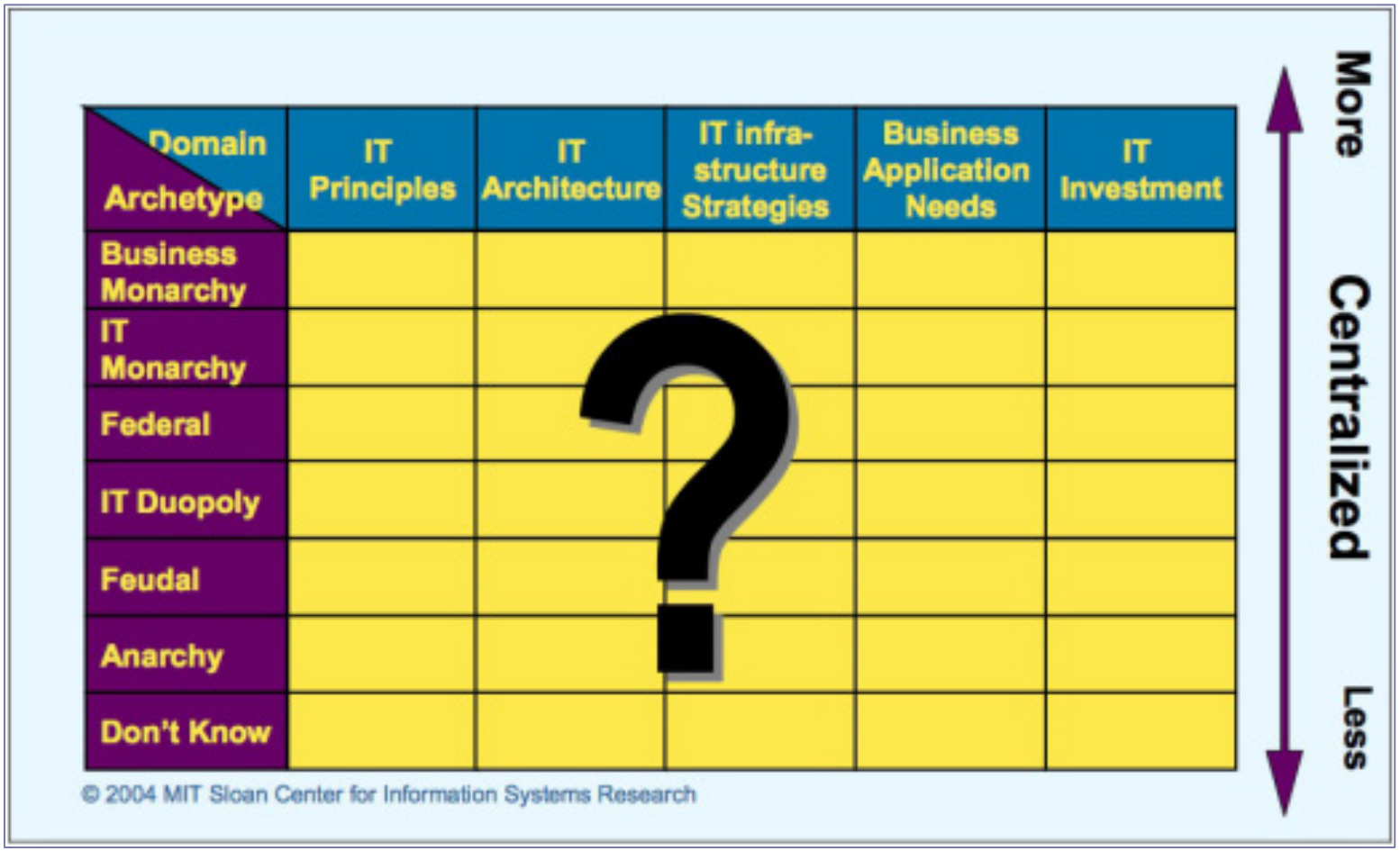
Business Application Decisions

IT Investment and Prioritization Decisions

IT governance archetypes

- Business monarchy — the most centralized approach — a senior business executive or a group of senior executives, sometimes including the CIO, makes all the IT-related decisions for the enterprise.
- IT monarchy — decisions are made by an individual IT executive or a group of IT executives.
- Federal system — C-level executives and business representatives of all the operating groups collaborate with the IT department. This is equivalent to the central government and the states working together.
- IT duopoly — a two-party decision-making approach involves IT executives and a group of business leaders representing the operating units.
- Feudal system — business unit or process leaders make separate decisions on the basis of the unit or process needs.
- Anarchy — the most decentralized system, in which each individual user or small group pursues his, her or their own IT agenda.

IT governance on one page

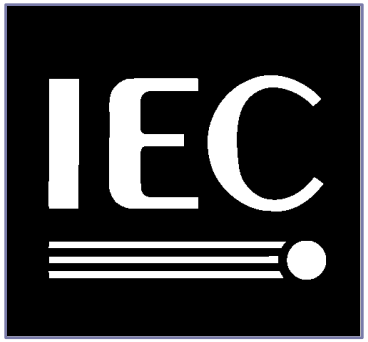


ISO IT Governance Standard

The ISO/IEC IT Governance Standard

ISO/IEC 38500 ~2008~

A high level, principles based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of IT.

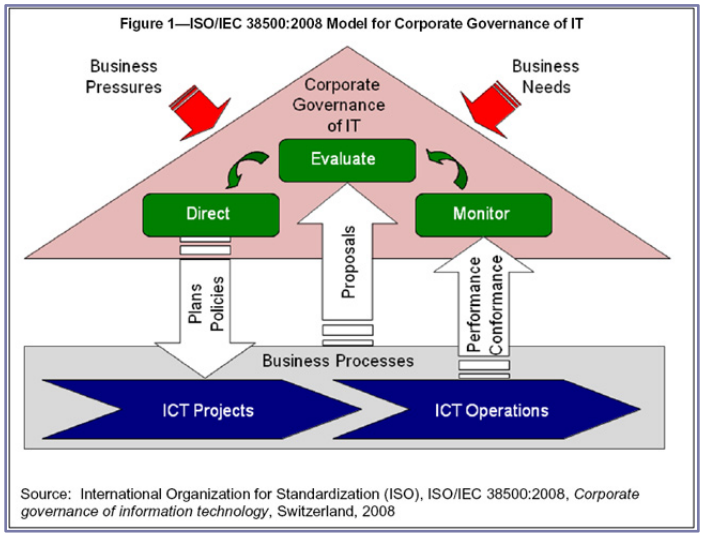


ISO/IEC IT governance definition

ISO 38500 definition: The system by which the current and future use of IT is directed and controlled. Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization.

The objective of ISO/IEC 38500

The objective of their standard is to provide a framework of principles for Directors to use when evaluating, directing and monitoring the use of information technology (IT) in their organizations.



The 'other' ISO/IEC objectives

- Proper corporate governance of IT may assist directors in assuring conformance with obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of IT.
- Inadequate IT systems can expose the directors to the risk of not complying with legislation. For example, in some jurisdictions, directors could be held personally accountable if an inadequate accounting system results in tax not being paid.

A standard rooted in risk aversion

Processes dealing with IT incorporate specific risks must be appropriately addressed. For example, directors could be held accountable for breaches of:

- security standards
- privacy legislation
- spam legislation
- trade practices legislation
- intellectual property rights
- record keeping requirements
- environmental legislation and regulations
- health and safety legislation
- accessibility legislation
- social responsibility standards

ISO/IEC 38500 principles

- Responsibility – Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
- Strategy – The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.
- Acquisition – IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

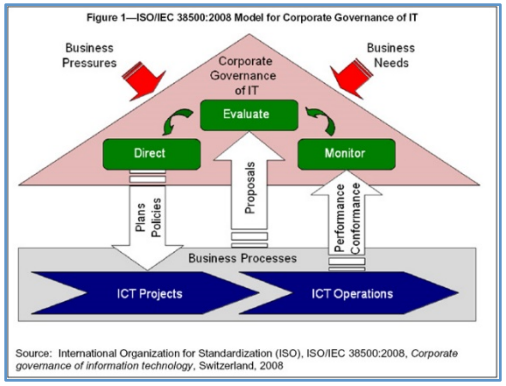
ISO/IEC 38500 principles

- Performance – IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.
- Conformance – IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
- Human Behavior – IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the 'people in the process'.

ISO/IEC 38500 Governance Model

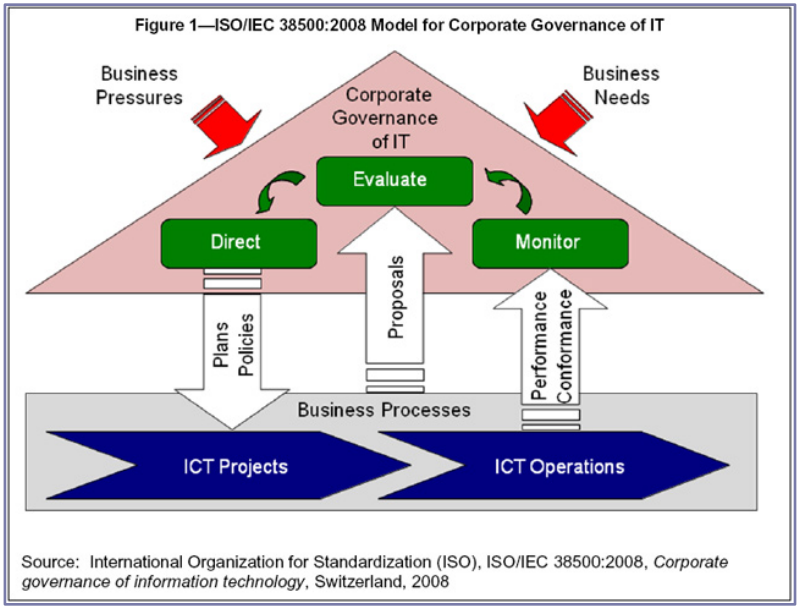
IT is governed through 3 main tasks

- 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



The governance and management "distinction"

"In ISO's view, governance is distinct from management, and for the avoidance of confusion, the two concepts are clearly defined in their standard."



COBIT ®


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

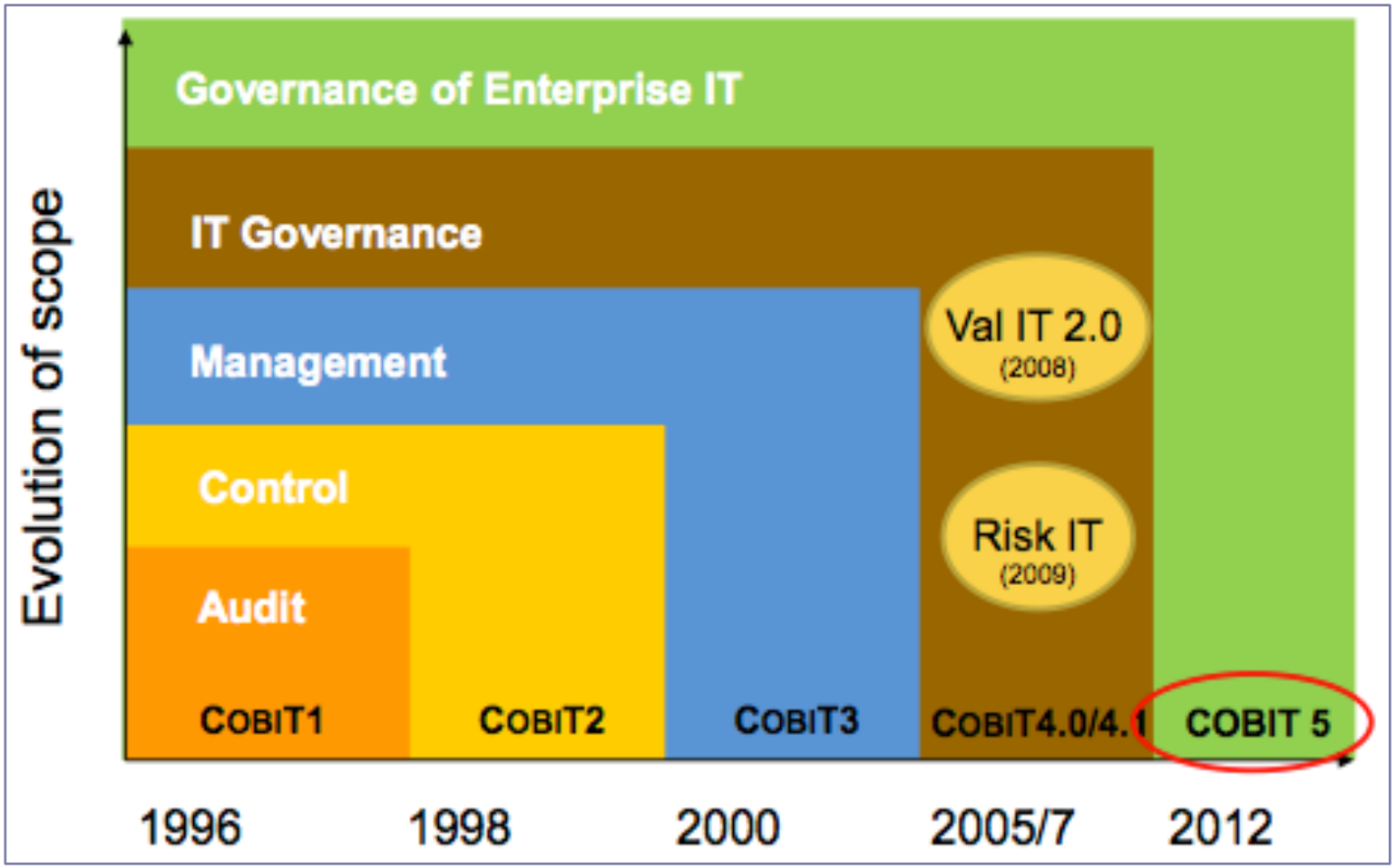
COBIT® 2012

~~Control Objectives for Information and Related Technology~~

What is COBIT®5?

- COBIT®5 is a foundational enterprise IT Governance framework, providing a basis to effectively integrate other complimentary frameworks, standards, and practices.
- As a single overarching framework it serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic, common language.

The evolution of COBIT®



What is the scope of COBIT®5?

- COBIT®5 addresses the governance and management of information and related technology from an enterprise-wide, end-to-end perspective, including the activities and responsibilities of both the IT function and non-IT business functions.
- The end-to-end aspect is further supported by COBIT®5 coverage of all critical business elements, e.g. processes, organizational structures, principles & policies, culture, skills, information, service capabilities.

IT governance according to COBIT®

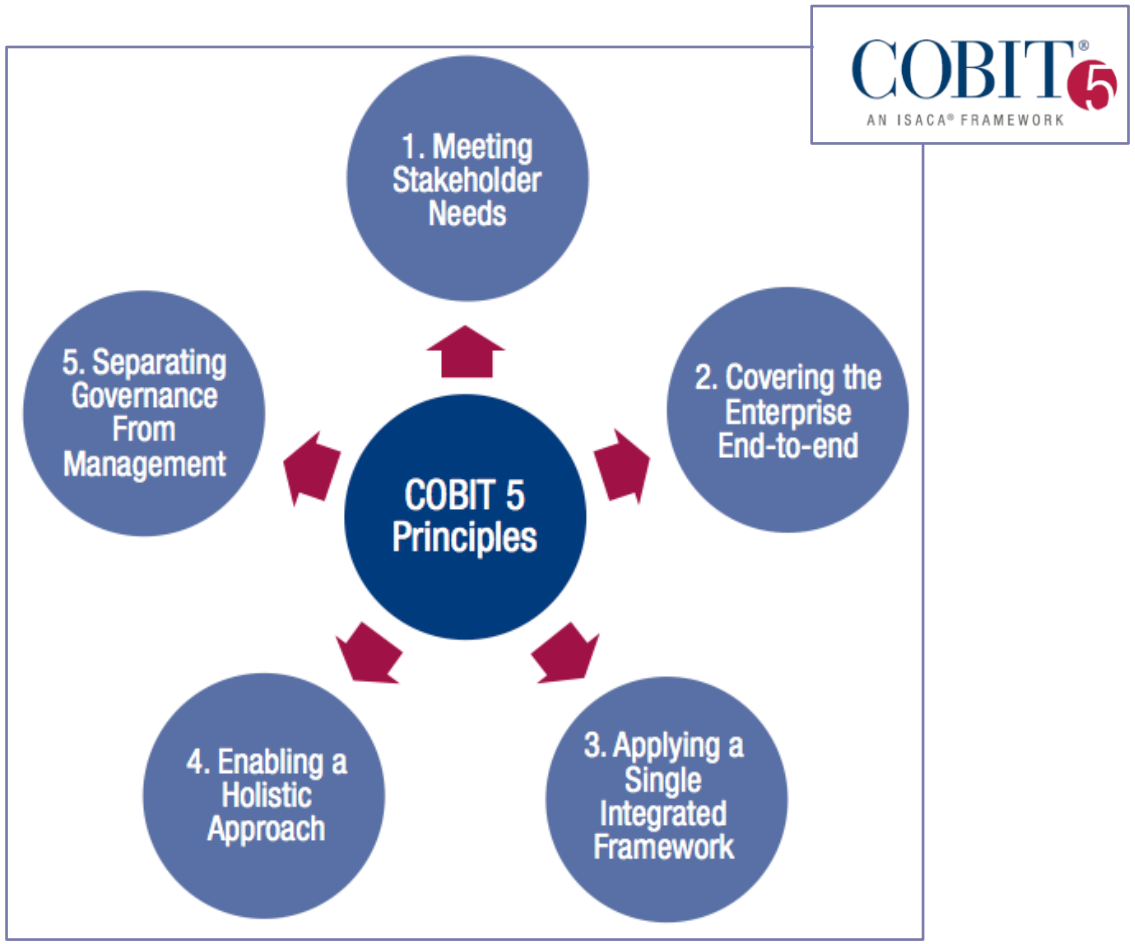
Governance

- Ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions, and options
- Sets direction through prioritization and decision making
- Monitors performance, compliance, and progress against the agreed upon direction and objectives

Management

- Plans, builds, runs, & monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives

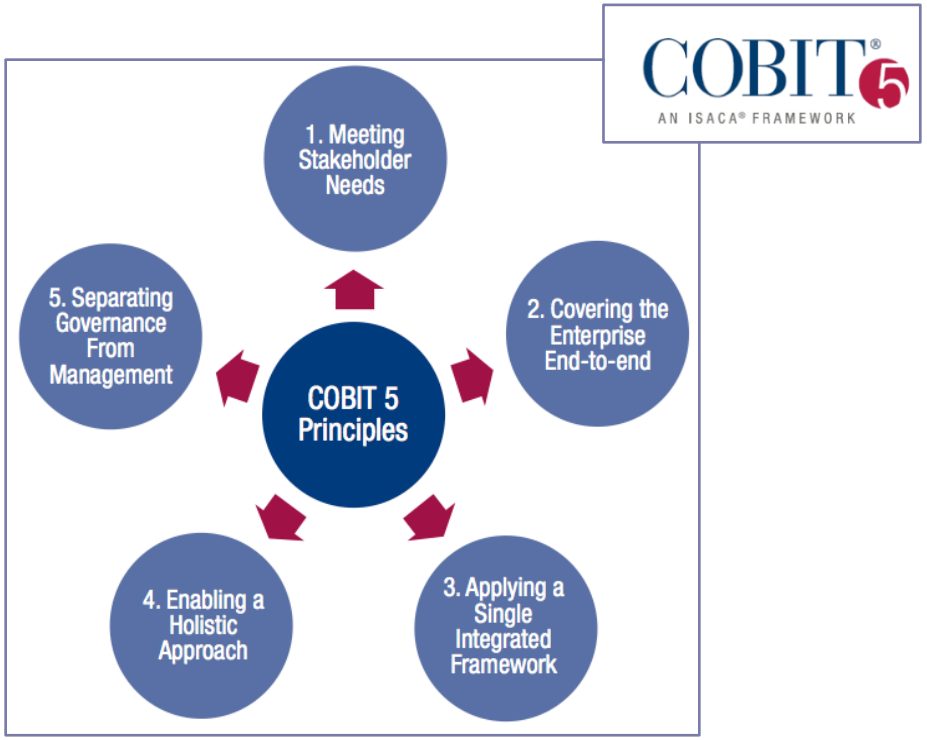
COBIT®5 (GEIT) principles



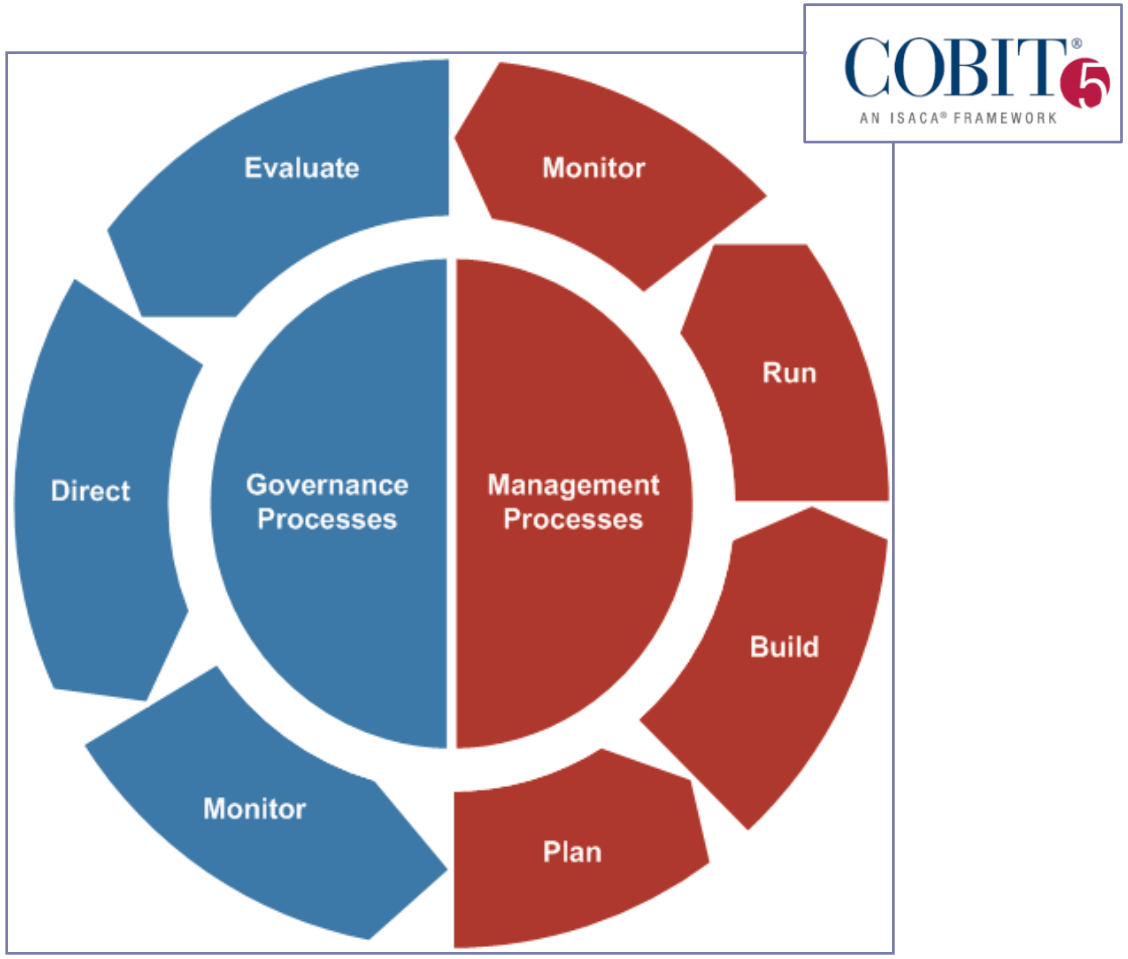
Dissimilar IT governance principles

ISO 38500

- Responsibility
- Strategy
- Acquisition
- Performance
- Conformance
- Human Behavior



Governance & management processes

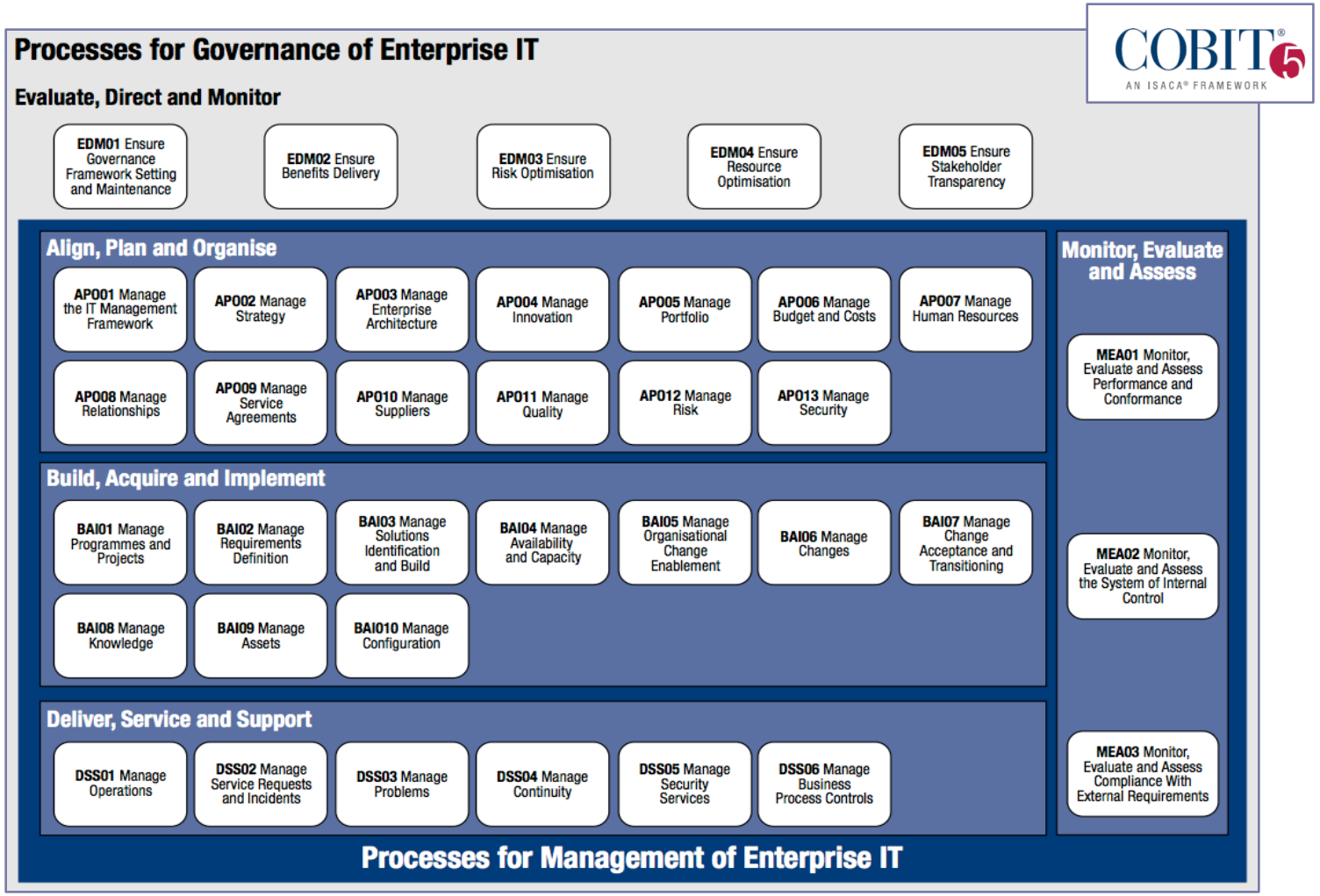


Principle 5: Separating gov & mgt

Process reference model: Divides governance and management processes into two primary domains:

- Governance (1 Domain, 5 Processes)
  - Within each process, evaluate, direct, and monitor practices are defined.
- Management (4 Domains, 32 Processes)
  - In line with responsibility areas of plan, build, run, and monitor, provide an end-to-end coverage of IT Management.

COBIT® Process reference model



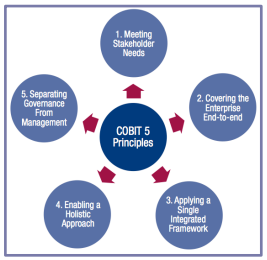
COBIT Governance Processes

Governance Domain – evaluate, direct, and monitor

- EDM01: Ensure governance framework setting and maintenance
- EDM02: Ensure benefits delivery
- EDM03: Ensure risk optimization
- EDM04: Ensure resource optimization
- EDM05: Ensure stakeholder transparency

Goals Cascade

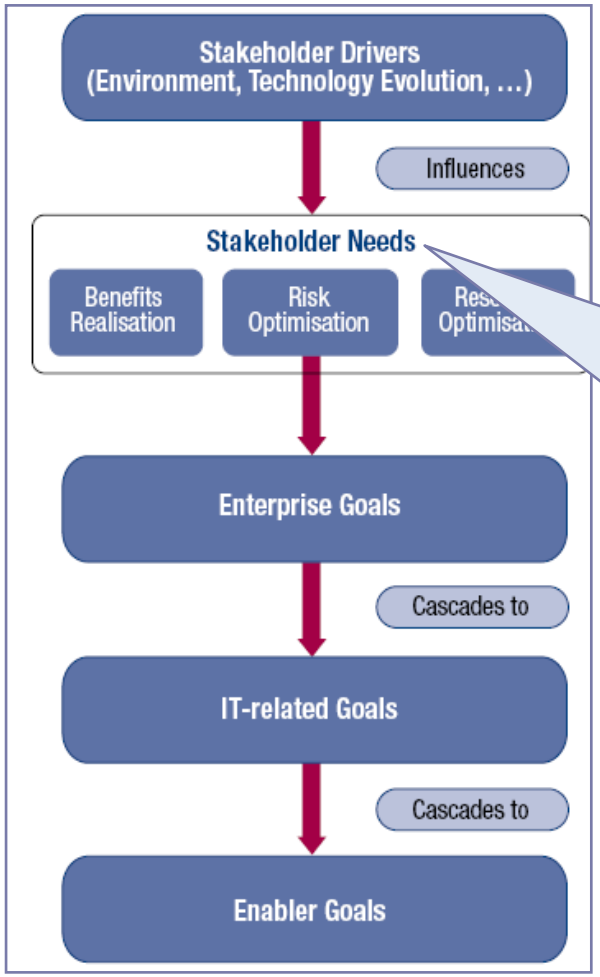
(Principle 1: Meeting stakeholder needs)



Governance Domain – evaluate, direct, and monitor

1. EDM01: Ensure governance framework setting and maintenance
2. EDM02: Ensure benefits delivery
3. EDM03: Ensure risk optimization
4. EDM04: Ensure resource optimization
5. EDM05: Ensure stakeholder transparency

Goals Cascade and ISO ITG principles



ISO 38500

- Responsibility
- Strategy
- Acquisition
- Performance
- Conformance
- Human Behavior

COBIT 5
AN ISACA® FRAMEWORK

Principle 1: Meeting stakeholder needs

Internal Stakeholders	Internal Stakeholder Questions
• Board • CEO • Chief financial officer (CFO) • CIO • Chief risk officer (CRO) • Business executives • Business process owners • Business managers • Risk managers • Security managers • Service managers • Human resource (HR) managers • Internal audit • Privacy officers • IT users • IT managers • Etc.	• How do I get value from the use of IT? Are end users satisfied with the quality of the IT service? • How do I manage performance of IT? • How can I best exploit new technology for new strategic opportunities? • How do I best build and structure my IT department? • How dependent am I on external providers? How well are IT outsourcing agreements being managed? How do I obtain assurance over external providers? • What are the (control) requirements for information? • Did I address all IT-related risk? • Am I running an efficient and resilient IT operation? • How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner? What are the most effective and efficient sourcing options? • Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance? • How do I get assurance over IT? • Is the information I am processing well secured? • How do I improve business agility through a more flexible IT environment? • Do IT projects fail to deliver what they promised—and if so, why? Is IT standing in the way of executing the business strategy? • How critical is IT to sustaining the enterprise? What do I do if IT is not available? • What concrete vital primary business processes are dependent on IT, and what are the requirements of business processes? • What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget? • How much of the IT effort goes to fighting fires rather than to enabling business improvements? • Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives? • How long does it take to make major IT decisions? • Are the total IT effort and investments transparent? • Does IT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?
External Stakeholders	**External Stakeholder Questions**
• Business partners • Suppliers • Shareholders • Regulators/government • External users • Customers • Standardisation organisations • External auditors • Consultants • Etc.	• How do I know my business partner's operations are secure and reliable? • How do I know the enterprise is compliant with applicable rules and regulations? • How do I know the enterprise is maintaining an effective system of internal control? • Do business partners have the information chain between them under control?

The State of IT Governance

That was then. Then is now.

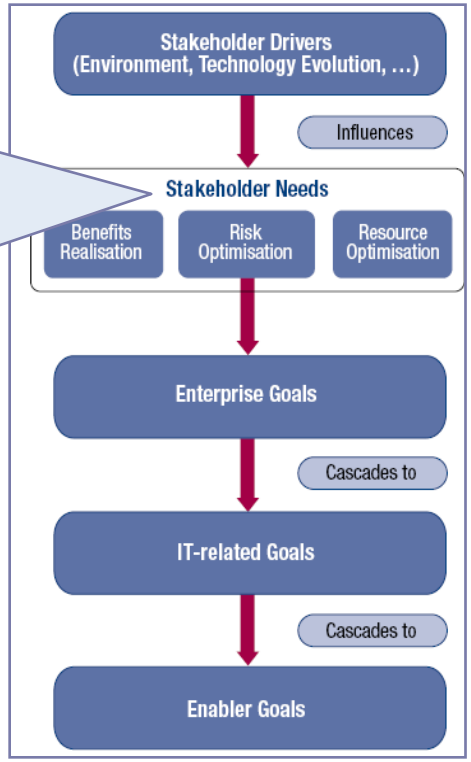
1998

- Ensure IT is aligned with the business
- Ensure IT delivers value to the business
- Ensure IT risk is managed
- Ensure IT resources are managed
- Ensure IT performance is managed

2008

- Responsibility
- Strategy
- Acquisition
- Performance
- Conformance
- Human Behavior

2012



Latest "Status of GEIT"

Based on a 2012 survey of 3700 ISACA members

- More than half of responding enterprises use a governance framework.
- 25% of respondents said management's level of involvement in governance is low.
- Nearly 50% said management involvement was "moderate."

ITG and the BoD

A Company's Board of Directors is responsible for IT governance

- IT matters are discussed predominantly on an ad hoc basis at the board level.

According to the ITGI 2009 Survey of 255 Non-IT Executives

- Forty-eight percent of directors of larger companies spent more than 10% of last year's total annual board hours discussing IT risks and opportunities, compared to 34% of directors of smaller companies.

Source: PwC's Annual Corporate Directors Survey - 2013

ITG and the BoD

Primary responsibility for IT oversight	2012	2013
The full board	25%	26%
The audit committee	56%	54%
A separate risk committee	7%	7%
A separate IT committee	2%	3%
Other	2%	3%
No board oversight	8%	6%

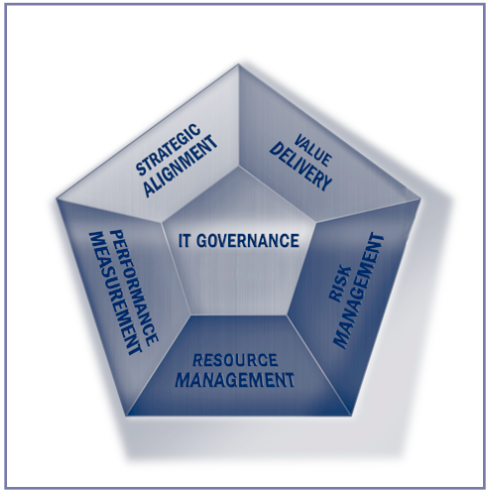
Obstacles to IT Governance

- Widely misunderstood
- Managers don't like to be governed
- Negative connotation and pervasive negative opinion
- Past IT governance failures
- Lack of process and process management proficiency (resulting in bureaucracy, increased cycle-time and costs, over-process vs. optimized process)
- Philosophically and intellectually vs. business-case driven
- Not business-sponsored or driven

What drives IT governance?

Increased IT Governance Awareness

- Audit Influence
  - ISACA/IT Governance Institute
  - Audit Issues
- Risk and Compliance
  - Regulatory Requirements
  - Legal Requirements
  - Security Requirements
- Investment Decision-making - PPM
  - IT-Business Alignment
  - IT Accountability to the Business



ITG is a function of the BoD

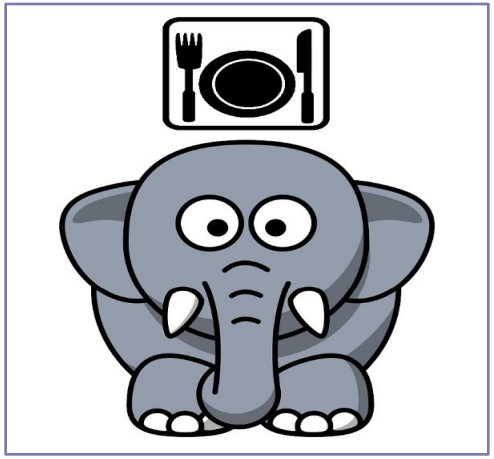
The Board is responsible for ensuring…

- IT is aligned with business strategy
- IT brings value to the business
- IT manages risk
- IT manages resources
- IT manages performance

How many boards are driving or even participating in the adoption and execution of IT governance frameworks?

Can you imagine the board using ISO38500? COBIT®5?

Great challenges to sustaining IT governance



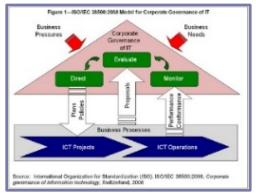
The Radical View

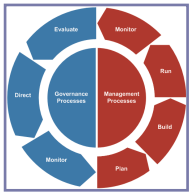
Introduction to the Radical View

The governance to management "distinction"

In ISO's and COBIT's view, governance is distinct from management, and for the avoidance of confusion, the two concepts are clearly defined in their standard/framework.

- …but governance is not separate from management
- Managers govern - evaluate, plan, organize, staff, direct, monitor, and control
- And governors may have some managing to do...when their monitoring exposes variances, gaps, deviations, and failures





The governance “vs.” management barrier

Governance is “distinct” from management, but not separate

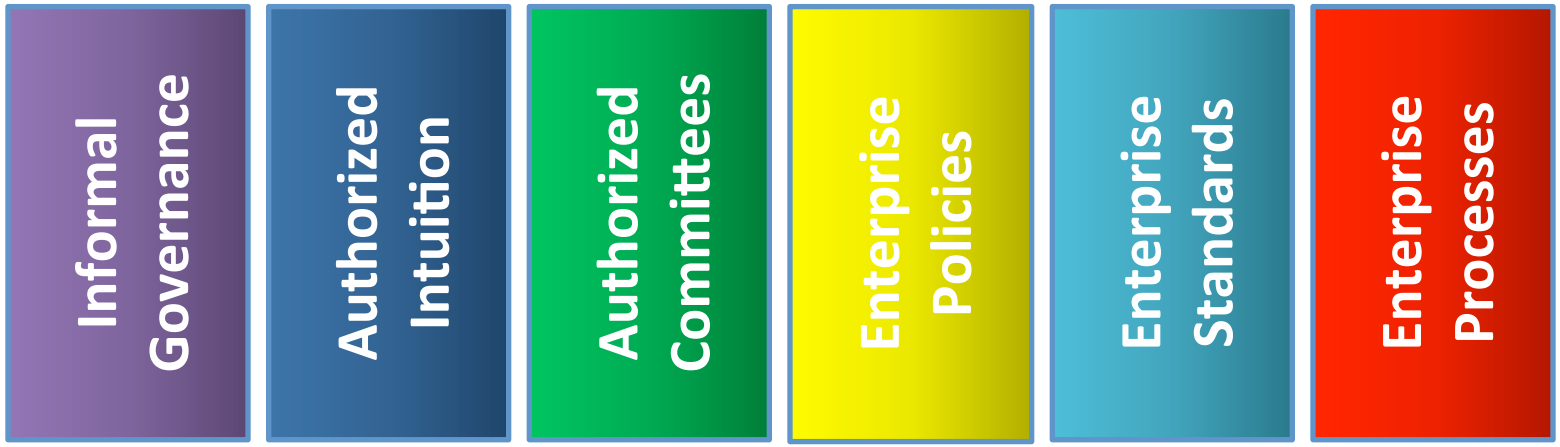
- Though necessary in understanding the terms, I argue distinguishing between governance and management is dangerous – potentially fostering “us and them”
- From the perspective of the ‘us’ manages, the governors are placed in the position of ‘them’ – and vice versa
- If governance is “distinct from management” then it is potentially viewed as an ‘add-on’ – an ‘extra step’ – a ‘roadblock’ – between “us and them”

Every decision is "governed"

Many organizations mistakenly believe, "We don't have IT governance."

- This view fails to recognize the omnipresence of governance – something is governing all decisions, it is simply a matter of whether those "governance mechanisms" are formally defined and managed
- Formal governance – laws, regulations, rules, boards, committees, policies, standards, processes, data (metrics), "authorized intuition"
- Informal governance – culture, beliefs, values, ethics, attitude, emotion, genetics, data (metrics), etc.

The IT Governance Spectrum



Every organization has governance

- The fact is, all managers (and all decisions) are 'governed' – even when there are no "governors"
- The purpose of governance is to enable and ensure reasoned and rational decision-making…
- …so formal governance mechanisms are only necessary when informal governance mechanisms don't enable and ensure reasoned and rational decision-making

Integration of governance and management

- Distinction between governance and management is often misunderstood 
- Effective integration of these two elements is critical for successful IT governance in any enterprise or organization
- IT governance is NOT responsible for “rendering” IT infrastructure
- IT governance IS responsible for “oversight of the management processes” that render IT infrastructure

Governance defined

"Governance is the system by which organizations are directed and controlled. It is essentially about leadership and involves overseeing the preparation of plans, overseeing the delivery of business change, overseeing operations, and overseeing the realization of benefits."

Basil Wood, New Zealand @bazpractice

IT governance simplified

The processes and relationships that lead to reasoned decision-making in the use of information technology

3 Key Questions:

- What information technology decisions need to be formally governed?
- Who will be assigned accountability for governing those decisions?
- How will those decisions be governed?
  - committees
  - policy / standard
  - process
  - "authorized intuition"

Governance accountability – roles

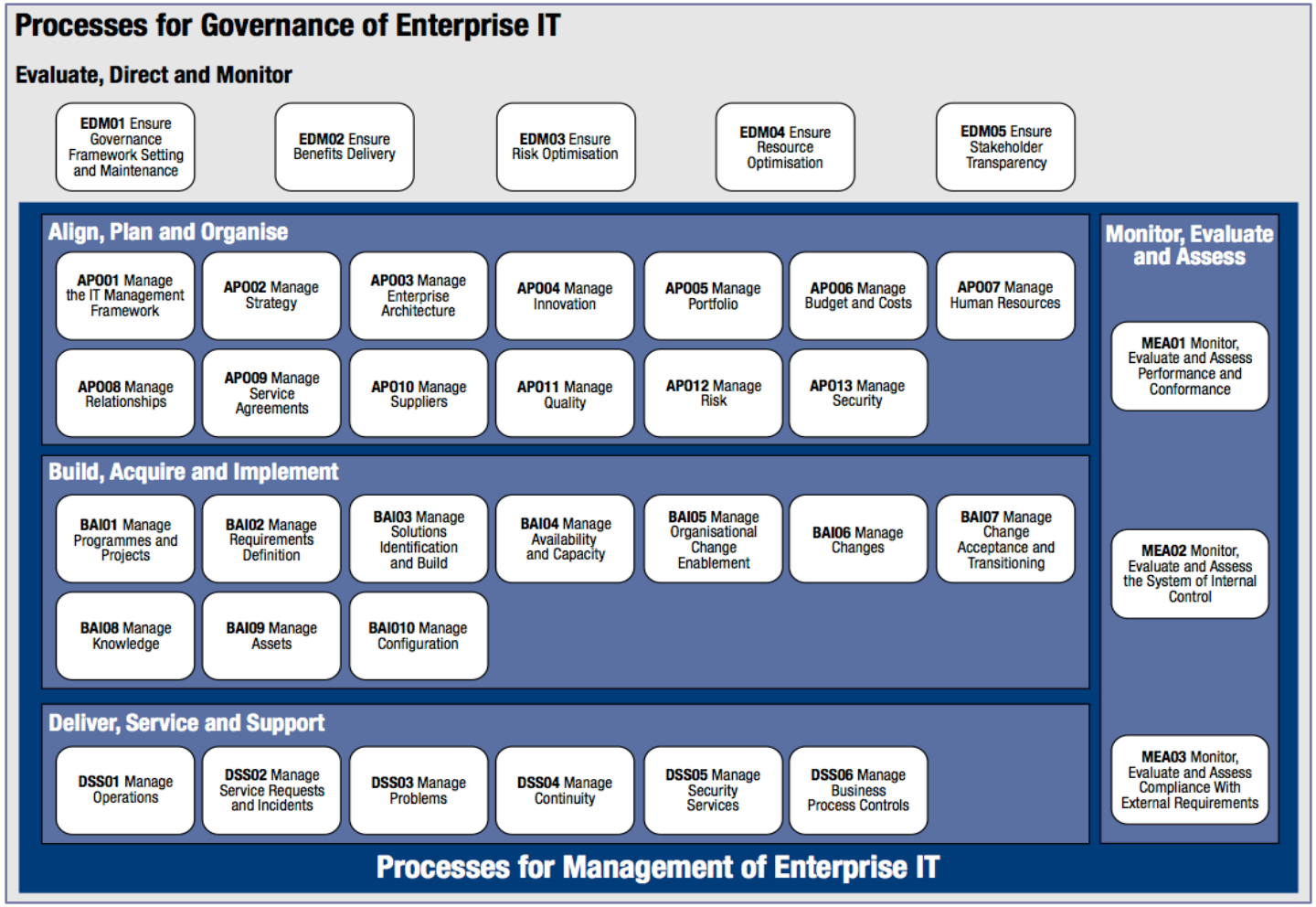
Examples of Decision-making Bodies

- Executive or Senior Management Committee
- IT Leadership Committee comprising IT Executives
- IT Project and Portfolio Management Committee
- IT Policies & Standards Committee
- Architecture Committee
- Process Teams and Owners
- Business IT Relationship Managers
- IT Council comprising Business and IT Executives
- External service management committee

Integration of governance and management

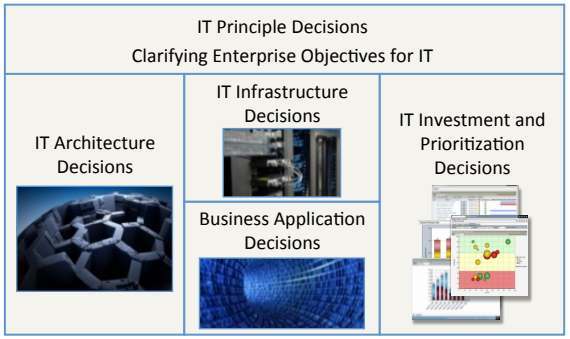
- Distinction between governance and management is often misunderstood
- Effective integration of these two elements is critical for successful IT governance in any enterprise or organization
- IT governance is NOT responsible for “rendering” IT infrastructure
- IT governance IS responsible for “oversight of the “management processes” that render IT infrastructure

COBIT® Process reference model



ITG decisions are enabled by ITG processes

- Integrated Business & IT Planning
- Architecture Management - Standards & Review
- IT Investment Assessment, Prioritization, Funding & Benefits Realization Accountability (PPM)
- IT Financial & Resource Allocation
- Project Execution & Decision-making
- Emerging Technology Evaluation & Adoption
- Client Relationship Management
- Building & Maintaining Applications & Infrastructure
- Provisioning of IT Services
- Strategic Sourcing Services
- Audit & Risk Management



The other half of the Weill and Ross IT governance mechanisms

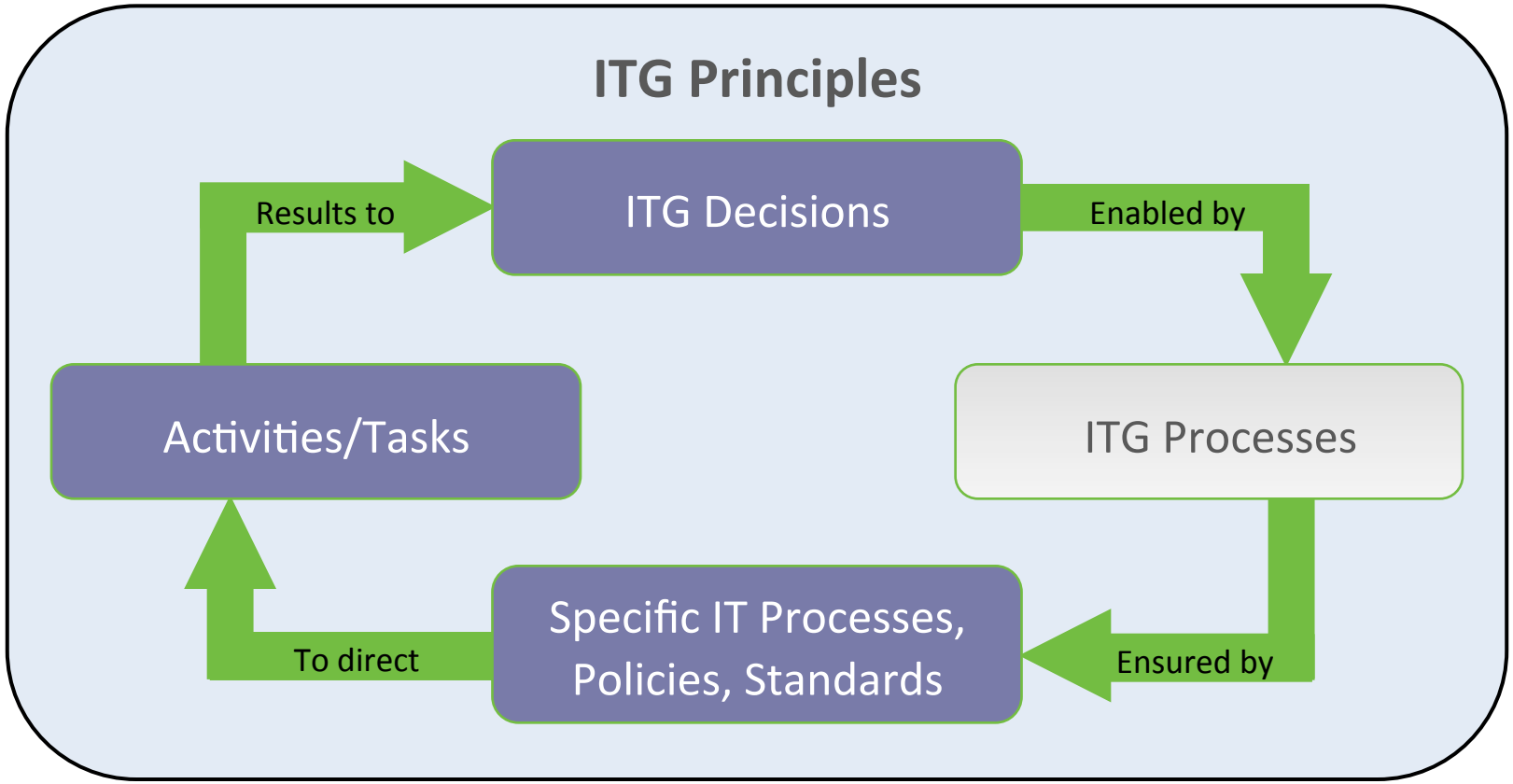
IT governance is a function of the business

The business is accountable for ensuring the principles of IT governance

- Ensure IT is aligned with the business
- Ensure IT delivers value to the business
- Ensure IT risk is managed
- Ensure IT resources are managed
- Ensure IT performance is managed

Why ITG?

To enable IT to support business strategy



Connection between business strategy and personnel action to realize the principles of IT Governance

Deep Dive

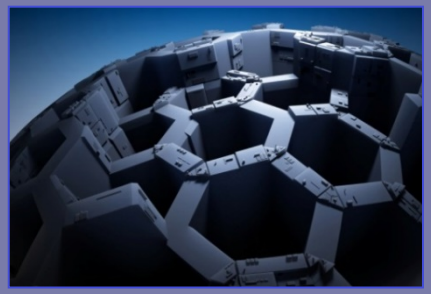

ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

IT Governance Decisions

Every organization addresses five key IT governance decisions

IT Principles for Digitization Decisions
Clarifying the Role for IT

Enterprise Architecture Decisions



IT Infrastructure Decisions

Business Application Decisions

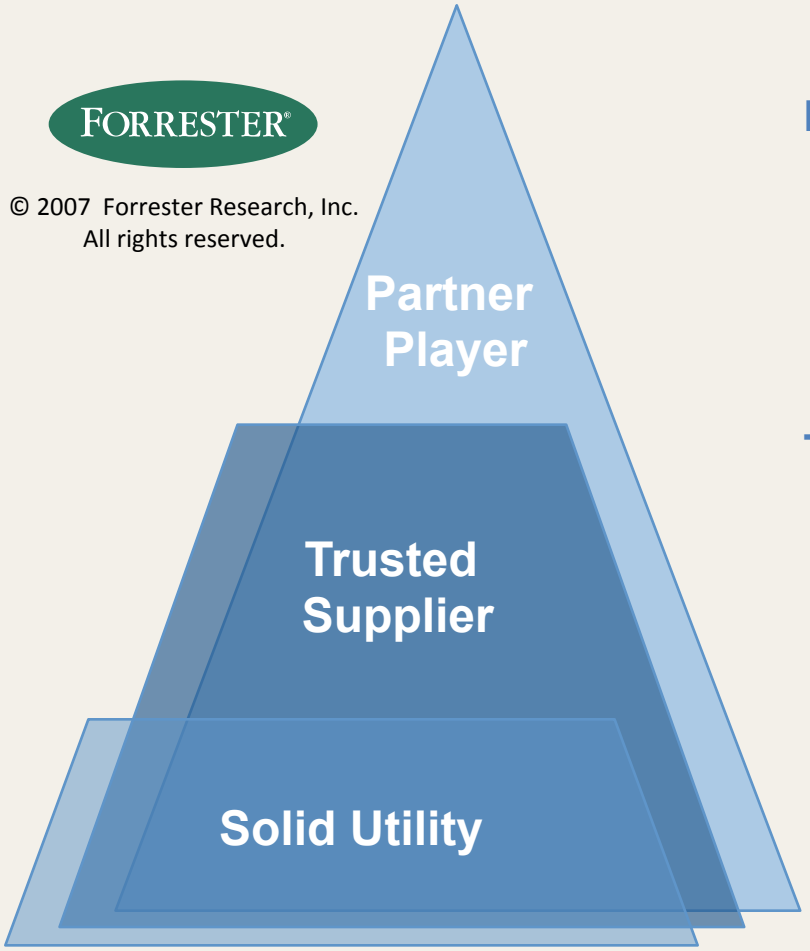
IT Investment and Prioritization Decisions

IT governance decisions

IT Principles for Digitization - clarifying the role of IT in the business – basis for defining IT Archetype

- Based on the Business Principles of the enterprise – business drives IT
- Driven by Business' expectations and industry sector constraints
- Developed by IT and business leadership
- A related set of high-level statements about how IT is used in the business
- IT Principles provide clarity and focus for the IT enterprise, establishing the direction for all other decisions

IT Archetypes



Partner Player

IT organizations expected to create unique and competitive solutions with customers, suppliers, and internal users — plus, being a Trusted Supplier.

Trusted Supplier

IT organizations expected to deliver app projects on time and on budget, based on operating units' requirements and priorities — plus, being a Solid Utility.

Solid Utility

IT organizations expected to provide cost-effective, dial-tone reliability with transparent, constantly declining costs.

Approximately one-third of companies are in each of the archetypes according to the Forrester State Of IT Governance In North American And European Enterprises Report © 2008, Forrester Research, Inc. All rights reserved.

IT governance decisions

Enterprise Architecture – the organizing logic for business process and IT infrastructure

- Reflects the integration and standardization requirements of a company's operating model
- Provides long-term view of processes, systems and technologies – used to build capabilities
- Captured in policies, relationships and technical choices
- Provides technical and data standardization and defines where shared infrastructure ends and applications begin
- Supports current and future application needs – fostering innovation

IT governance decisions

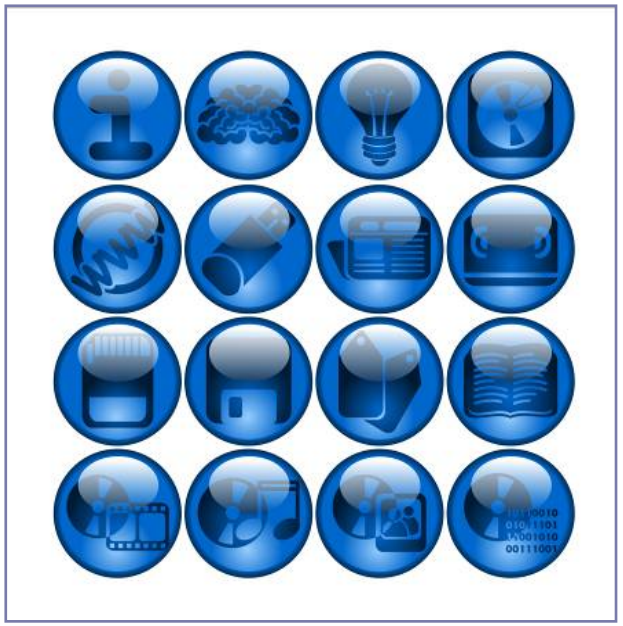
IT Infrastructure Strategies - determining shared and enabling services

- Foundation of planned IT capability
- Shared and reliable services used by multiple applications
- Includes infrastructure applications
- All communications pass through a security and risk capability
- Enables rapid implementation of future business initiatives

IT governance decisions

Fulfilling business needs - Determining shared and enabling services

- Fundamentally improve business processes
- Enables operating efficiency
- Balance of creativity and discipline
- Willingness to sacrifice functionality for architectural integrity
- Contributes to strategic value



IT governance decisions

IT Investment and Prioritization - Choosing which initiatives to fund and determining how much to spend

- How much do we spend?
- What do we spend it on?
- How do we reconcile the needs of different constituencies?
- Requires business-led and IT-enabled Portfolio Management
- Ensures IT spending reflects strategic priorities

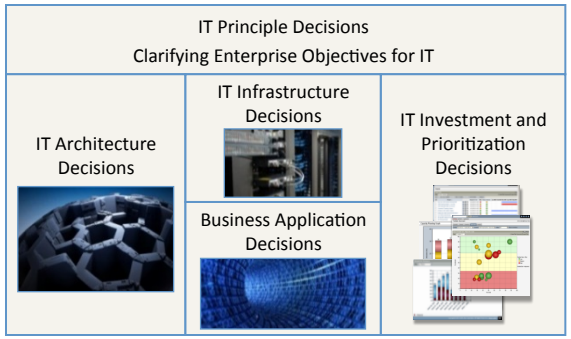
Key issues for each IT decision

Decision	Key Issues
IT Principles	• How do the business principles translate to IT principles that guide IT decision making? • What is the role of IT in the business? • What are desirable IT behaviors • How will IT be funded?
IT Architecture	• What are the core business processes of the enterprise? How are they related? • What information drives these core processes? How must this data be integrated • What technical capabilities should be standardized enterprise-wide to support IT efficiencies and facilitate process standardization and integration? • What activities must be standardized enterprise-wide to support data integration? • What technology choices will guide the enterprise's approach to IT initiatives?
IT Infrastructure	• What infrastructure services are most critical to achieving the enterprise's strategic objectives? • What infrastructure services should be implemented enterprise-wide and what are the service-level requirements for those services? • How should infrastructure services be priced? • What is the plan for keeping underlying technologies up-to-date? • What infrastructure services should be outsourced?
Business Application Needs	• What are the market and business process opportunities for ne business applications? • How are strategic experiments designed to assess success? • How can business needs be addressed within architectural standards? When does a business need justify an exception to a standard? • Who will own the outcomes of each project and institute organizational changes to ensure the value?
IT Investment and Prioritization	• What process changes or enhancements are strategically most important to the enterprise? • What is the distribution in the current IT portfolio? Is this portfolio consistent with the enterprise's strategic objectives? • What is the relative importance of enterprise-wide versus business unit investments? Do actual investment practices reflect their relative importance? • How is the business value of IT projects determined following their implementation?

IT Governance Processes

ITG decisions are enabled by ITG processes

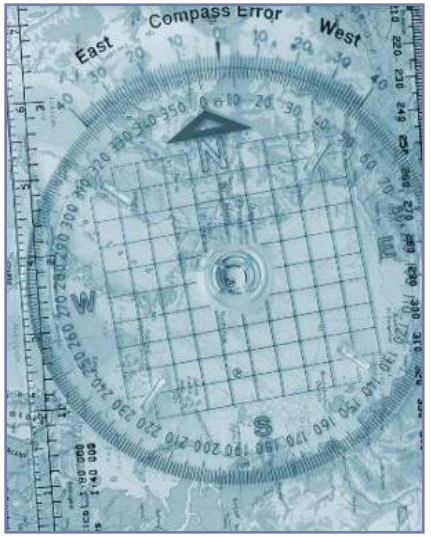
- Integrated Business & IT Planning
- Architecture Management - Standards & Review
- IT Investment Assessment, Prioritization, Funding & Benefits Realization Accountability (PPM)
- IT Financial & Resource Allocation
- Project Execution & Decision-making
- Emerging Technology Evaluation & Adoption
- Client Relationship Management
- Building & Maintaining Applications & Infrastructure
- Provisioning of IT Services
- Strategic Sourcing Services
- Audit & Risk Management



IT governance processes

Integrated Business and IT Planning

- IT Strategy “embedded” in business strategy
- IT Strategic Plan based on Business Strategic Plan
- IT Tactical Plans based on IT Strategic Plan
- IT Operational Plans based on IT Tactical Plan



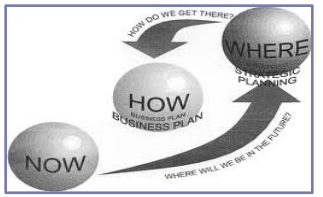
IT governance processes

Architecture Management

- Architecture Committee
- Defined architecture
- Policies, standards, relationships and technical choices
- Enabling future capability – fostering innovation

IT governance processes

IT Investment Assessment, Prioritization, Funding & Benefits Realization Accountability (PPM)



- Demand Management
- Portfolio Management
  - Project, Demand, Resource, Asset, Application, Service
- Governance or Steering Committee
- PMO Supported

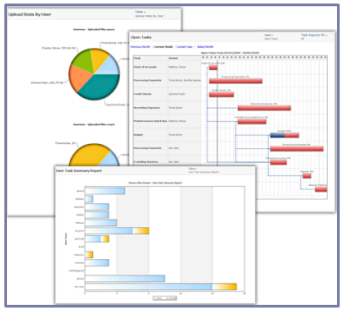
IT governance processes

IT Financial and Resource Allocation

- Financial Services for IT
- Financial plans
- Budgets and forecasts
- Cost accounting
- Cost modeling and benchmarking
- Chargeback
- Resource management

IT governance processes

Project Execution and Decision-making



- Project Management
- Fact-based decision-making
- Scenarios and what-if analysis
- Monitoring, speeding, slowing, stopping, trade-offs and killing projects
- Empowered PMO - Project management best practices and center of excellence

IT governance processes

Emerging Technology Evaluation and Adoption

- Enable enterprise innovation
- Research and development
- Market side – not just supply side
- Linked to business strategy
- Hand-in-hand with enterprise architecture
- Almost half of business respondents report their enterprises have implemented or are planning initiatives to promote IT innovation.

According to the ITGI Global Status Report of Governance of Enterprise IT 2011 Survey of 834 Business Executives and heads of IT

IT governance processes

Client Relationship Management

- Advocate for business and IT
- Acute understanding of business needs
- Acute understanding of IT capability
- Facilitate communication and collaboration
- Speed and improve decisions
- Improve requirements processes
- Ensure value and performance

IT governance processes

- Building & Maintaining Applications & Infrastructure
- Provisioning
  - SDLC – CMMI – Testing – Q&A
  - ITIL Service Lifecycle
  - Provisioning of IT Services
  - ITIL Service Lifecycle

Strategy to Operation

Service Strategy
- Demand Mgt.
- Service Portfolio Mgt.

Service Operation
- Event Mgt.
- Incident Mgt.
- Problem Mgt.
- Request Fulfilment

Service Design
- SLM
- Service Catalogue
- Capacity Mgt.

Service Transition
- Change Mgt.
- Service Asset Mgt.
- Configuration Mgt.

Continual Service Improvement
- Improve quality of service

IT governance processes

Strategic Sourcing Services

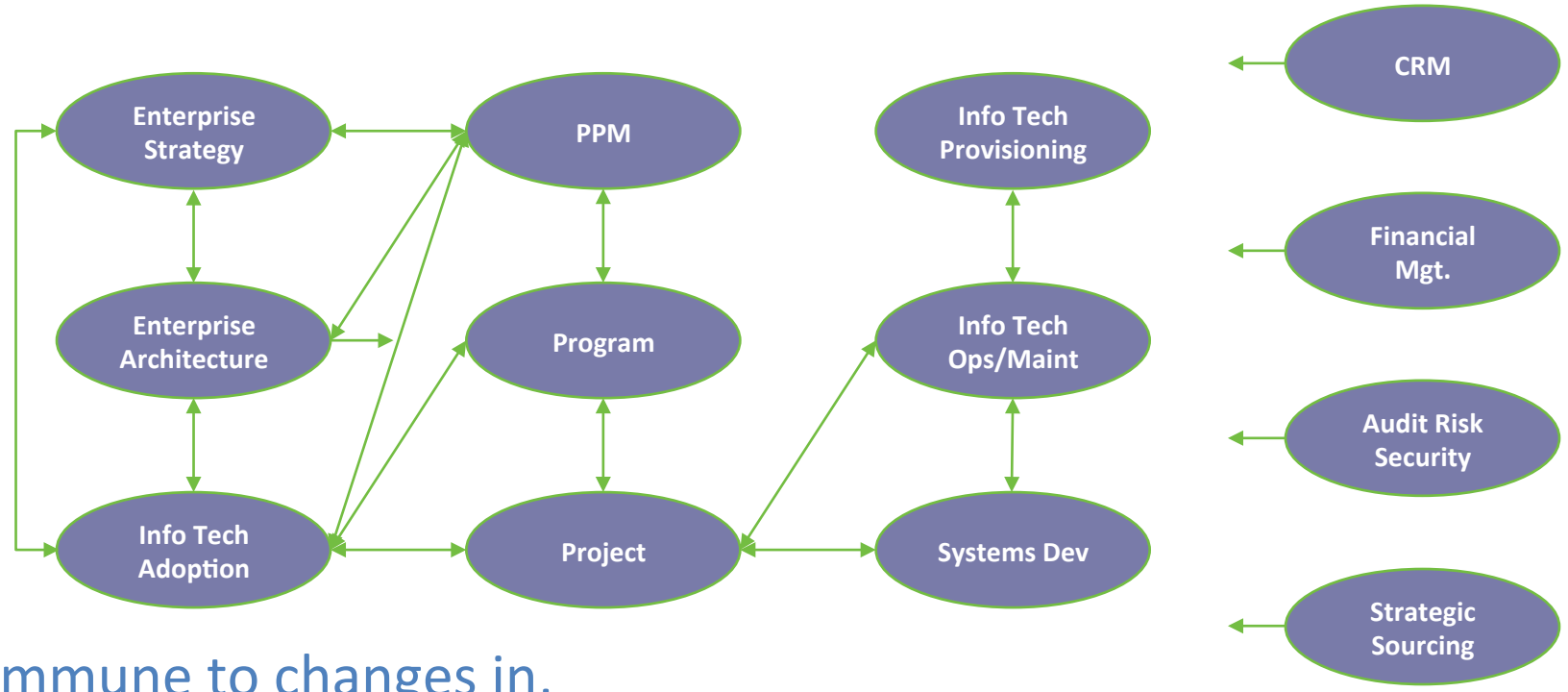
- Facilitates decision that services are better provided externally
- Ensures architectural fit
- Fact-based price comparisons
- Vendor and contract management
- Mitigate risks and prevent 'value-leakage'
- Sets clear expectations for provider performance/service levels
- Ensure compliance with corporate and regulatory requirements

IT governance processes

Audit and Risk Management

- Risk modeling and assessment
- Partner with IT Audit – COBIT
- Security
- Compliance
- Policies & Standards
- Service continuity and disaster recovery

IT governance process flows



Immune to changes in,

- economic environment
- business environment
- information technology trends and advances

Sustaining IT Governance

IT governance principle metrics

Strategic Alignment

> Show how IT supports the Enterprise Strategy

> Show how IT Operations are aligned with current Enterprise Operations

Value Delivery

> Show how IT delivers appropriate quality on-time and within budget

> Show how actual cost and ROI is managed

Risk Management

> Risk Controls

> Transferring risk

> Risk acceptance

Resource Management

> Show how IT optimizes the infrastructure

> Show how IT optimizes human resources

Performance Management

> Show how IT measures performance (balanced scorecard, KPIs, etc.)

> Use of automated systems providing performance data and information

Strategic alignment

Focus on aligning with the business and collaborative solutions

- Show how IT supports the Enterprise Strategy
- Show how IT Operations are aligned with current Enterprise Operations

Show how IT:

- Delivers against the strategy
- Adds value to products and services
- Improves customer satisfaction and customer retention
- Assists in competitive positioning
- Balances investments between systems that support the enterprise as is, and transforms the enterprise to create an infrastructure that enables the business to grow
- Contains costs and improves administrative efficiency
- Increases managerial effectiveness

Value delivery

Optimizing expenses and proving the value of IT

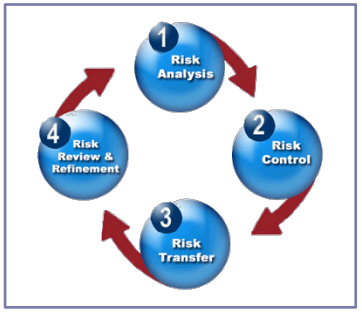
- Show how IT delivers appropriate quality on-time and within budget
- Show how actual cost and ROI is managed

Show how IT:

- Is fit for purpose, meeting business requirements
- Flexible to adopt to future requirements
- Provides required throughput and response times
- Enables ease of use, resiliency and security
- Provides integrity, accuracy and currency of information

Risk Management

Addressing the safeguard of IT assets, disaster recovery and continuity of operations



- Risk Controls
- Transferring risk
- Risk Acceptance

Show how IT:

- Mitigates risk by implementing controls (e.g. Risk Management Systems, Audit controls, acquiring and deploying security technology to protect the infrastructure, Business Continuity Planning, Disaster Recovery, etc.)
- Transfers risk by sharing risk with partners or transfers risk to insurance coverage
- Accepts risk by formally acknowledging that the risk exists and it is being monitored

Resource management

Optimizing knowledge and IT infrastructure

- Show how IT optimizes the infrastructure
- Show how IT optimizes human resources

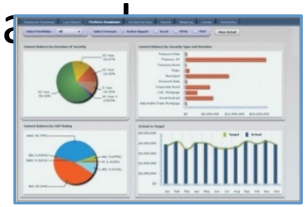
Show how IT:

- Manages system procurement
- Benefits from service procurement
- Manages the lifecycle of hardware, software licenses and services contracts
- Applies appropriate methods and adequate skills to manage and support IT Projects and Systems
- Improves workforce planning, recruiting and workforce retention
- Provides IT education and development

Performance management

Tracking project delivery and monitoring IT services

- Show how IT measures performance (balanced scorecard, KPIs, etc.)
- Use of automated systems providing performance data and information



Show how IT:

- Establishes and measures financial objectives
- Maps financial objectives to customer requirements and needs
- Measures process performance, effectiveness, efficiency and criticality to the business
- Addresses innovation requirements and future needs
- Determines how business executives and users view the IT department

Symptoms of poor IT Governance

- Senior executives can't describe your IT Governance
- Decisions take too long
- There is little accountability for decisions

- Senior management less than happy (IT Governance performance self-assessment is poor or varies widely by respondent)
- There is ineffective IT Portfolio Management – duplication, too many applications, low percentage spend on new initiatives
- IT Governance seen as overhead and "red-tape"

Assess your IT Governance resilience

For each of the following assess your IT Governance on a score of 1 (strongly disagree) to 5 (strongly agree) – X 2 = Total

- Our senior executives could accurately describe our ITG
- Our ITG was actively designed – not a series of uncoordinated mechanisms
- Our ITG is stable with few changes in recent years.
- Managers who ignore the ITG are counseled to follow the guidelines
- There are a small number of key business objectives driving our ITG design
- We have a well defined and fast exceptions process that requires political capital to escalate
- The ITG has a clear owner(s) and measures of success
- The pay, incentives, and the ITG are well aligned
- We have effective ITG at both firm wide and BU levels which are linked
- Our CIO could leave for two months and our ITG would work well

Maturing IT Governance requires…

- Acknowledging that governance is both decision-making and accountability (should be empowering, not bureaucratic)
- Linking the firm's other key assets and incentives to governance
- Recognizing the link to financial performance (firms with superior IT Governance also had more than 20% higher profits)
- Determining what should be shared at enterprise, sector and BU levels and govern at that level

Maturing IT Governance requires…

- Relying on a few IT governance mechanisms (utilizing non-IT governance mechanisms e.g., exec committee, CapEx process, etc.)
- Focusing on how each project and service contributes to a reusable digitized platform
- Centralizing for cost focus – decentralizing for innovation and growth and blended governance to achieve both
- Simplification, removing bureaucracy and fostering more communication

Advice when addressing IT governance

- Ensure IT Governance is driven by business problems and opportunities – not Governance for its own sake
- Transparency is the most critical aspect of IT Governance
- Design deliberately at enterprise and BU levels
- No one-size-fits all – find the right flavor

Advice when addressing IT governance

- Redesign and constantly strike the balance – not too much, not too little
- Governance processes can be sophisticated and complex, or incredibly simple and should quickly address and respond to exceptions
- Assign ownerships that continually educates, engages, incentivizes, and proves the value of IT Governance – The three M's: metrics, measures and marketing

IT governance critical success factors

- Absolutely requires Executive sponsorship and leadership – vision and enablement
- Absolutely requires Business participation – IT facilitates but the business must be a partner, if not the leader in the effort
- Business process initiative – This requires skills in process management, design, implementation – and organizational change
- Decisions require fact-based information – This requires a systematic approach to collect, integrate, analyze and provide meaningful data

Auditing IT Governance

FDIC Bus Technology Strategic Plan 2013-2017

IT Service Management

Governance

Governance ensures that information technology is aligned with the business and delivers value, performance is measured, resources are properly allocated and risks are managed and mitigated. The governance of information technology at the FDIC is a collaborative endeavor, led by the CIO Council. The CIO Council advises the CIO on all aspects of adoption and use of IT at the FDIC. The Council provides a leadership forum and is part of the governance structure for discussing issues of mutual interest across organizational boundaries. The Council champions the creative use of IT to support FDIC stakeholders and maximize the efficiency of FDIC's internal operations. The Council prioritizes and selects IT projects for funding and reviews the progress of these projects on a monthly basis. The Council is chaired by the CIO and its membership includes senior managers from the FDIC divisions and offices. The CIO Council is heavily involved in the execution of the business technology strategy, guiding the sequencing of application modernization efforts.

Major information technology investments are overseen by the Capital Investment Review Committee (CIRC). The Committee determines whether a proposed investment is appropriate for the FDIC Board's consideration, oversees approved investments throughout their life cycle, and provides quarterly reports to the Board of Directors. The committee is co-chaired by the CFO and CIO and its membership includes all division directors.

The implementation of the strategic imperatives outlined in this plan will be monitored by the FDIC's Enterprise Architecture Board (EAB). The EAB provides guidance, direction and oversight necessary to ensure that FDIC's enterprise architecture provides a comprehensive and effective mechanism for ensuring that IT solutions are optimized to support the mission and strategic direction of the FDIC.

The FDIC follows industry best practices and employs governance frameworks and methodologies to ensure successful execution of information technology projects, investments, and services. Chief among these methodologies are the Information Technology Infrastructure Library (ITIL) and Rational Unified Process (RUP). ITIL is a framework of best practice approaches to facilitate the delivery of high-quality IT services. The framework outlines best practices for IT data center operations and services. The FDIC uses ITIL to help with internal integration and standardization efforts, and to ensure data center operations are better documented, repeatable, and easier to audit. RUP is a full life cycle process framework for delivering IT solutions, and is intended to be tailored to allow project teams to select the appropriate elements of the process for each IT effort. The FDIC has adapted the base RUP framework to support a wide range of IT projects such as system maintenance and enhancement, implementation of commercial off the shelf products, and custom software development. RUP is based on a set of core principles and best practices, which emphasize an iterative and incremental approach to conducting IT projects, the use of a component-based architecture, visual modeling, and close management of requirements.

Federal Financial Institutions Examination Council

IT Examination Handbook – Management

Introduction

Risk Overview

- Operational / Transaction Risk

Roles and Responsibilities

- IT Roles
  - Board of Directors / Steering Committee
  - Chief Information Officer / Chief Technology Officer
  - IT Line Management
  - Business Unit Management
- IT Responsibilities and Functions
  - Risk Management Functions
  - Project Management
  - Other IT Functions and Support Roles

IT Risk Management Process

- Planning IT Ops & Investment
  - Strategic IT Planning
  - Operational IT Planning
- Risk Identification and Assessment
- IT Controls Implementation
  - Policies, Standards, and Procedures
  - Internal Controls
  - Personnel
  - Insurance
  - Information Security
  - Business Continuity
  - Software Development and Acquisition
  - Operations
  - Management Booklet
  - Outsourcing Risk Management
- Measure and Monitor
  - Plan-to-Actual Outcome Measures
  - Performance Benchmarks
  - Service Levels
  - Quality Assurance/Quality Control
  - Policy Compliance

Mgt. Considerations for Technology

- Financial Information
- Contracts
- Audit Reports
- Customer Service

FFIEC - IT Governance

Federal Financial Institutions Examination Council

The IT Governance Institute defines IT governance as "...an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives." Due to the reliance on technology, effective IT management practices play an integral role in achieving many goals related to corporate governance. The ability to manage technology effectively in isolation no longer exists. Institutions should integrate IT management into the strategic planning function of each line of business within the institution. Financial institutions face many challenges in today's marketplace that increase the importance of IT management.

FFIEC – ITG Definition

From the glossary

Governance:

In computer security, governance means setting clear expectations for the conduct (behaviors and actions) of the entity being governed and directing, controlling, and strongly influencing the entity to achieve these expectations. It includes specifying a framework for decision making, with assigned decision rights and accountability, intended to consistently produce desired behaviors and actions.

Global Technology Audit Guide (GTAG®)

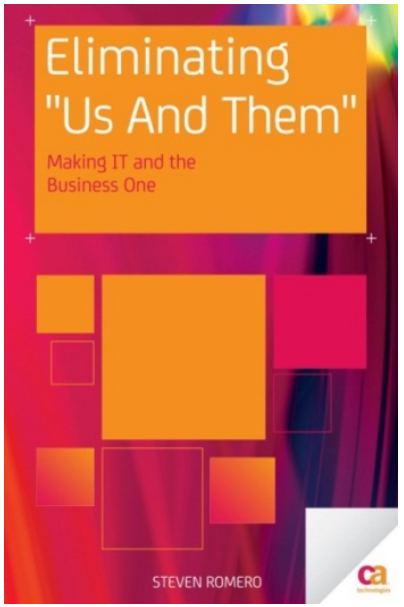
Auditing IT Governance: What is IT Governance?

IT governance involves managing IT operations and IT projects to ensure alignment between these activities and the needs of the organization defined in the strategic plan. Proper alignment between IT and the organization means:

- organization management understands the potential and limitations of IT;
- the IT function understands the objectives and corresponding needs of the organization; and
- this understanding is applied and monitored throughout the organization via an appropriate governance structure and accountability. Understanding the value and the cost of IT is important for the board and senior and IT management. Successful alignment between the organization and IT occurs when goals and objectives of the organization are aligned with the needs of the organization, and IT is able to meet those needs in collaboration with management.

A book about IT governance, process, & culture

Romero Consulting



June 2011

Eliminating 'Us and Them' – Making IT and the Business One

http://www.amazon.com/Eliminating-Us-Them-Making-Business/dp/1430236442

Thank you

Steven Romero

IT Business Value Activist

and IT Governance Evangelist

steve@itgevangelist.com

Twitter @itgEvangelist

http://www.itgevangelist.com/