IT Governance

What is it and how to audit it

21 April 2009

Ernst & Young

Quality In Everything We Do

Agenda

- Can you define IT Governance
- What are the key objectives of IT Governance
- How should IT Governance be structured
  - Roles and responsibilities
- Key challenges and barriers
- Auditing IT Governance
  - Scope
  - Test procedures
  - Recommendations
  - Reporting
- Questions

What are the key objectives of IT Governance

- IT Governance should be a component of an overall enterprise-wide Governance structure
  - Strategy alignment
  - Value delivery
  - Risk management
  - Resource management
  - Performance measurement
- Should establish
  - Transparency
  - Accountability
  - Open communication
  - Common language

What are the key objectives of IT Governance

Strategic Alignment

- Strategic Alignment focuses on the investment decision and the realization of optimal benefits from IT. It involves maintaining and validating the IT value proposition. Strategic Alignment ensures a clear linkage between the enterprise strategy, the portfolio of IT-enabled investment programs that execute the strategy, the individual investment programs, and the business and IT projects that make up the programs. It is based on the principle that value is only achieved from IT when IT-enabled investments are managed as a portfolio of programs which include the full scope of changes that the business has to make in order to optimize the value from IT capabilities in delivering on the strategy.

- Strategic Alignment increases the understanding and transparency of cost, risks and benefits resulting in much better informed management decisions. It increases the probability of selecting investments that have the potential to generate the highest return and increases the likelihood of success of executing selected investments such that they achieve or exceed their potential return. Strategic Alignment reduce costs by not doing things they should not be doing, and taking early corrective action on or terminating investments that are not delivering to their expected potential. It reduces the risk of failure, especially high-impact failure. Finally it reduces the surprises relative to IT cost and delivery, and in so doing increase business value, reduce unnecessary costs and increase the overall level of confidence in IT.

What are the key objectives of IT Governance

Value Delivery

- Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing expenses and proving the value of IT, and on controlling projects and operational processes with practices that increase the probability of success (quality, risk, time, budget, cost, etc).

- Value Delivery enables the management of IT-enabled investment programs and other IT asset and services to ensure that they deliver the greatest possible value in supporting the enterprise's strategy and objectives. It ensures that the expected business outcomes of IT-enabled investments, and the full scope of effort required to achieve those outcomes, is understood; that comprehensive and consistent business cases are created and approved by stakeholders; that assets and investments are managed throughout their economic lifecycle; and that there is active management of the realization of benefits, such as contribution to new services, efficiency gains and improved responsiveness to customer demands.

- Value Delivery enforces a disciplined approach to portfolio, program and project management, insisting that the business takes ownership of all IT enabled business initiatives and that IT ensures optimization of costs of delivering IT capabilities and services. It ensures that technology investments are standardized to the greatest extent possible to avoid the increased cost and complexity of a proliferation of technical solutions.

What are the key objectives of IT Governance

Risk Management

- Risk Management requires risk awareness of senior corporate officers, a clear understanding of the enterprise's appetite for risk and transparency about the significant risks to the enterprise; it specifically addresses the safeguarding of IT assets, disaster recovery and continuity of operations.

- A risk assessment framework should be established to enable a consistent and comprehensive approach to risk management for IT within the context of enterprise-wide risk management. This should incorporate a regular assessment of the relevant risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an agreed level. The enterprise's risk appetite for IT risks defined and communicated with agreement on a risk management plan. Risk management responsibilities should be embedded into the organization, ensuring that business and IT regularly assess and report IT related risks and the impact on the business. IT management should follow-up on risk exposures, paying special attention to IT control failures and weaknesses in internal control and oversight, and their actual and potential business impact. The enterprise's IT risk position should be transparent for all stakeholders.

What are the key objectives of IT Governance

Resource Management

- Resource management focuses on optimal investment, use and allocation of IT resources (people, applications, technology, facilities, infrastructure, data) in servicing the needs of the enterprise, while maximizing the efficiency of these assets and optimizing their costs.

- Optimization of the investment, use and allocation of IT assets is achieved through regular assessment, making sure that IT has sufficient, competent and capable resources to execute the current and future strategic objectives, and able to meet business demands. Clear, consistent and enforced procurement policies and mechanisms need to be ratified and institutionalized to ensure resource requirements are fulfilled effectively and conform to architecture policies and standards. The IT infrastructure should be assessed on a periodic basis to ensure that it is standardized wherever possible and interoperability exists where required.

- A key challenge is to know where and how to outsource and then to know how to manage the out-sourced services in a way that delivers the values promised at an acceptable price. Resource Management ensures that knowledge is retained and shared across the company.

What are the key objectives of IT Governance

Performance Measurement

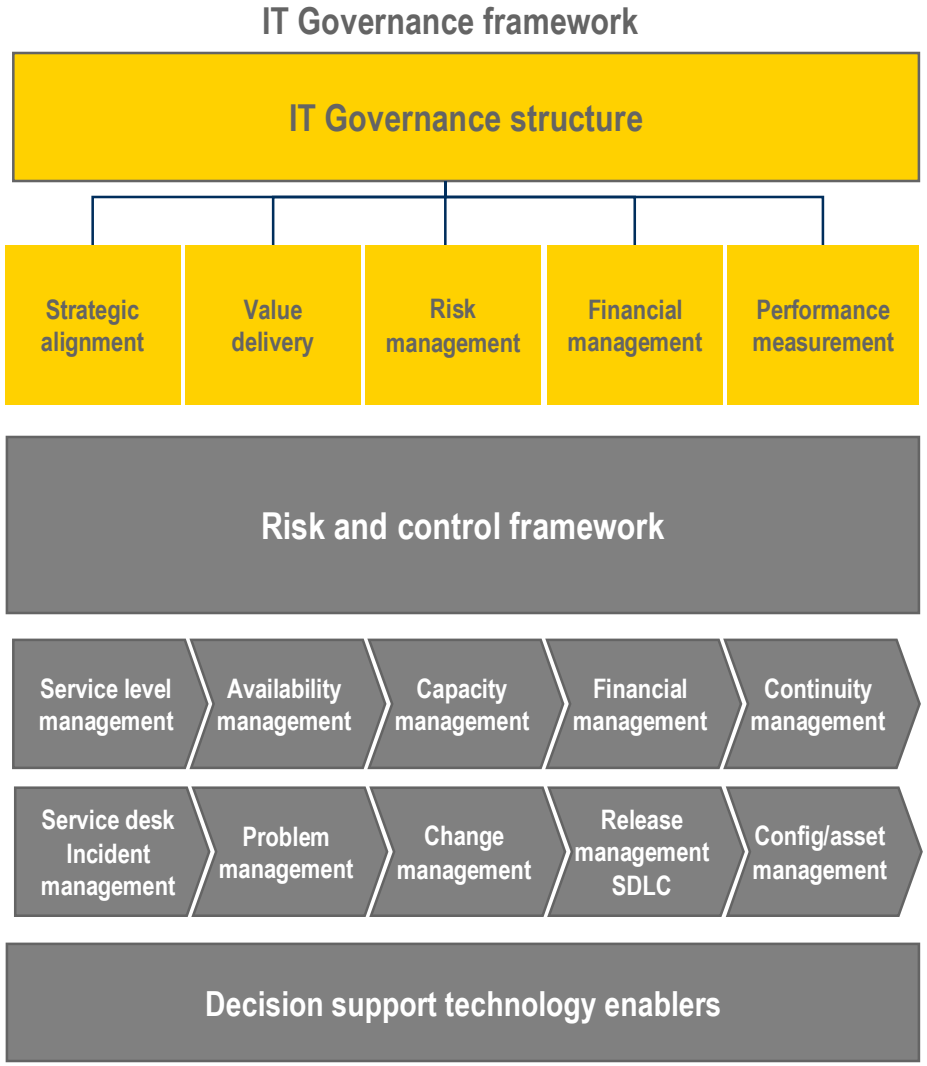
- Performance Measurement involves the tracking of project delivery and monitoring IT services, using balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age: customer focus, process efficiency and the ability to learn and grow.

- Relevant portfolio, program and IT performance should be reported to the Board and Executive in a timely and accurate manner. Management reports should be provided for senior management's review of the enterprise's progress toward identified goals. Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Integrate reporting with similar output from other business functions. The performance measures should be approved by key stakeholders. The Board and Executive should challenge these performance reports and IT Management be given an opportunity to explain deviations and performance problems. Upon review, appropriate management action should be initiated and controlled.

How should IT Governance be structured

- Governance starts with the Board of Directors
  - Audit Committee or IT Strategy Committee
    - Drive enterprise alignment
    - Direction of value
    - Monitor risks
    - Measure performance
- IT Steering Committee
  - CEO, Business Executives, CIO, Audit, Legal, Finance, HR
    - Align and structure IT organization with overall business goals
    - Establish risk framework to manage and monitor risks
    - Measure performance to goals
    - Establish IT competencies
    - Manage resources
    - Create an innovative environment
- Architecture Review Board
  - Technology standardization

Example IT Governance framework



Key challenges and barriers

- Limited board and executive support
- Lack of accountability
- Poor communication
- Project and resource management
- Inflexible IT organizational structure
- “Wild Wild West” architecture
- Inconsistent policies and procedures
- No defined governance or risk framework

- Don’t “boil the ocean”

Auditing IT Governance

- Communicate expectations with senior management
  - Expect to spend time helping management understand what IT Governance includes
- Scope
  - This is not an audit of IT project management or key controls
  - Start broad and don't dive deep into controls
- Test procedures
  - Interview board members, C-suite, business management, finance, IT management and process managers
    - Leverage a consistent questionnaire for each of the five governance domains
  - Inspect documentation and observe tools and reports
    - Could test the completeness and accuracy as part of other audits
  - Sampling or attribute testing is not usually required
- Reporting
  - Utilize a maturity model to establish current and future state
  - Who will take ownership? CIO, CFO, CEO, COO, Board, AC

Audit Reporting
Where are we and where do we want to go

Maturity rating	Non Existent: 0	Initial: 1	Repeatable: 2	Defined: 3	Managed: 4	Optimized: 5
Description	Management processes are not applied at all	Processes are ad hoc and disorganized	Processes follow a regular pattern	Processes are documented and communicated	Processes are monitored and measured	Processes are integrated and automated

Domain/Maturity	Current state indicators	Associated potential risks
Strategic alignment (1.5)	► Coherent processes have not been defined, implemented or consistently followed to provide for clear and active linkage among the enterprise strategy, and the portfolio of IT-enabled investment programs that execute the strategy.	► Strategic IT planning not aligned with the overall corporate strategy. ► Improper or inconsistent allocation of IT investments ► Inability to support the enterprise's objectives ► IT directions not defined and not supporting business goals
Value delivery (1.0)	► The company has not formally defined a suite of guiding or core IT principles that are based on business maxims. Furthermore, the company does not appear to have a formal risk-based Enterprise IT architecture based on business strategies.	► Lack of alignment between the business objectives and the IT architecture ► Full value of IT assets and services are not realized by the business ► Increasing costs for IT investments and operations
Risk management (1.5)	► Although the organization has adopted an IT risk management framework, clear guidelines/methodology for measuring risk appetite, inherent risk and residual risk is not defined or embedded within the risk framework.	► Lack of alignment between the IT risk and Enterprise risk ► Ineffective management of IT risks ► Increased expenses and costs incurred to manage unanticipated risk
Financial management (3.0)	► While mature financial management processes are practiced within the IT organization, improvement opportunities exist in areas of management information concerning financial targets, cost of resources, and actions necessary to achieve financial targets.	► Lack of business awareness of costs associated with IT ► Over/under funding associated with IT resource allocation ► Inaccurate financial planning and monitoring of the IT budget against financial targets.
Performance measurement (1.5)	► Processes and practices are not in place to measure the success of IT investments that is developed jointly and agreed between business units and IT during both strategic planning and the beginning of major programs.	► Performance gaps not identified in a timely manner ► Service deviations and degradations not recognized and addressed, resulting in failure to deliver business requirements

Note: The maturity ratings do not represent a conclusion on the adequacy or effectiveness of internal controls.

How do we improve?
Strategic alignment

Current state indicators	Associated potential risk
► Coherent processes have not been defined, implemented or consistently followed to provide for clear and active linkage among the enterprise strategy, and the portfolio of IT-enabled investment programs that execute the strategy.	► Strategic IT planning not aligned with the overall corporate strategy ► Improper or inconsistent allocation of IT investments ► Inability to support the enterprise's objectives ► IT directions not defined and not supporting business goals

Observations	Suggested next steps	Potential challenges
► A process to align enterprise business objectives with IT initiatives is not formalized.	► An IT Steering Committee (ITSC) should be established that includes executive members of management and IT ► The ITSC should evaluate how IT initiatives / drivers map back to business objectives and approve based on priority ► The initial ITSC meetings should be facilitated to provide open discussion and communication	► Members of the ITSC may have individual or business unit interests and not an overall organizational perspective ► May not be structured as an effective governing body
► IT investments are inconsistently managed	► IT should adopt a formal strategy of managing investments based on portfolio (ie, Infrastructure, Applications, Service Support) ► Establish a clear definition of how IT investments are categorized and funded.	► Organizational structure and alignment with business units ► Ability to raise accountability for IT & Business ► Resistance to change
► A defined set of performance objectives, measures, targets and benchmarks have not been approved ► A clear understanding of the total cost of ownership by key stakeholders does not exist	► The ITSC should agree on how IT will be measured ► An executive dashboard / scorecard should be presented during each ITSC	► Ability to capture meaningful information in a cost efficient manner ► Metrics are not meaningful and measure effectiveness and efficiencies ► Metrics are not tied to performance or business initiatives

References

- Board Briefing on IT Governance 2nd Edition
- IT Alignment: Who is in Charge?
- Information Risks: Whose Business Are They?
- Optimizing Value Creation From IT Investments
- Measuring and Demonstrating the Value of IT
- IT Governance Implementation Guide 2nd Edition

Thank You

Scott V. Andress
Ernst & Young, LLP
Advisory Executive Director
(901) 528-7572
scott.andress@ey.com

Ernst & Young LLP

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 135,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com.

0811-1007855