University of Dar es Salaam

Lecture 5 – IT Governance & Strategy

Aron Kondoro

Introduction

- IT governance provides the structure to achieve the **alignment of the IT strategy with the business strategy,** to incorporate IT into the **enterprise risk management program**, to **manage the performance of IT** and ensure delivery of value, and to **ensure adequate internal controls** and **regulatory compliance**

Enterprise Risk Management(ERM)

- Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to **identify potential events** that may affect the entity, and **manage risks** to be within its risk appetite, to provide **reasonable assurance** regarding the achievement of entity objectives.

What is ERM?

- Organizational Oversight
- Increasing Business Risks
- Regulatory Issues
- Market Factors
- Corporate Governance
- Best Practices

Regulatory Compliance

- Number of laws and regulations based on industry and jurisdiction
- Sarbanes-Oxley increased focus on internal controls
- CoBiT provides a framework to evaluate IT controls
- Need for continuous monitoring

Purpose of Controls

- Reduce or eliminate risk.
- *"Policies, procedures, practices, and organization structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected." (CoBiT, 1998)*

Management Responsibilities

- Assure that adequate, reliable and auditable controls will be used
- Determine that specified controls are functioning reliably

Independent Assurance

- Importance of IT to achieving organizational objectives
- CoBiT framework for governance and control of information technology
- Auditors assist organizations evaluate internal controls
- Management is responsible for internal controls

IT Governance Frameworks

- IT Infrastructure Library (ITIL)
  - https://www.axelos.com/certifications/itil-service-management
- COBIT
  - https://www.isaca.org/resources/cobit
- British Standard International Organization for Standardization (ISO)/International Electrotechnical Commission 27002 (ISO/IEC 27002)
  - https://www.iso.org/standard/54533.html

ITIL

- Library of best practice processes for **IT service management**
- Developed by UK's cabinet office of govt commerce (OGC)
- Core guidelines
  - **Strategy**: map IT strategy with overall business goals
  - **Design**: processes toward a solution designed to meet business needs
  - **Transition**: manage change, risk, & QA during deployment
  - **Operation**: maintain IT services once implemented in production
  - **Continuous improvement**: constantly looking for ways to improve process and services

COBIT (Control Objectives for Information and Related Technologies

- IT gov framework that helps orgs in regulatory compliance, risk management, and aligning IT strategy with organizational goals
- Authoritative, international set of IT practices or control objectives
- Ensures tech provides business with **relevant**, **timely**, and **quality info** for decision making
- Helps in: understanding IT systems, discharging fiduciary responsibilities, and deciding adequate levels of security and controls
- Auditors use to substantiate internal controls assessments

CoBiT Processes

- Planning and Organization
  - Strategies and tactics
- Acquisition and Implementation
- Delivery and Support
  - Includes actual processing of data
- Monitoring
  - Management's oversight of operations

ISO/IEC 27002

- Global standard that provides best practice recommendations related to information security management (ISM)
- Assists in implementing commonly accepted info security controls and procedures
- Standards
  - ISO/IEC 27001:2013 – implementing, maintaining, assessing ISM in context of the org
  - ISO/IEC DIS 27003 – information security management system implementation
  - ISO/IEC 27010:2015 – implementing ISM for inter-sector & inter-org communication
  - ISO/IEC 27013:2015 – integrated implementation of ISM and service management system
- Helps organizations select proper security measures using available domains of security controls

Joint Framework

- Organizations need to implement an **integrated framework** that draws on all 3 standards
- IT Governance Institute (ITGI) and OGC put together **The Joint Framework**
- Helps organizations comply with regulations and improve their competitiveness
- The framework allows organizations to:
  - Implement a single, integrated, compliance method
  - Meet regulatory requirements of data & privacy-related regulations
  - Prepare for ISO 27001 and ISO 20000 certifications

IT Performance Metrics

- Measuring performance is important to ensure IT meets goals and objectives of organizations
- An effective measure must be **reliable** and **valid**
- An example of an effective measure is the **IT Balanced Scorecard**

IT Balanced Scorecard (IBS)

- Provides an overall picture of IT performance aligned to the objectives of the organization
- Answers key questions: is our investment plan consistent with strategic goals? was the IT app just developed a success? Was it implemented effectively and efficiently? Is the IT department adding value? Should IT be outsourced?
- Measures and evaluates IT-related activities
  - IT-generated business value
  - Future orientation
  - Operational efficiency and effectiveness
  - End-user service satisfaction

IBS Aspects

- IT-generated business value
  - Through project and service delivery
  - Automating business processes – lower business costs (or higher revenue)
  - Agility in responding to new business opportunities
  - Metrics: perceived relationship between IT & Management; ROI; actual vs budgeted expenses; % over/under IT budget; revenue from IT-related services
- Future orientation
  - Training IT personnel for future challenges; improving service capabilities; enhancing enterprise architecture; researching emerging technologies
  - Metrics: No. of trainings; Staffing metrics by function; Project delivery schedules
- Operational efficiency and effectiveness
  - Internal processes to deliver IT products and services in an efficient and effective manner
  - Quality, responsiveness, security, and safety
- End-user service satisfaction
  - Whether user jobs are completed in time and accurately
  - Metrics: satisfying end-user needs; preferred supplier if applications and operations

Example of an IBS

Exhibit 5.1 Example of an IT Balanced Scorecard

Mission	*Objectives*	*Metric to Measure*	*Target Values/ Initiatives*
To contribute to the value of the business	**IT-GENERATED BUSINESS VALUE**		
	Business value and strategic contribution of IT department	– Completion of strategic initiatives – Percentage of resources devoted to strategic projects – Perceived relationship between IT management and senior-level management	
	Business value of IT projects	– Business evaluation based on financial measures (ROI, payback period, etc.)	
	Management of IT investment	– Actual versus budgeted expenses – Percentage over/under overall IT budget	
	Sales to outsiders or third parties	– Revenues from IT-related services and/or products	
To deliver continuous improvement and prepare for future challenges	**FUTURE ORIENTATION**		
	Knowledge management	– Completion of education, training, and development courses – Percentage of positions with qualified backup personnel – Expertise with specific technologies	
	Service capability improvement	Deliver internal projects to plan: – Internal process improvement – Organization development – Technology renewal – Professional development	

Regulatory Compliance and Internal Controls

- Organizations need to manage their compliance with laws and regulations
- Organization implement controls outlined in COBIT

IT Strategy

- A formal vision to guide in the **acquisition**, **allocation**, and **management** of resources to fulfill the organization's objectives
- Provides a roadmap for operating plans and framework for evaluating technology investments
- Should be part of an overall corporate strategy for IT and should align to the business strategy
- IT governance provides the structure and direction to achieve the alignment of IT & business strategy
- Without IT strategy risk is **increased cost of technology**

IT Steering Committee

- Composed of decision makers from various constituencies in the organization to resolve conflicting priorities
- Responsible for
  - Determining the overall IT investment strategy
  - Ensuring IT investments align with business priorities
  - IT & business resources are available to IT
- Tasks include
  - Prioritizing major development projects
  - Reviewing development and implementation plans
  - Monitoring status, schedule, and milestones for all major projects
  - Reviewing project budgets and ROIs

Operational Planning

- At the end, IT strategy needs to be translated into operating plans I.e. operationalization
- Operating planning process includes
  - Developing annual budget
  - Creating resource and capacity plans
  - Preparing individual performance plans for all IT staff
- Delivery of these plans is guided by a series of **governance processes**

Governance Process

1. Demand management
   - Requirements and business case approved by management
   - Technology costs approved by IT
2. Project initiation
   - Capacity and service levels approved by management
   - Technology resources approved by IT
3. Technical review
   - Solution design approved by management
   - Technical design approved by IT
4. Procurement and vendor mgt.
   - Requirements and solution approved by management
   - Technology vendors approved by IT
5. Financial management
   - Scope, schedule, and budget approved by management and IT
   - Progress is monitored by management and IT

Governance Process

- Demand Management
  - Ensures resources are devoted to projects with strongest business case
  - Ensures each project has business justification, business/IT sponsor & consistent approval process
- Project Initiation
  - Determines total cost and benefit
- Technical Review
  - Ensures right technical solution is selected, integrates with other components & requires minimum investment in infrastructure
- Procurement and Vendor Management
  - Defining requirements and specifications; selecting appropriate vendor; performing IT service or resource acquisition
- Financial Management
  - Cost/Benefit analysis
  - Budgeting

Conclusion

- IT governance establishes a foundation for managing IT to deliver value to the organization
- Realizing the value of IT requires partnership between management and IT
- Effective performance measurement aligns delivery to objectives

Further Readings

- Chapter 5 – Information Technology Control and Audit – 5th Edition
- Lecture 5 readings