IT Governance & the Control Environment

Week 2

ISACA' View of Governance

- What is IT governance and what are its components?
- How does this view fit with the concept "Do the right thing and do it right"?

- IT strategic alignment
- Risk management
- Value delivery
- Resource management
- Performance management

- Do the right thing
  - Strategic alignment
  - Risk management
- Do it right
  - Resource management
  - Value delivery
  - Performance management

What Does a Company Expect From Its IT Systems?

- Make a list of attributes that a company would want in its IT systems
- For example: a company wants its IT systems to be available

- Effective
- Efficient
- Confidential
- High integrity
- Available
- Compliant
- Reliable

COBIT 5 Enterprise Goals

Figure 4—COBIT 5 Enterprise Goals				
		Relation to Governance Objectives		
BSC Dimension	Enterprise Goal	Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

COBIT 5 IT-Related Goals

Figure 5—IT-related Goals		
IT BSC Dimension	**Information and Related Technology Goal**	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

What Are Controls?

Controls are the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented.

What Types of Controls Are There?

- Preventive
- Detective
- Corrective

What examples of each come to mind?

Where Are Controls Applied?

General Controls

- General controls apply to an IT service
- An example is identity management

Application Controls

- Application controls apply to a business process.
- For example, was a transaction
  - Recorded correctly?
  - Processed correctly?
  - Authentic?

Another View of Controls

- What are layered controls?
- Layered controls are sometimes referred to as “defense in depth”

What is a Control Environment?

The actions, policies, values, and management styles that influence and set the tone of a firm's day-to-day activities

BusinessDictionary.com

Control Environment
Role of Corporate Leadership

- Set the tone
- Bear ultimate responsibility for outcomes
- Develop and model principles and policies that represent desired outcomes
- Gain board support for policies and communicate outcomes

Control Environment
Role of Management

- Develop and document the practices and activities that are designed to ensure that the organization will meet the goals set by senior leadership
  - Processes
  - Standards
  - Guidelines

- Management defines the pathway to consistently meeting corporate objectives

Use of Controls by Management

- Controls are put in place to ensure that processes, standards and guidelines are being followed
- Controls help mitigate risk that undesired outcomes will occur
- Controls are usually used in combinations
  - They are unlikely to all fail simultaneously

Control Environment Monitoring & Audit

- Management should monitor controls to assess the degree to which desired behaviors and outcomes are consistently occurring
- Audits examine the adequacy (sufficiency) and effectiveness of the controls an organization has put in place