CS4050 – WEEK 7: INFORMATION SYSTEMS AUDIT AND CONTROL

FAST NUCES – SPRING 2024

BS COMPUTER SCIENCE

IT STRATEGY COMMITTEE VS. IT STEERING COMMITTEE

Level	IT Strategy Committee	IT Steering Committee

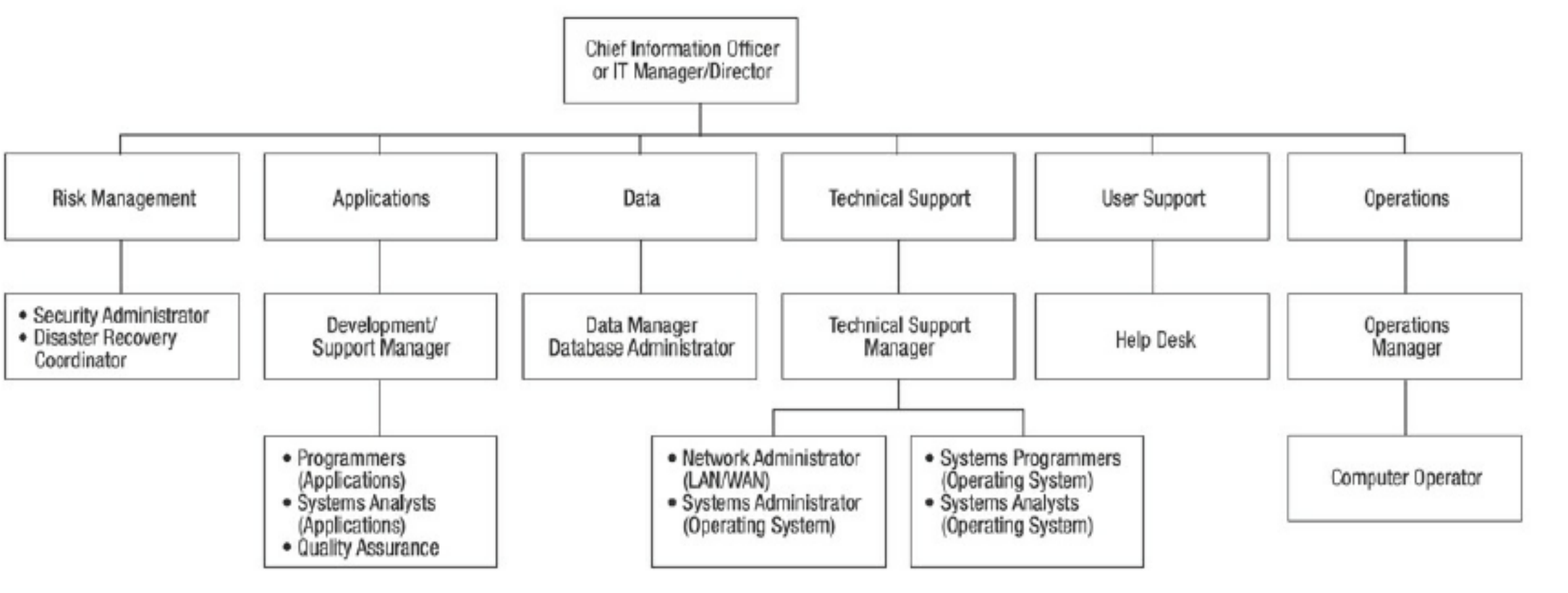
Responsibility	• Provides insight and advice to the board on:
	  ○ The relevance of developments in IT from a business perspective
	  ○ The alignment of IT with the business direction
	  ○ The achievement of strategic IT objectives
	  ○ The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives
	  ○ Optimization of IT costs, including the role and value delivery of external IT sourcing
	  ○ Risk, return and competitive aspects of IT investments
	  ○ Progress on major IT projects
	  ○ Containment of IT risk
	  ○ Direction to management relative to IT strategy
	  ○ Drivers and catalysts for the board's IT strategy
		• Decides the overall level of IT spending and how costs will be allocated
		• Aligns and approves the enterprise's IT architecture
		• Approves project plans and budgets, setting priorities and milestones
		• Acquires and assigns appropriate resources
		• Ensures that projects continuously meet business requirements, including reevaluation of the business case
		• Monitors project plans for delivery of expected value and desired outcomes, on time and within budget
		• Monitors resource and priority conflict between enterprise divisions and the IT function as well as between projects
		• Communicates strategic goals to project teams

Authority	• Advises the board and management on IT strategy • Is delegated by the board to provide input to the strategy and prepare its approval • Focuses on current and future strategic IT issues	• Assists the executive in the delivery of the IT strategy • Oversees day-to-day management of IT service delivery and IT projects • Focuses on implementation
Membership	• Board members and specialists who are not board members	• Sponsoring executive • Business executives (key users) • Chief information officer (CIO) • Key advisors as required (i.e., IT, audit, legal, finance)

SECURITY GOVERNANCE - MATRIX OF OUTCOMES & RESPONSIBILITIES

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	ProcessAssurance
Board of directors	Require demonstrable alignment.	• Establish risk tolerance. • Oversee a policy of risk management. • Ensure regulatory compliance.	Require reporting of security activity costs.	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilization.	Oversee a policy of assurance process integration.
Executive management	Institute processes to integrate security with business objectives.	• Ensure that roles and responsibilities include risk management in all activities. • Monitor regulatory compliance.	Require business case studies of security activities.	Require monitoring and metrics for security initiatives.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration.
Steering committee	• Review and assist security strategy and integrationefforts. • Ensure that business owners support integration.	Identify emerging risk, promote business unit security practices and identify compliance issues.	Review and advise on the adequacy of security initiatives to serve business functions.	Review and advise whether security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	• Identify critical business processes and assurance providers. • Direct assurance integration efforts.
CISO/ information security management	Develop the security strategy, oversee the security program and initiatives, and liaise with business process owners for ongoing alignment.	• Ensure that risk and business impact assessments are conducted. • Develop risk mitigation strategies. • Enforce policy and regulatory compliance.	Monitor utilization and effectiveness of security resources.	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	• Liaise with other assurance providers. • Ensure that gaps and overlaps are identified and addressed.
Audit executives	Evaluate and report on degree of alignment.	Evaluate and report on corporate risk management practices and results.	Evaluate and report on efficiency.	Evaluate and report on degree of effectiveness of measures in place and metrics in use.	Evaluate and report on efficiency or resource management.	Evaluate and report on effectiveness of assurance processes performed by different areas of management.

TYPICAL IT ORGANIZATIONAL STRUCTURE



CONSIDERATIONS FOR AUDITING IT GOVERNANCE STRUCTURE

- Excessive costs
- Budget overruns
- Late projects
- High staff turnover
- Inexperienced staff
- Frequent HW/SW errors
- An excessive backlog of user requests
- Slow computer response time
- Numerous aborted or suspended development projects
- Unsupported or unauthorized HW/SW purchases
- Frequent HW/SW upgrades
- Extensive exception reports
- Exception reports that were not followed up
- Lack of succession plans
- A reliance on one or two key personnel
- Lack of adequate training

ENTERPRISE ARCHITECTURE (EA)

EA involves documenting an organization's IT assets in a structured manner to facilitate understanding, management and planning for IT investments. An EA often involves both a current state and an optimized future-state representation (e.g., a road map).

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
Objective/Scope (contextual) *Role: Planner*	List of things important in the business	List of Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goal & Strategies
Enterprise Model (conceptual) *Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (logical) *Role:Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (physical) *Role:Builder*	Physical Data/Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Reprentation (out of context) *Role: Programmer*	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
Functioning Enterprise *Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

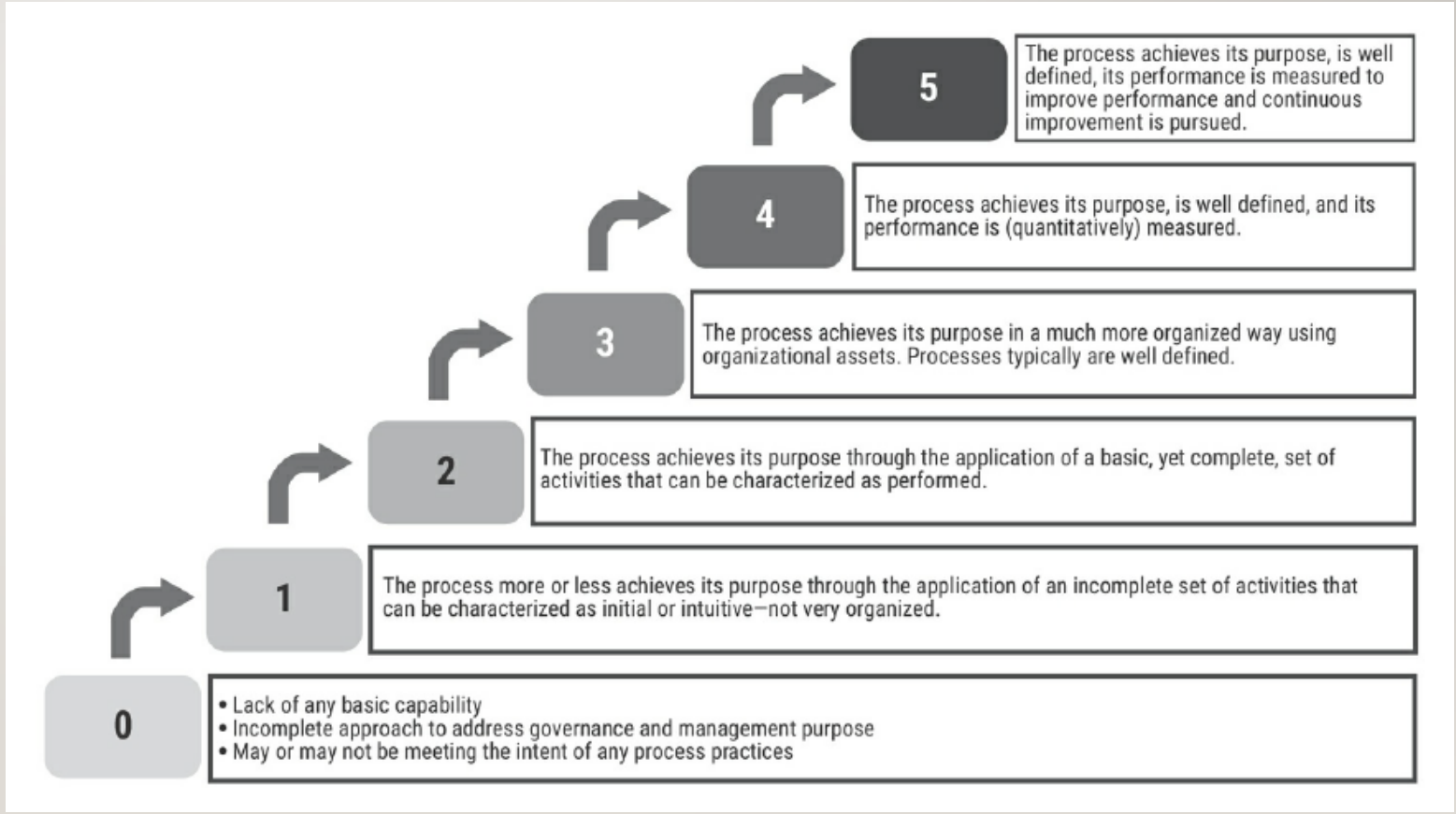
John Zachman's framework for EA

ENTERPRISE RISK MANAGEMENT

- Risk Management Process
  - **Asset** Identification
  - Evaluation of **threats** and **vulnerabilities** to assets
  - Evaluation of the **impact**
  - **Calculation** of risk
  - **Evaluation** of and **response** to risk

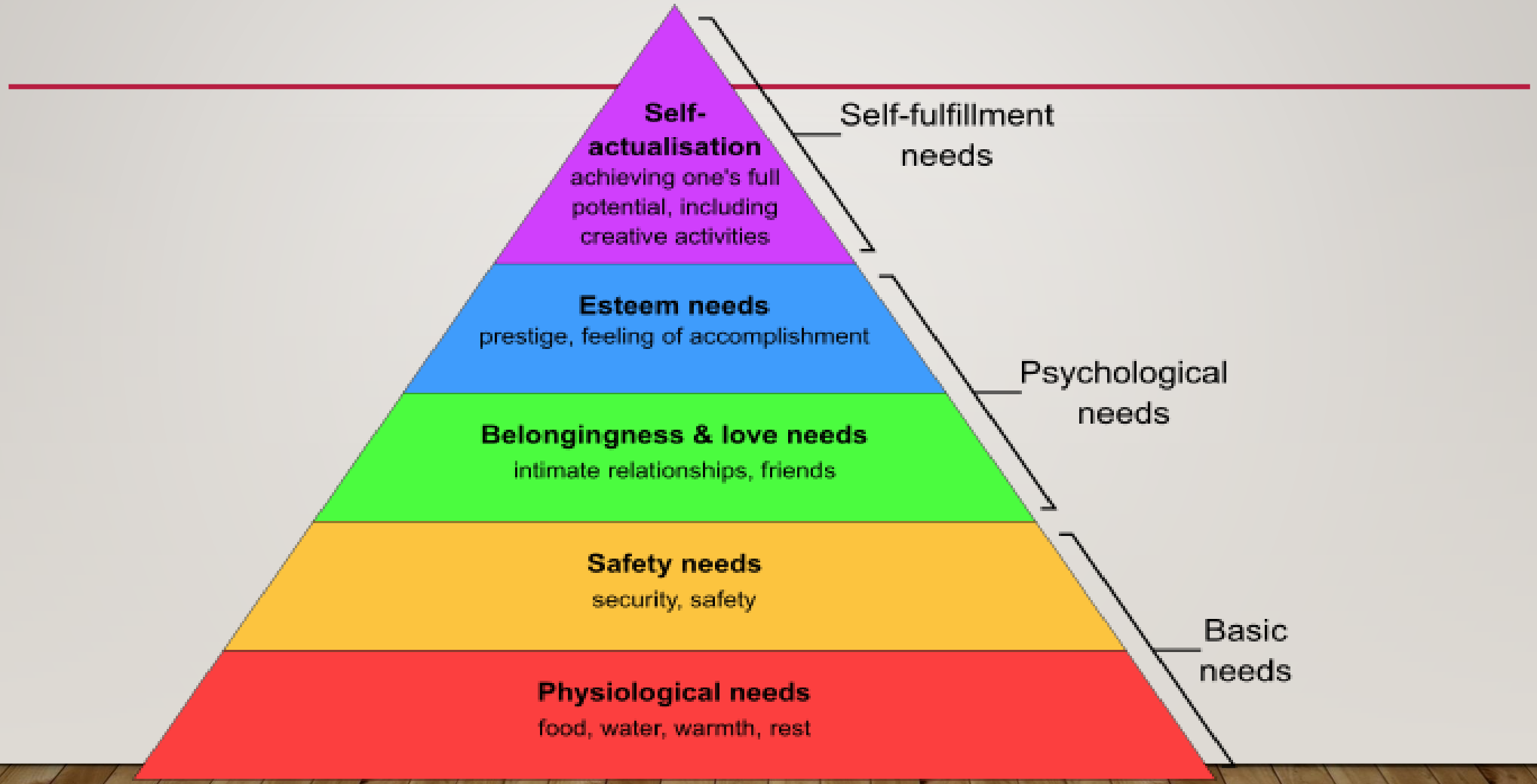
MATURITY MODELS

- Implementation of IT governance requires ongoing performance measurement of an organization's resources that contribute to the execution of processes that deliver IT services to the business. Maintaining consistent efficiency and effectiveness of processes requires implementing a process maturity framework. The framework can be based on various models such as Capability Maturity Model Integration (CMMI®) and the Initiating, Diagnosing, Establishing, Acting and Learning (IDEAL) model.



Characteristics of the Maturity Levels (CMMI)

MASLOW'S HIERARCHY OF NEEDS



PRIORITIZATION OF NEEDS