



BNAI MIS 3504

Controlling Business Processes

Controls

Photo: Installation by Jenny Holzer, US Pavillion, Venice Biennale 1990

Agenda

- **Quiz**
- **Review**
- **Day 7 Material: Business Controls**
- **Group Activity**
- **Project Review**
- **Exam Review**



Quiz-20 minutes

Quiz Review

Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
	95	60	55	90	30



What does a Business Rule look like

TERM1 –FACT- TERM2

Types of Business Rules

Restriction – **must or must not happen**

An order must not have more than one ship-to address.

Heuristics – **guidance on how to do something**

A customer is delinquent when their account is more than 30 days past due.

Inference – **given a condition, assume other conditions**

A generic version of a prescription drug will be used when one exists.

Timing – **activity based on elapsed time**

Each open compliant must be deleted when the root cause is identified.

Triggers – **cause and effect relationship**

The product ship date must be agreed when an order is taken.

From Business Analysis Body of Knowledge (BABOK)



IT Controls



Controls

Controls are defined as 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 are IT controls?

- They are specific activities performed by a person or system that have been designed to prevent or detect the occurrence of a risk that could threaten your information technology infrastructure and supported business applications.
- IT controls are generally grouped into two broad categories:
 - General controls commonly include controls over data center operations, system software acquisition and maintenance, logical security, and application system development and maintenance.
 - Application controls such as computer matching and edit checks are programmed steps within application software; they are designed to help ensure the completeness and accuracy of transaction processing, authorization, and validity.

Management's Use of Controls

Controls are put in place to **ensure** that the Processes, Standards and Guidelines are being followed.

Therefore, they help mitigate the risk that undesired outcomes will occur. These risks are call the **control objectives**

Types of Controls

Preventative ■ tries to avoid a risk or lessen its impact

Detective ■ discovers that a risk has occurred and needs to be addressed

Corrective ■ takes action to eliminate the problem and restore the environment

**Controls are usually used in combinations. This is called
“layered” controls or “defense in depth.”**

What is an example of this with which you are all very familiar?

COSO Framework

Operational objectives include performance measures and safeguarding the organization's assets against fraud. They focus on the effectiveness and efficiency of business transactions.

Reporting objectives, including internal and external financial reports and non-financial information, refer to the transparency, timeliness, and trustworthiness of the organization's reporting habits.

Compliance objectives are internal control targets based on adherence to governmental laws and compliance regulations.



COSO Internal Controls

1. Risk Assessment

- All organizations have risks and are exposed to factors that cause them not to reach their objectives. Risk assessments are performed to evaluate internal and external factors. Assessments provide reasonable assurance that organizations are managing risks to an acceptable tolerance.

COSO Internal Controls

2. Control Activities

- Control activities are taken to mitigate risk at all levels of the organization. The COSO framework helps to assure that the control activities performed by organization members are effective for the company to achieve its goals and eliminate unnecessary risks.

COSO Internal Controls

3. Information & Communication

- The controls provided by COSO help assure that productive communication occurs.

This includes using consistent language and following best practices for sharing appropriate levels of information with the right stakeholders. Formal management business reviews and all-employee meetings, as well as informal chats and emails, fall under this component.

COSO Internal Controls

4. Control Environment

- The control environment creates a top-down approach to drive the COSO Framework throughout the organization. It consists of a set of standards, processes, and procedures which are overseen and enforced by management. Establishing controls across the environment assures that standard practices and ethical values are used throughout the organization.

COSO Internal Controls

5. Monitoring Activities

- Ongoing monitoring and internal audits of all internal control systems identify early signs of trouble and assure effectiveness. Metrics and reports are provided to management and the board of directors for ongoing evaluation. Information gathered and evaluated by regulators and auditors verify control activities. Audits of financial reporting also help with fraud deterrence.

Implementing the COSO Framework

- 1. Understand and learn the framework**
- 2. Develop a plan**
- 3. Assess the plan's success and get buy in**
- 4. Remediation**
- 5. Test, Inform, and Optimize**



Hierarchy of IT Controls

Monitoring & Audit

Management should **monitor** their controls to see if the desired behavior is being realized.

Audits examine the **sufficiency (adequacy) and effectiveness** of the controls that an organization has put in place.

How are process controls set up?

Identify the **process** in question and its limits.

What are the process' **expected outcomes** and risks?

What can you do to help **assure/avoid** these objectives?

What **evidence** can you collect to monitor if these controls are working?

Importance of IT Controls

Needs for IT controls from a business perspective:

- **Controlling cost**
- **Remaining competitive**
- **Complying with laws and regulations**

Implementing effective IT control improves efficiency, reliability, flexibility, and availability of assurance evidence



Team Work: The Sales Book Management Case



Assignment: 60 minutes

Answer:

Questions in the case (multiple choice)

Create:

ERD

Business Rules

Controls

All in a PowerPoint Presentation (each team will present today for 5 minutes).



Break: 15 minutes



Final Project Reminders

Reminders

Final Exam Sunday (8-9AM)

Group Presentation (9AM-11AM)

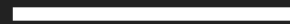
Group Project due to Professor by Sunday Night-30-October



Final Project Work: 50 minutes



Exam Review



Please Review

Swimlane diagrams

ERDs

Business Requirements

Saffers Rules of Research

IT Controls (COSO)

Business Rules

Project Roles

Anything you have read, watched, or studied OUTSIDE of class is fair game!



GOODBYE

再见