

Systems Design Fundamentals II

CSIT883 System Analysis and Project Management



UNIVERSITY
OF WOLLONGONG
AUSTRALIA



Outline

What Is Systems Design?

Systems Design Activities

System Controls and Security

Part I

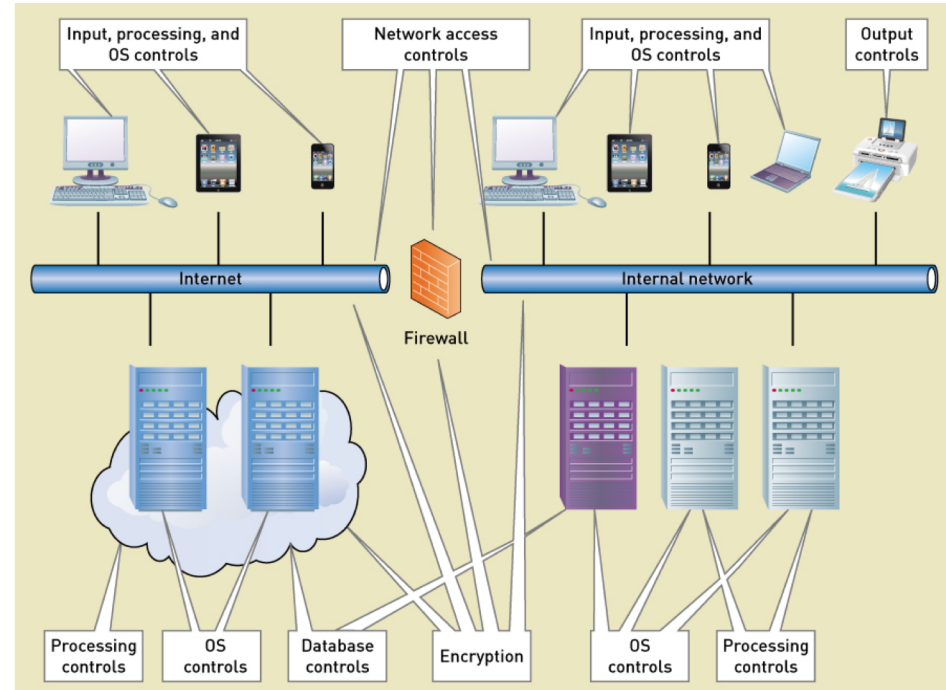
Part II



System Controls and Security

- **Importance** of Controls and Security for modern information systems
- Consider the security-specific activity a major systems design activity (similar to those discussed in the previous video)?
- Controls and security are embedded in all design activities

Security and integrity control locations





Designing Integrity Controls

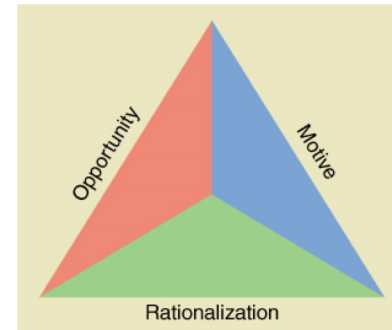
- **Controls** – mechanisms and procedures that are built in to a system to safeguard the system and the information within it.
- **Integrity controls** – controls that reject invalid data inputs, prevent unauthorised data outputs, and protect data and programs against accidental or malicious tampering
 - In contrast to system controls (talked later)
- Primary objectives of integrity controls:
 - To ensure that only appropriate and correct business transactions occur
 - To ensure that the transactions are recorded and processed correctly
 - To protect and safeguard the assets of the organization (including hardware, software, and information)



Designing Integrity Controls

Key aspects of Integrity Controls:

- **Input control**: controls that prevent invalid or erroneous data from entering the system
- **Output control**: controls that ensure that output arrives at the proper destination and is accurate, current, and complete
- **Redundancy, backup, and recovery**: procedures are designed to protect software and data from hardware failure and malicious destruction
- **Fraud prevention**: means to preventing users (especially rightful users) to commit frauds
 - Fraud triangle: *Opportunity, Motive and Rationalization*





Design Security Control

- **Security Control** – controls that protect the assets of an organization from all threats, with a primary focus on external threats
- In addition to the objectives for integrity controls, security controls must:
 - Maintain a stable, functioning operating environment for users and application systems.
 - Protect information and transactions during transmission across insecure environments such as public wireless networks and the Internet.



Design Security Control

- **Access control**: a security control that limits a user's ability to access resources, such as servers, files, Web pages, application programs, and database tables
- **Authentication**: the process of identifying users who request access to sensitive resources
- An **access control list**: a list attached or linked to a specific resource that describes users or user groups and the nature of permitted access
- **Authorization**: the process of allowing or restricting a specific authenticated user's access to a specific resource based on an access control list



Design Security Control

- **Data Encryption**: a method of securing data with interval systems and during transmission
- **Encryption**: the process of altering data so unauthorized users can't view them
- **Decryption**: the process of converting encrypted data back to their original state
- **Encryption algorithm**: an encryption algorithm is a complex mathematical transformation that encrypts or decrypts binary data
 - encryption key
 - symmetric key encryption
 - asymmetric key encryption



Summary

- Systems design is the process of organising and structuring the components of a system to enable the construction of the new system.
- The design encompasses key parts of the system, including its environment, application components, user interfaces, database, and software classes and methods.
- Integrity and security controls are important design elements:
 - Integrity controls operate within a specific system to reject invalid data inputs, prevent unauthorized data outputs, and protect data and programs against accidental or malicious tampering.
 - Security controls cross multiple systems to protect assets of an organisation from all threats, with a primary focus on external threats.