Information Systems

Chapter 3

Building Blocks of Information Security

Basic principle of Information Systems Security

-Sanket Mohan Pandhare

Building Blocks of Information Security

Basic Terms and Definitions

- Encryption
  - Modification of data for security reasons prior to their transmissions so that it is not comprehensible without the decoding method.
- Cipher
  - Cryptographic transformation that operates on characters or bits of data.
- Cryptanalysis/Decryption
  - Methods to break the cipher so that encrypted message can be read.

Building Blocks of Information Security

- Electronic Signature
  - Process that operates on a message to assure message source authenticity, integrity and non-repudiation.
- Non-Repudiation
  - Methods by which the transmitted data is tagged with sender's identity as a proof so neither can deny the transmission.
- Steganography
  - Method of hiding the existence of data. The bit map images are regularly used to transmit hidden messages.

Building Blocks of Information Security

- Identification
  - It is a method by which a user claims his identity to a system.
- Authentication
  - It is the method by which a system verifies the identity of a user or another system
- Accountability
  - It is the method by which a system tracks the actions performed by a user or a process.
- Authorization
  - It is a method by which a system grants certain permissions to a user.
- Privacy
  - It is protection on individual data and information.

Building Blocks of Information Security

Terms for Information Classification

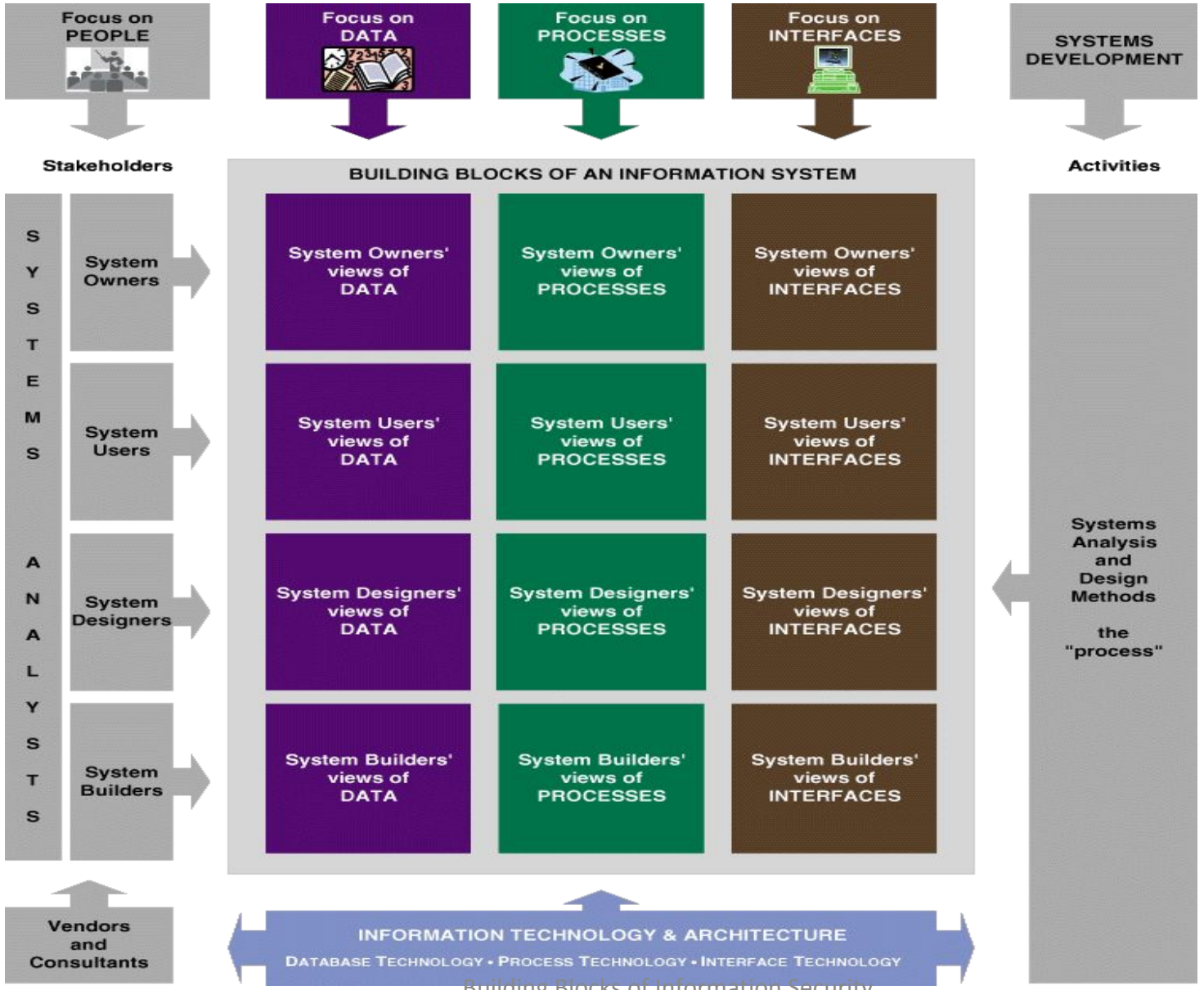
- Unclassified
  - Not so important information. Can be disclosed to public.
- Sensitive but unclassified
  - Information is somewhat important but if disclosed to public will not cause any damage.
- Confidential
  - Unauthorized disclosure may cause some damage.
- Secret
  - Unauthorized disclosure may cause serious damage.
- Top secret
  - Unauthorized disclosure may cause vary serious damage.

Building Blocks of Information Security

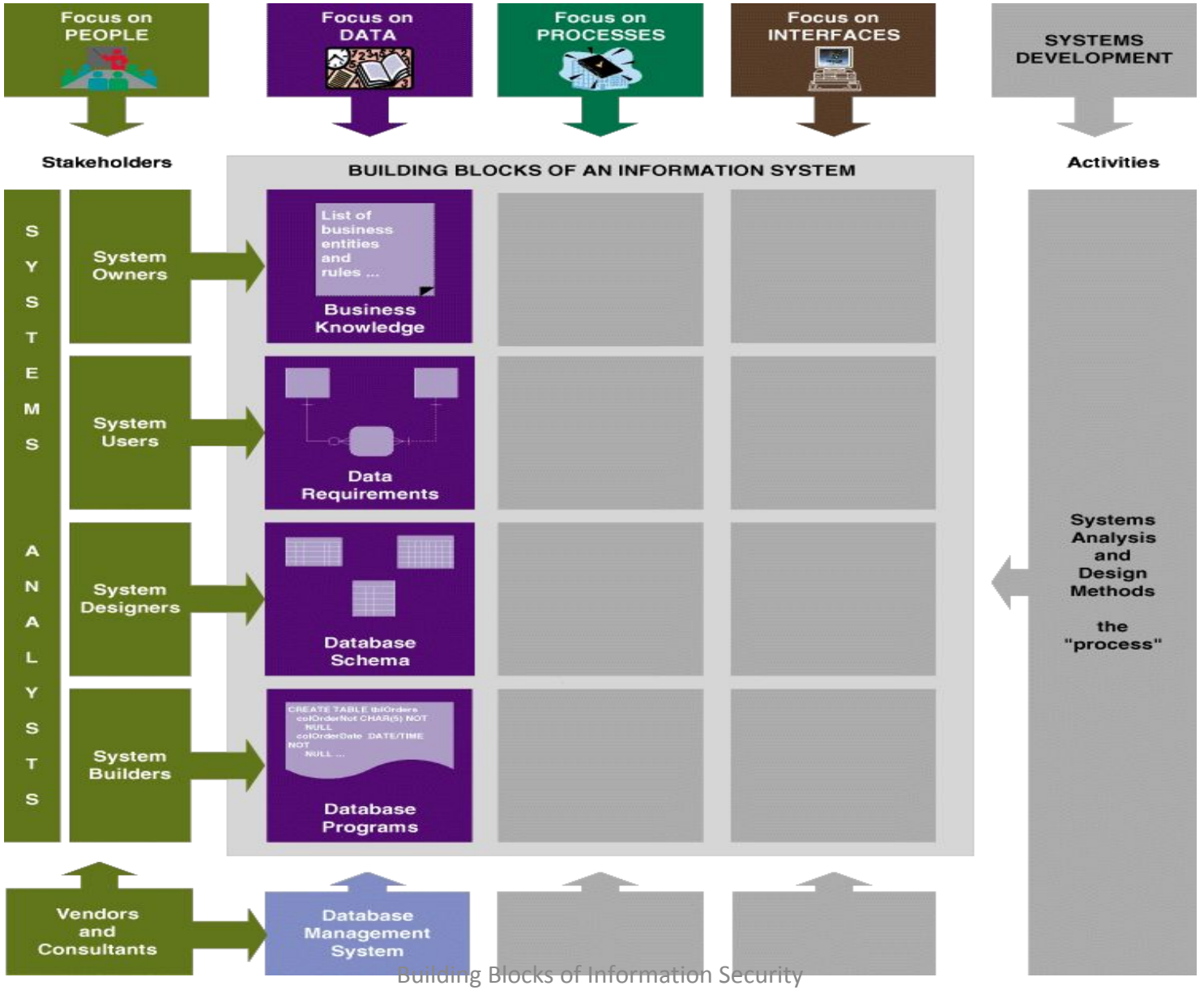
- How ever some organizations classify information as
  - Public
  - Sensitive
  - Private

- Following criteria are used to determine the classification of information
  - Value
  - Age
  - Useful Life
  - Personal Association

Information system building blocks



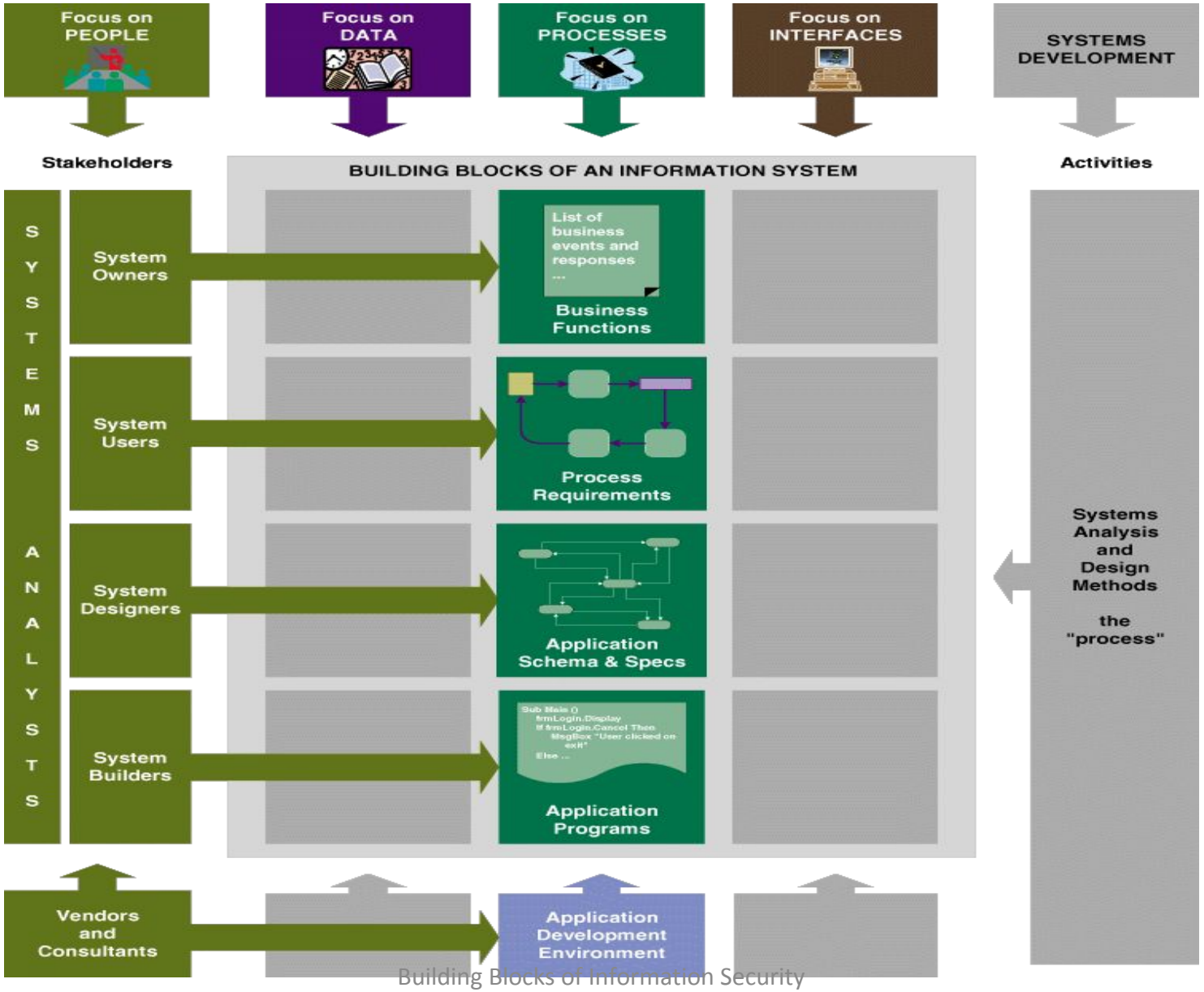
Data focus


Focus on PEOPLE
Focus on DATA
Focus on PROCESSES
Focus on INTERFACES
SYSTEMS DEVELOPMENT
Stakeholders
BUILDING BLOCKS OF AN INFORMATION SYSTEM
Activities
SYSTEMS ANALYSTS
System Owners
System Users
System Designers
System Builders
List of business entities and rules ...
Business Knowledge
Data Requirements
Database Schema
CREATE TABLE tblOrders colOrderNot CHAR(5) NOT NULL colOrderDate DATE/TIME NOT NULL ...
Database Programs
Systems Analysis and Design Methods
the "process"
Vendors and Consultants
Database Management System

Data focus

- System owners' perspective
  - **Business knowledge** is the insight that is gained from timely, accurate, and relevant information. (Recall that information is a product of raw data.)
- System users' perspective
  - **Data requirements** are a representation of users' data in terms of entities, attributes, relationships, and rules. Data requirements should be expressed in a format that is independent of the technology that can or will be used to store the data.
- System designers' perspective
  - **Database schema**
- System builders' perspective
  - **Database management system**

Process focus



Process focus

- System owners' perspective
  - **Business functions** are ongoing activities that support the business. Functions can be decomposed into other subfunctions and eventually into processes that do specific tasks.
  - A **cross-functional information system** supports relevant business processes from several business functions without regard to traditional organizational boundaries such as divisions, departments, centers, and offices.

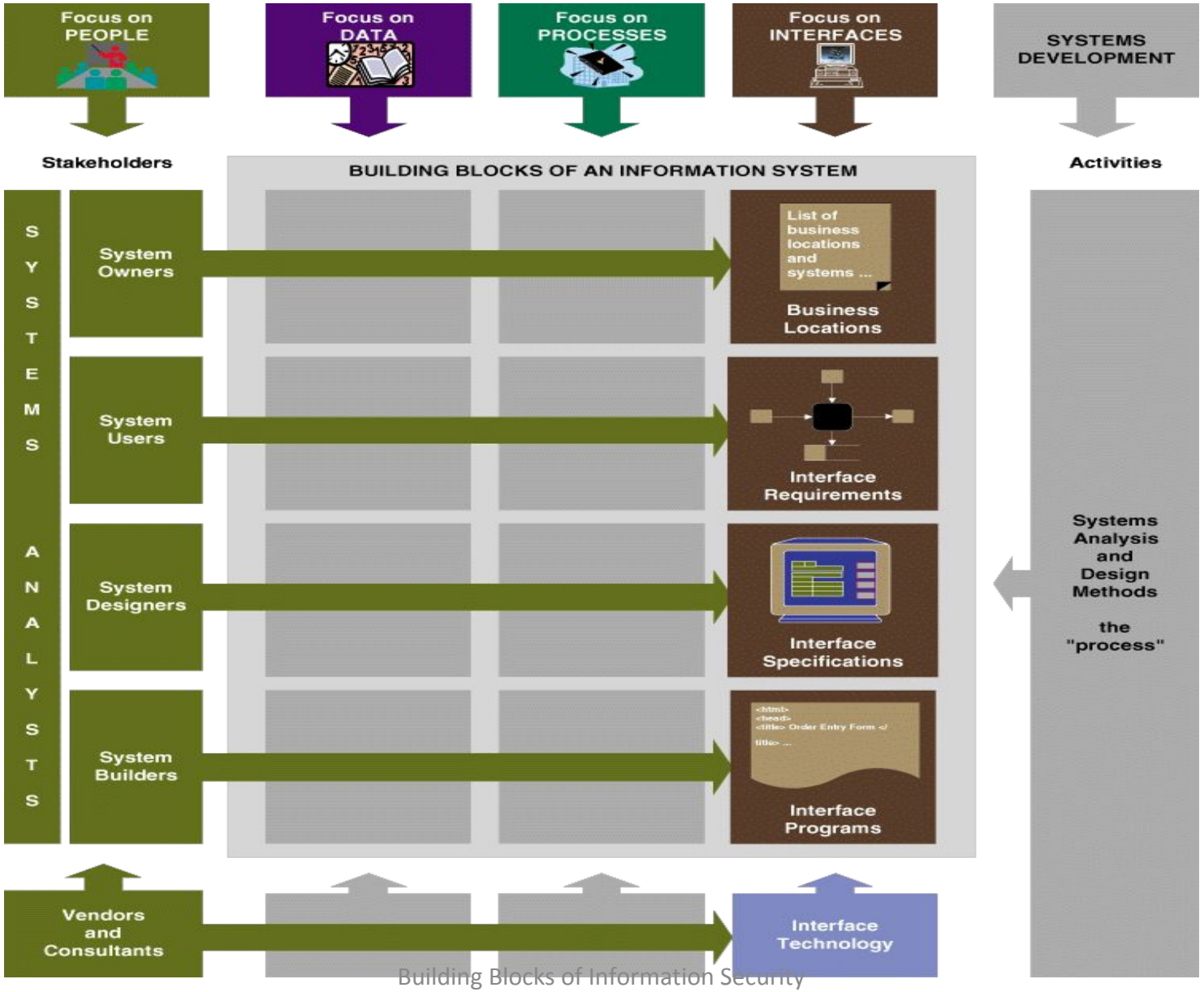
Process focus (Cont'd)

- System users' perspectives
  - **Business processes** are activities that respond to business events. Business processes are the "work" performed by the system.
  - **Process requirements** are a representation of the users' business processes in terms of activities, data flows, or work flow.
  - A **policy** is a set of rules that govern a business process.
  - A **procedure** is a step-by-step set of instructions and logic for accomplishing a business process.

Process focus (Cont'd

- System designers' perspectives
  - An **application schema** is a model that communicates how selected business processes are, or will be, implemented using the software and hardware.
  - **Software specifications** represent the technical design of business processes to be automated or supported by computer programs to be written by system builders.
- System builders' perspectives
  - **Application programs** are language-based, machine-readable representations of what a software process is supposed to do, or how a software process is supposed to accomplish its task.
  - **Prototyping** is a technique for quickly building a functioning, but incomplete model of the information system using rapid application development tools.

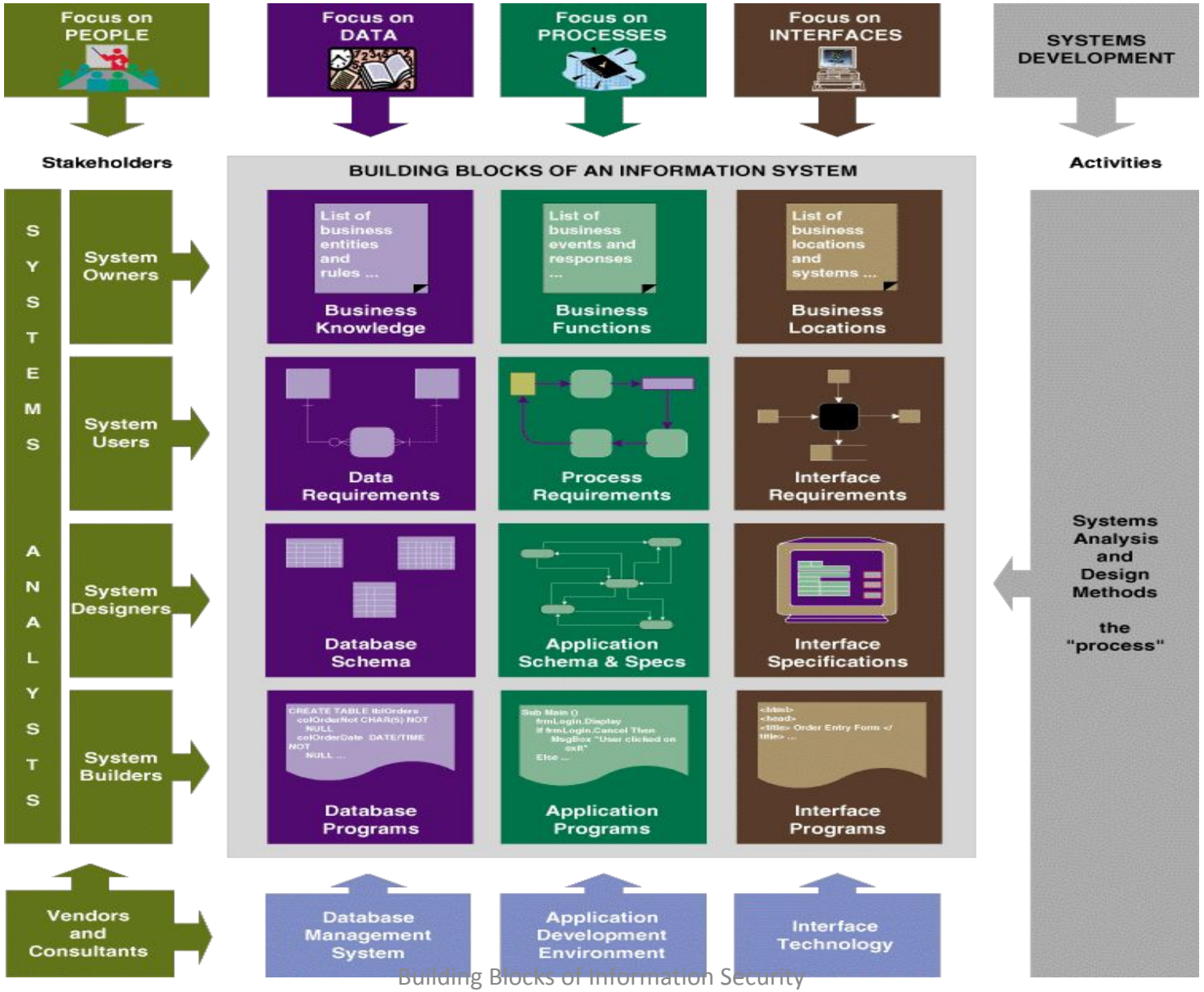
Interface focus



Interface focus

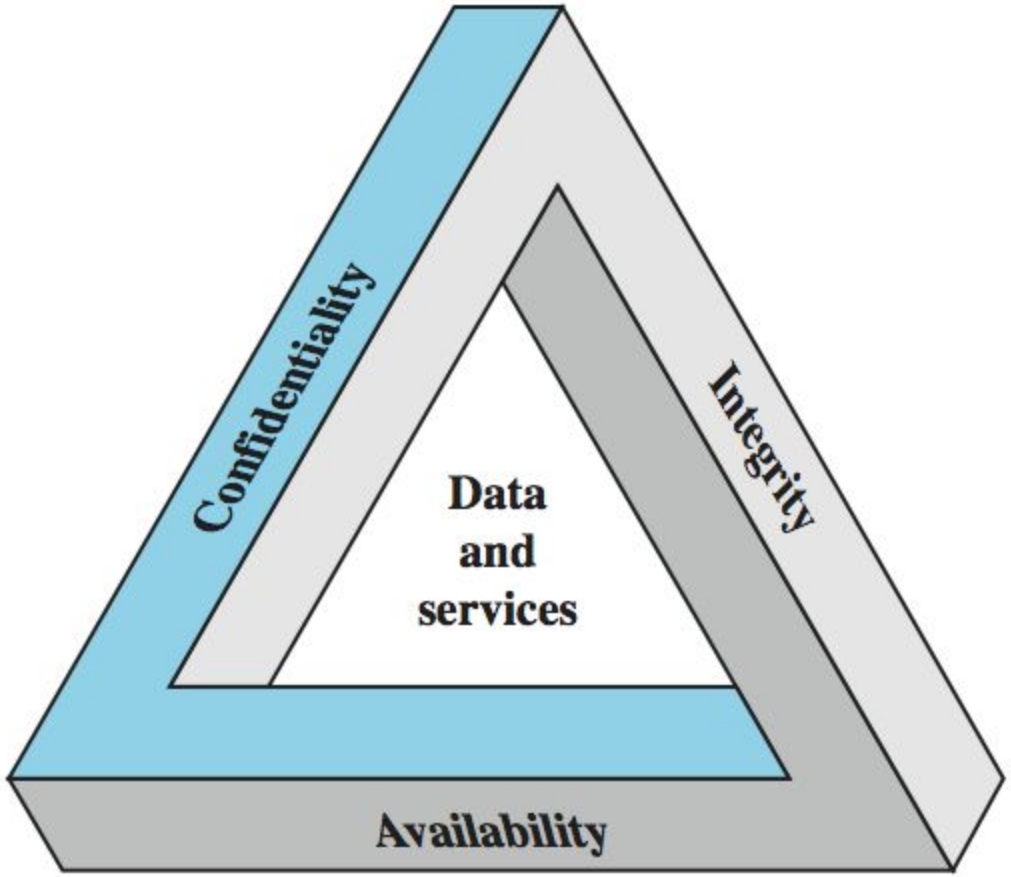
- System owners' perspective
  - List of different business locations & integrated reporting
- System users' perspectives
  - **Interface requirements** are a representation of the users' inputs and outputs.
- System designers' perspective
  - **User dialogues** describe how the user moves from window-to-window, interacting with the application programs to perform useful work.
- System builders' perspective
  - Developing interface of programs.

Information system building blocks



Basic principle of Information Systems Security

- Information security is aimed at protecting the company's digital assets against the ever-growing cyber-attacks.
- Information security can be ensured by deploying appropriate security controls to provide several security features such as prevention, and detection and correction of computer abuse.
- The main purpose of Information Security is to ensure **Confidentiality, Integrity, and Availability (CIA)** of data. CIA is also known as CIA triad.
- **CIA triad** is essential in Information security as it provides vital security features, helps in avoiding compliance issues, ensures business continuity, and prevents reputational damage to the organization.


Confidentiality
Integrity
Data
and
services
Availability

What Is Confidentiality?

- **Confidentiality** ensures privacy to the sensitive information while it is in transit over a network.
- Some proactive measures must be taken to prevent sensitive data from unauthorized disclosure while making it available only to the intended parties.
- The malicious actors must not intercept the data to use it for nefarious(devilish) purposes.
- There are various implementations which can be incorporated to ensure the confidentiality of data.

What Is Confidentiality?(Cont.)

- Cryptography is the best solution in this regard.
- The encryption mainly ensures the confidentiality of sensitive data.
- It converts the plaintext of data into the cipher text, which is an unreadable form for humans.
- **Cipher text** can only be understood by the authorized entities.
- **Encryption** involves two vital security controls including Symmetric Encryption and Asymmetric Encryption.
- Use of **Strong passwords** and **Two-way authentication** are some of the other methods to ensure confidentiality.
- In addition, you can also use **Steganography** to hide data into another type of data such as images, audio, or video files.
- Hiding sensitive data in large media files is much difficult to compromise.

Examples of security requirements: Confidentiality

- Student grade information is an asset whose confidentiality is considered to be very high
- Student enrollment information: may have moderate confidentiality rating; less damage if enclosed
- Directory information: low confidentiality rating; often available publicly

What Is Integrity?

- **Integrity** refers to preventing data from being tampered with, modified, or altered in an unauthorized way to achieve malicious goals.
- That means data which is sent must be received intact and unaltered by an authorized party.
- Integrity is essential for data whether it is in transit or it is in a storage media.
- **Data integrity** is crucial for E-commerce and business websites.
- Various attacks that compromise data integrity include a Man-In-the-Middle (MITM) attack, penetrating into the web server, and introducing malicious code in databases.

What Is Integrity?(Cont.)

- Use of **Hashing Algorithms** such as MD5 and SHA1 are normally provided by developers in order to check the integrity of data.
- Other techniques include **certificates**, **digital signatures**, and **non-repudiation**

Examples of security requirements: Integrity

- A hospital patient's allergy information (high integrity data): a doctor should be able to trust that the info is correct and current
  - If a nurse deliberately falsifies the data, the database should be restored to a trusted basis and the falsified information traced back to the person who did it
- An online newsgroup registration data: moderate level of integrity
- An example of low integrity requirement: anonymous online poll (inaccuracy is well understood)

What Is Availability?

- **Availability** is also a security service which ensures the constant availability of resources and services to only authorized parties in a timely manner.
- Reliable hardware must be maintained in order to provide constant services to a large number of customers in any organization.
- There must be less downtime during upgrades and backup of sensitive data in external drives will be helpful in case of data loss.

What Is Availability?(Cont.)

- Quick disaster recovery plans should be followed in worst case scenarios.
- Other important security controls for availability include **data backup**, **patching**, and redundant systems.
- **Redundancy** ensures **fault tolerance**.
- It means, when a primary system fails to perform, the secondary machine is available to continue the delivery of functions and services.
- In this case, security analysts redirect all traffic or workload to a backup system

Examples of security requirements: Availability

- A system that provides authentication: high availability requirement
  - If customers cannot access resources, the loss of services could result in financial loss
- A public website for a university: a moderate availably requirement; not critical but causes embarrassment
- An online telephone directory lookup: a low availability requirement because unavailability is mostly annoyance (there are alternative sources)

Importance of CIA Triad in Information Security

- Security breaches and Data thefts are becoming headaches in businesses nowadays.
- The recent data breach scandal of Facebook is on the limelight where the private data of millions of users were compromised.
- Most companies have unprotected data due to poor policies that could result in data breaches and massive penalties due to compliance issues such as that of **GDPR – General Data Protection Regulation**.

Summary

- Information System building blocks
  - Multiple stakeholder interact with DATA, Processes and Interfaces in order to develop Information System.

- CIA Triad