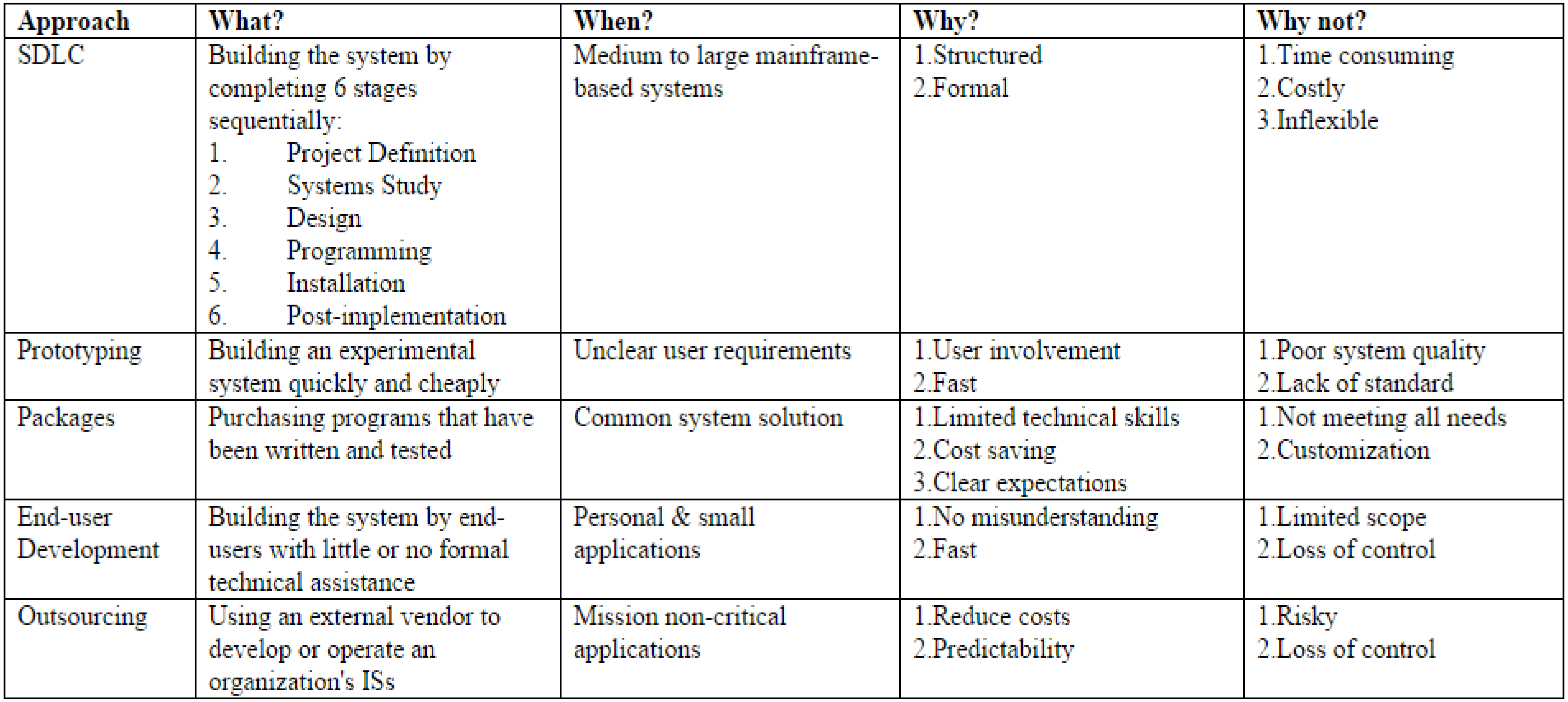
UNIT 3

Developing Secure Information Systems



Approach	What?	When?	Why?	Why not?
SDLC	Building the system by completing 6 stages sequentially: 1. Project Definition 2. Systems Study 3. Design 4. Programming 5. Installation 6. Post-implementation	Medium to large mainframe-based systems	1.Structured 2.Formal	1.Time consuming 2.Costly 3.Inflexible
Prototyping	Building an experimental system quickly and cheaply	Unclear user requirements	1.User involvement 2.Fast	1.Poor system quality 2.Lack of standard
Packages	Purchasing programs that have been written and tested	Common system solution	1.Limited technical skills 2.Cost saving 3.Clear expectations	1.Not meeting all needs 2.Customization
End-user Development	Building the system by end-users with little or no formal technical assistance	Personal & small applications	1.No misunderstanding 2.Fast	1.Limited scope 2.Loss of control
Outsourcing	Using an external vendor to develop or operate an organization's ISs	Mission non-critical applications	1.Reduce costs 2.Predictability	1.Risky 2.Loss of control

Application Development Security

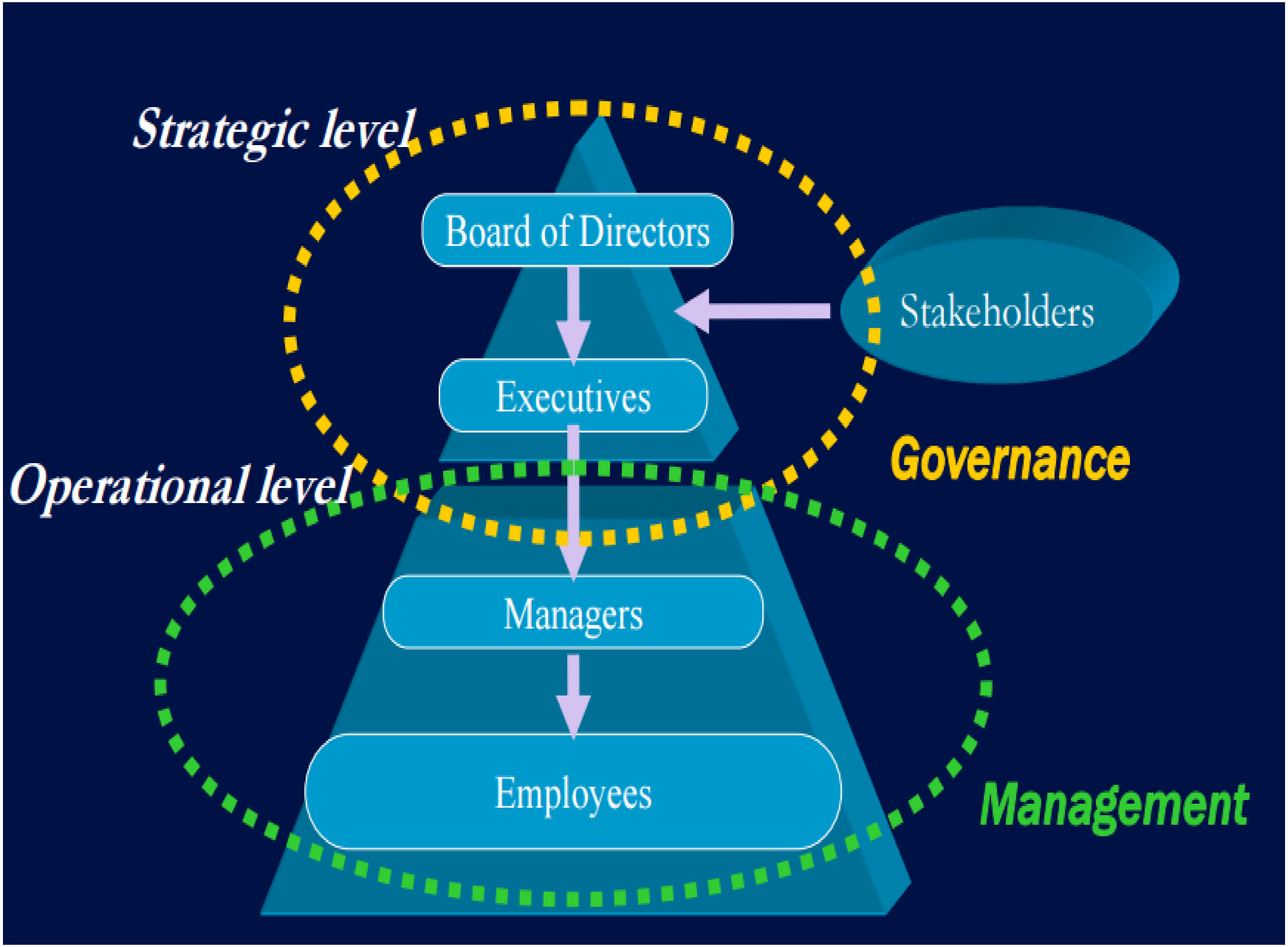
- **Protect the Brand Your Customers Trust.**Security breaches diminish customer confidence in your brand. At all times, keep in mind that your organization has an obligation to protect itself and its customers from cybercriminals.
- **Know Your Business and Support it with Secure Solutions.**Technical knowledge is not enough. To identify potential security risks, regulatory requirements, and training needs, you need to know your business inside and out.
- **Understand the Technology of the Software.** Whether building software in-house or buying software from a vendor, you must understand the technology underlying both the software and the existing infrastructure to be sure they are integrated securely.
- **Ensure Compliance to Governance, Regulations, and Privacy.** You must have a thorough and up-to-date understanding of the internal and external policies that govern the business.
- **Know the Basic Tenets of Software Security.** You must be familiar with the basics of software security: confidentiality, integrity, availability, authentication, authorization, auditing, and the management of configuration, sessions, and exceptions. For example, encryption can help to maintain confidentiality, while proper load-balancing can ensure availability.

Application Development Security

- **Ensure the Protection of Sensitive Information.** Sensitive information is any information that is of measurable value to your organization. Sensitive information must be correctly classified so it can be properly controlled and secured.
- **Design Software with Secure Features.** Many software security problems are not code-related, but are introduced during the design stage. When designing the software, use threat models and abuse case modeling to identify security threats.
- **Develop Software with Secure Features.** The security controls you design must be implemented properly. Perform security code reviews and security testing.
- **Deploy Software with Secure Features.** Stay on top of change management, making sure the test environment always reflects the production environment. Prevent regenerative bugs by managing software releases correctly. Perform vulnerability and penetration testing before deploying new software.
- **Educate Yourself and Others on How to Build Secure Software.** These days, the norm for software development is "release and patch": an unsatisfactory approach. A cultural change is needed, and that can only happen when people are educated about the importance of security.

Information Security Governance

- The set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organization's immediate and future regulatory, legal, risk, environmental and operational requirements.
- *Guidance for Information Security Managers* discusses how to develop an information security strategy within the organization’s governance framework and how to drive that strategy through an information security program.
- It provides guidance on determining information security objectives and how to measure progress toward achieving them.
- It is an exposition on the rationale and necessity for senior management to integrate information security into overall organizational governance at the highest levels.
- It provides information developed in recent years that mandates the business case for information security governance.


Strategic level
Board of Directors
Stakeholders
Executives
Governance
Operational level
Managers
Employees
Management

Risk Management

- Risk management is the process of identifying vulnerabilities in an organization’s information systems and taking carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in the organization’s information systems
- The primary deliverable from risk assessment was a list of documented vulnerabilities, ranked by criticality of impact

Risk Control Strategies

- When risks from information security threats are creating a competitive disadvantage, the information technology and information security communities of interest take control of the risks
- Four basic strategies are used to control the risks that result from vulnerabilities:
  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce the impact (mitigation)
  - Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

Avoidance

- Avoidance attempts to prevent the exploitation of the vulnerability
- This is the preferred approach, as it seeks to avoid risk in its entirety rather than dealing with it after it has been realized
- Accomplished through countering threats, removing vulnerabilities in assets, limiting access to assets, and/or adding protective safeguards
- Three areas of control:
  - Policy
  - Training and education
  - Technology

Security Architecture and Design

- Security Architecture and Design describes fundamental logical hardware, operating system, and software security components, and how to use those components to design, architect, and evaluate secure computer systems. Understanding these fundamental issues is critical for an information security professional. Security Architecture and Design is a three-part domain. The first part covers the hardware and software required to have a secure computer system. The second part covers the logical models required to keep the system secure, and the third part covers evaluation models that quantify how secure the system really is.

Security Issues in Hardware

- ***Site security***

You should check the physical security of your premises, concentrating on access through windows and doors. You can improve the physical security of desktop PCs by using devices such as metal cages and anchoring devices, making them more difficult to remove. Employees should also not allow building access to delivery personnel or other visitors but have them ring through to reception staff or other designated person.

- ***Laptop security***

Laptops should always be equipped with security cables and securely locked away when not in use. Docking stations should lock them firmly in place when on the desk. Mobile workers should be particularly careful not to leave their laptops in their cars or in other exposed places. Laptop users should ensure they choose secure passwords - ideally a random collection of letters and numbers. Users should also change their passwords regularly.

Security Issues in Software

- Since the number of threats specifically targeting software is increasing, the security of our software that we produce or procure must be assured. "Dependence on information technology makes software assurance a key element of business continuity, national security, and homeland security."

- **Non-conformance, or a failure to satisfy requirements**

A non-conformance may be simple–the most common is a coding error or defect–or more complex (i.e., a subtle timing error or input validation error). The important point about non-conformance is that verification and validation techniques are designed to detect them and security assurance techniques are designed to prevent them. Improvements in these methods, through a software security assurance program, can improve the security of software.

- **Errors or omissions in software requirements**

The most serious security problems with software-based systems are those that develop when the software requirements are incorrect, inappropriate, or incomplete for the system situation. Unfortunately, errors or omissions in requirements are more difficult to identify. For example, the software may perform exactly as required under normal use, but the requirements may not correctly deal with some system state. When the system enters this problem state, unexpected and undesirable behavior may result. This type of problem cannot be handled within the software discipline; it results from a failure of the system and software engineering processes which developed and allocated the system requirements to the software.

Security Issues in data storage

- Data storage security is a wide-ranging area that covers everything from legal compliance, through preparedness for e-discovery requests to user access control and the physical security of data storage.

Dimension	Security Issues
Physical	Your computers must be physically inaccessible to unauthorized users. This means that you must keep them in a secure physical environment.
Personnel	The people responsible for system administration and data security at your site must be reliable. You may need to perform background checks on DBAs before making hiring decisions.
Procedural	The procedures used in the operation of your system must assure reliable data. For example, one person might be responsible for database backups. Her only role is to be sure the database is up and running. Another person might be responsible for generating application reports involving payroll or sales data. His role is to examine the data and verify its integrity. It may be wise to separate out users' functional roles in data management.
Technical	Storage, access, manipulation, and transmission of data must be safeguarded by technology that enforces your particular information control policies.

Physical Security of IT Assets

- Without paying proper attention to the physical security of information asset your IT assets and infrastructure are always under security threats from known or unknown sources or from accidental hazards.
- An IT security manager or designer will always need to pay equal or even more attention to ensure that his all the information assets are physically secured.
- It is not necessary that all the physical security risk to IT assets can be only from physical break into the IT server or assets room, but there are major risk related to environmental risks such as fire.
- To control the physical security of all IT assets you need to identify all the assets that you consider sensitive and important for your organization.
- The physical security of IT assets can be broadly categorized based on the following criteria:

1. Security of Asset Location
2. Human access control to the security room
3. Environtal control

Access Control

- Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.
- There are two main types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access limits connections to computer networks, system files and data.
- The four main categories of access control are:

  Mandatory access control

  Discretionary access control

  Role-based access control

  Rule-based access control
- Access control systems perform authorization identification,authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

CCTV

- **Closed-circuit television** (**CCTV**), also known as **video surveillance**, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores. Videotelephony is seldom called "CCTV" but the use of video in distance education, where it is an important tool, is often so called.

Intrusion Detection Systems

- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
- The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security.

Categories of IDS

- **misuse detection** vs. **anomaly detection**: in misuse detection, the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the networks traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.
- **network-based** vs. **host-based systems**: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.
- **passive system** vs. **reactive system**: in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Backup Security Measures

- Backups should be performed locally to an external media like an external hard drive or DVD.
- Local backups need to be stored away from the computer, preferably to another location in case of fire or flooding.
- Online backups should be performed on a regular basis so important files can be accessed from other devices even if the backed up PC is no longer available
- Computer security is another very important and often overlooked aspect of healthy computing. Virus protection software is the easiest protection from viruses but there are so many more security issues that virus software alone will not defend against that could easily make your PC quite worthless. A total protection suite of security applications is the recommended solution for full protection. While there are many programs available to accomplish total PC security, only a few are worth mentioning. We will explore and review the different backup and security programs and point out the good and the bad of each application. It is up to you to decide which is the correct solution for your scenario.