# DLE 2083: INTRODUCTION TO SECURITY MANAGEMENT

## CHAPTER 5

## TARGET, VULNERABILITY AND EXPOSURE

VISION COLLEGE

# Chapter 5: Learning Outcomes

- At the end of the topic, students should be able to:
  - Describe what is meant by target, vulnerability, and exposure.
  - Defines security program and it's important to organization
  - Understand the basic concept of defense in depth.
  - Identify the layers of security functions and features.
  - Identify the components of security program.

VISION COLLEGE

# Defining Target

- A **target** is the **object** of a risk or plan.
- The **threat** is the **subject** whose actions cause harm to the object.

VISION COLLEGE

# Defining Target

- In the semantic frame risk two types of object are routine:
  - a human victim (the individual who stands to suffer if the harm occurs) **OR**
  - a valued possession of the victim

VISION COLLEGE

# Identifying Target

- Identifying targets is a key step in assessing the risks associated with certain threats.
- Analytically, no threat should be identified except in relation to a particular target.
- Targets can be identified by their attractiveness to threats and by their risk factors or indicators.

VISION COLLEGE

# Defining Vulnerability

- Vulnerability essentially means that the target can be harmed by the threat.
  - For example, I would be vulnerable to a threat armed with a weapon that could harm me.
  - The threat would cease if I were to acquire some armour that can protects me from the weapon.

VISION COLLEGE

# Defining Vulnerability

- Vulnerabilities defined as factors that increase an organization's exposure to threats.
- However, vulnerability and exposure are usefully differentiated.
- Basically, vulnerability means that we are undefended against the threat, while exposure means we are subject to the threat.

# Defining Exposure

- Exposure often is treated as synonymous with vulnerability and even risk.
- Exposure implies that we are subject to the threat, while vulnerability implies our lack of defenses against the threat.

RISK = HAZARD x EXPOSURE

VISION COLLEGE

# Exposure by Area

- Someone's exposure to a threat could be defined by the space known to be coincident with that threat.
- For example, crime tends to concentrate in certain areas or sometimes known as hot spots.

VISION COLLEGE

# Exposure by Time

- We are exposed in time whenever the threat is coincident with us or knows where we are and can target us at that time.
- We could measure our exposure in time in either:
  - absolute terms; e.g. we could calculate the time we spend every day travelling by vehicle as a measure of our exposure to road traffic accidents.
  - proportional terms, such as flood season of a year.

VISION COLLEGE

# Security Program

- A set of protection plan of combination between systems and elements from physical actions and events that could cause serious loss or damage to an organization.
- This includes protection from the man-made threats and natural forces. For example; fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

# Layered Security

- Layered security, also known as layered defence, describes the practice of combining multiple mitigating security controls to protect resources and data.

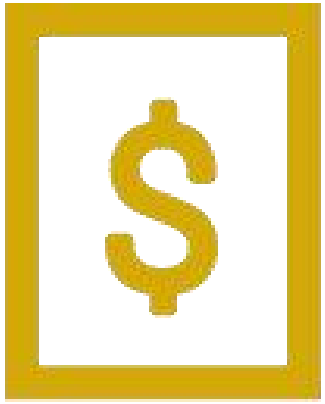
# Layered Security

- The term bears some similarity to defense in depth, a term adopted from a military strategy that involves multiple layers of defense that seeks to delay rather than prevent the advance of an attacker or intruder by yielding space to buy time.

VISION COLLEGE

# Layered Security

- Defence in depth is a protection concept on the organization asset in which multiple layers of security controls (defence) are placed throughout the organization to protect their vital assets.



High Value Assets

VISION COLLEGE

# Layered Security

- In terms of vital asset protection, defence in depth measures should not only prevent security breaches but also buy an organization time to detect and respond to an attack and so reduce and mitigate the consequences of a breach.

VISION COLLEGE

# Defense in depth - Controls

- Defense in depth can be divided into three areas:
  - Physical controls
  - Technical controls
  - Administrative controls

# Defense in depth - Controls

- **Physical controls**
  - Physical controls are anything that physically limits or prevents access to the organization vital assets.
  - Example: perimeter fences, drainage, signage, gates, crossbar, bollards, security guard, canine (K9), CCTV and alarm systems.


VISION COLLEGE





# Defense in depth - Controls

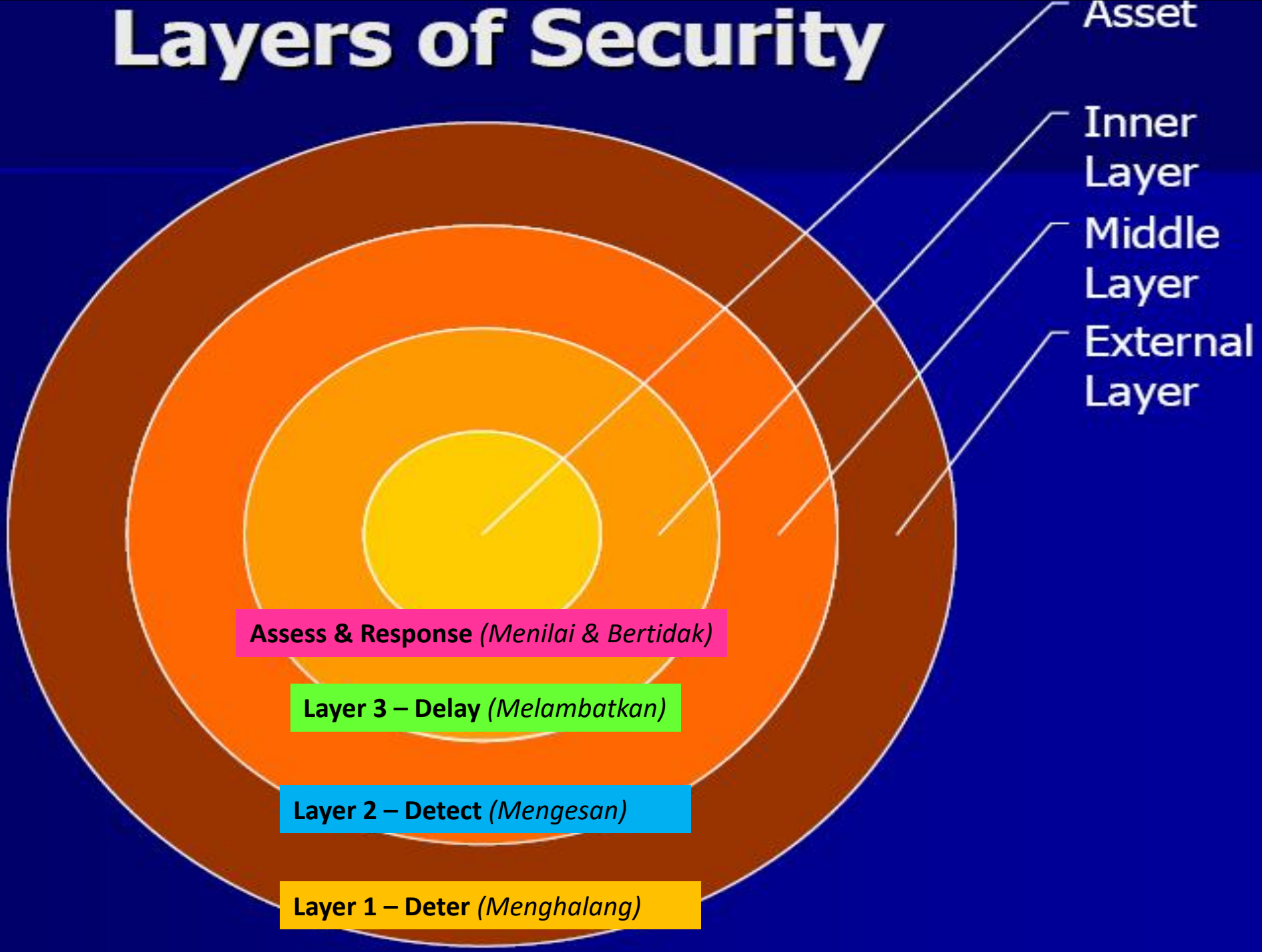
- **Technical controls**
  - Technical controls are hardware or software whose purpose is to protect systems and resources.
  - Examples of technical controls would be access card, fingerprint, biometric, PIN, password, mechanical locks, pad locks, firewall, IDS and etc.

VISION COLLEGE

# Defense in depth - Controls

- **Administrative controls**
  - Administrative controls are an organization's policies and procedures.
  - The purpose is to ensure that there is proper guidance available in regards to security and that regulations are met.
  - These can include such as hiring practices, data handling procedures and security requirements.

# Layers of Security



# Layers of Security: Functions and Features

- **External layer**
  - To **deter** intruders from entering the organization.
  - Examples: security personnel, gate, crossbar, fences, bollard, drainage, lighting system and etc.


VISION COLLEGE

# Layers of Security: Functions and Features

- **Middle layer**
  - To **detect** any intrusion activities.
  - Example: CCTV, alarm system, security patrols, canine (K9), and etc.


VISION COLLEGE

# Layers of Security: Functions and Features

- **Inner layer**
  - To **delay** the intruders movement before reach to organization main asset.
  - Examples: thumb print, eyes scan, body frisking, mantrap with interlocking door system, password, PIN, armed guard, vault room or safe box with combination.

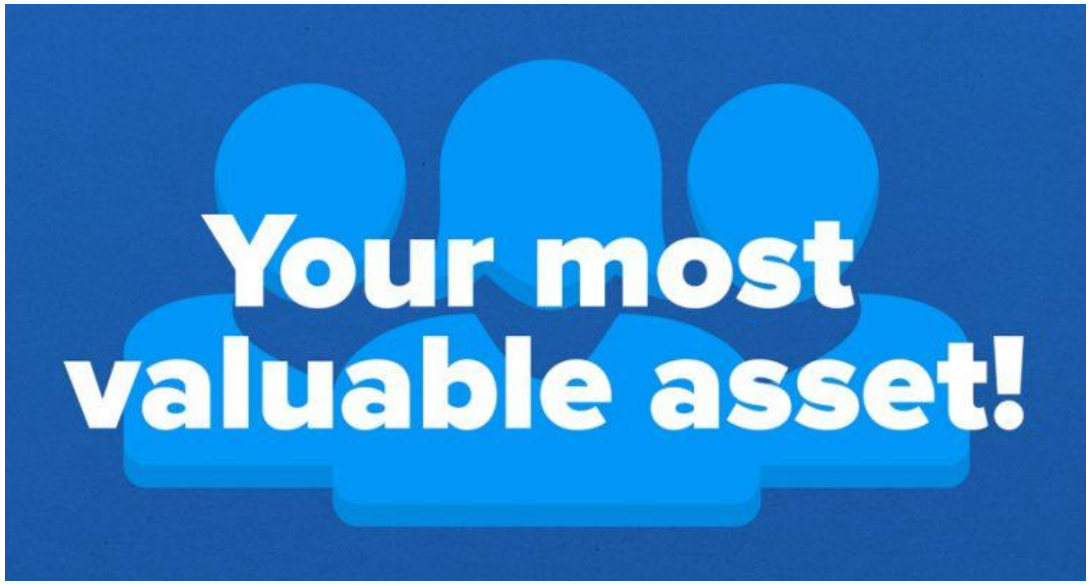

VISION COLLEGE

# Layers of Security: Functions and Features

- **Assess and response**
  - Assess the capability of intruders from all perspective.
  - Response and take necessary action before the intruders get in to the organization main assets.
  - For example, give command to security personnel to make arrest of the intruders or in worse case, call police to handle the situation.

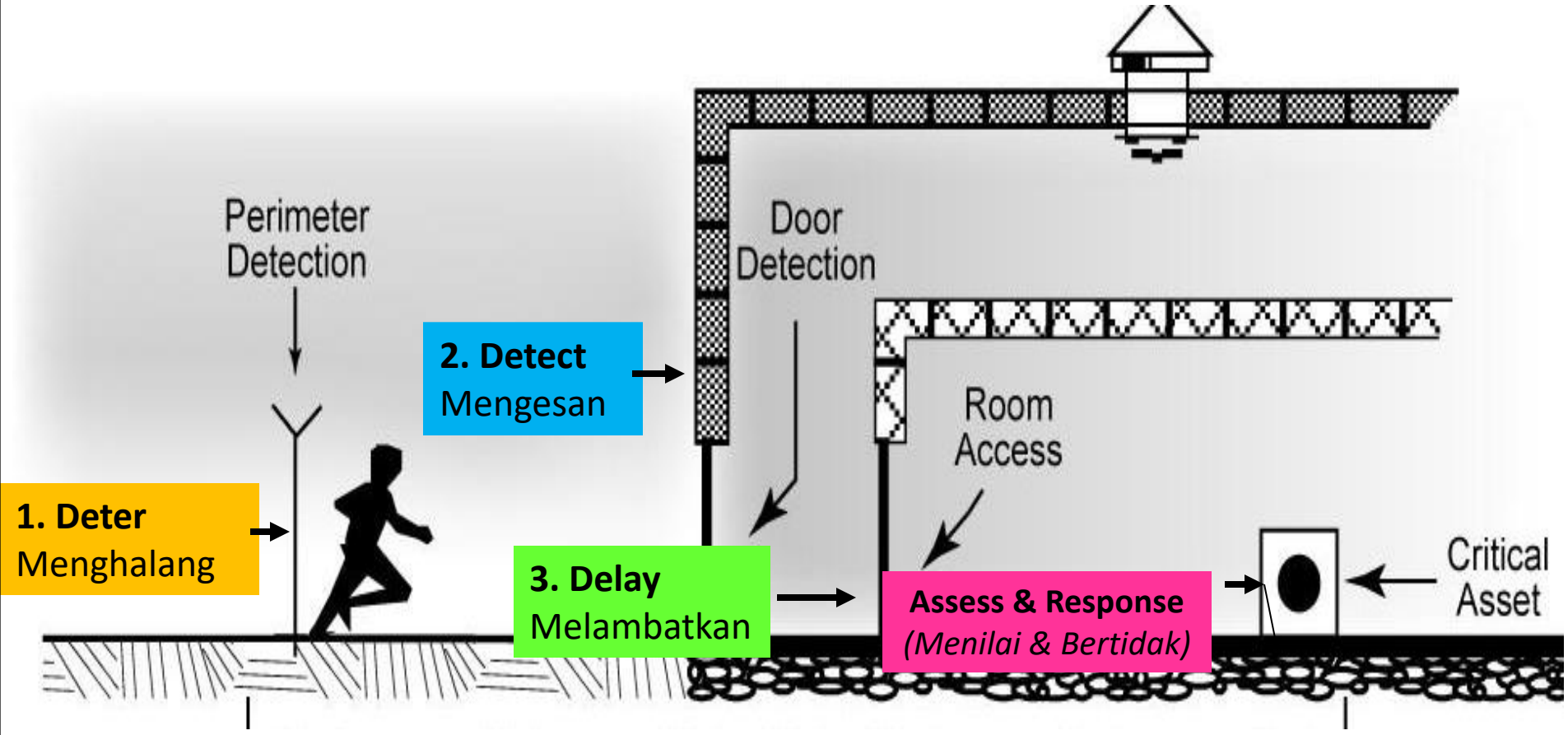
# Layers of Security: Functions and Features

- **Asset**
  - High values of organization assets.
  - Examples: cash, microchips, business strategies plans, gold, diamond, database system, and etc.



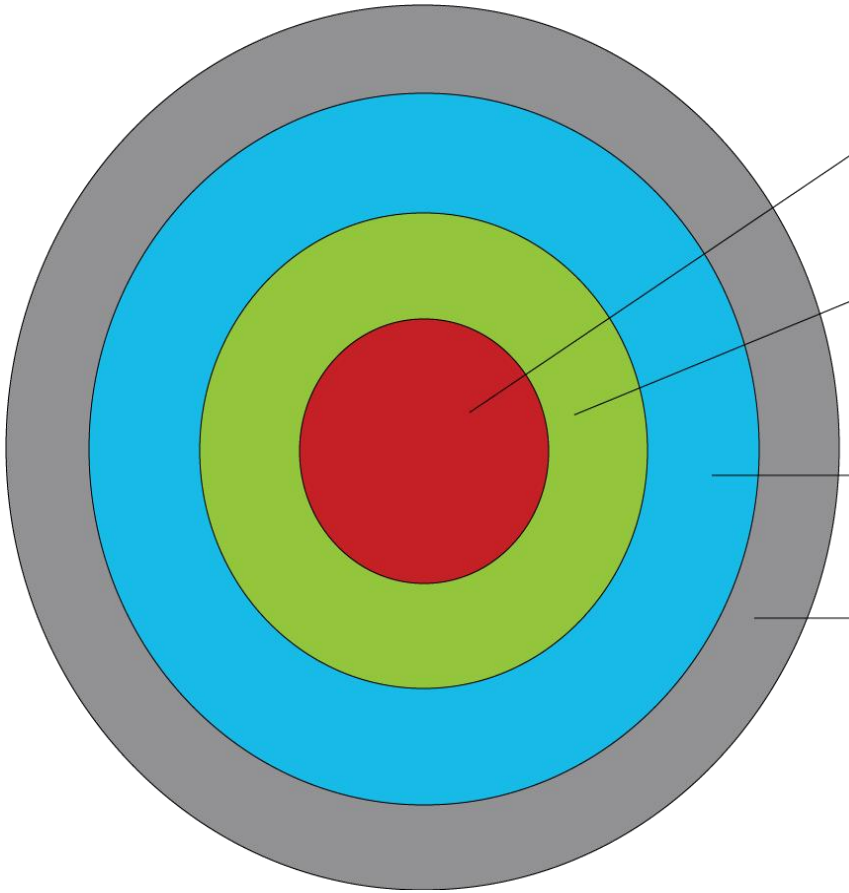

VISION COLLEGE

# Defence in depth concept




VISION COLLEGE

# LAYERED SECURITY FOR DATA CENTER PROTECTION



**Data Center Suite**
Biometric and key card access controls

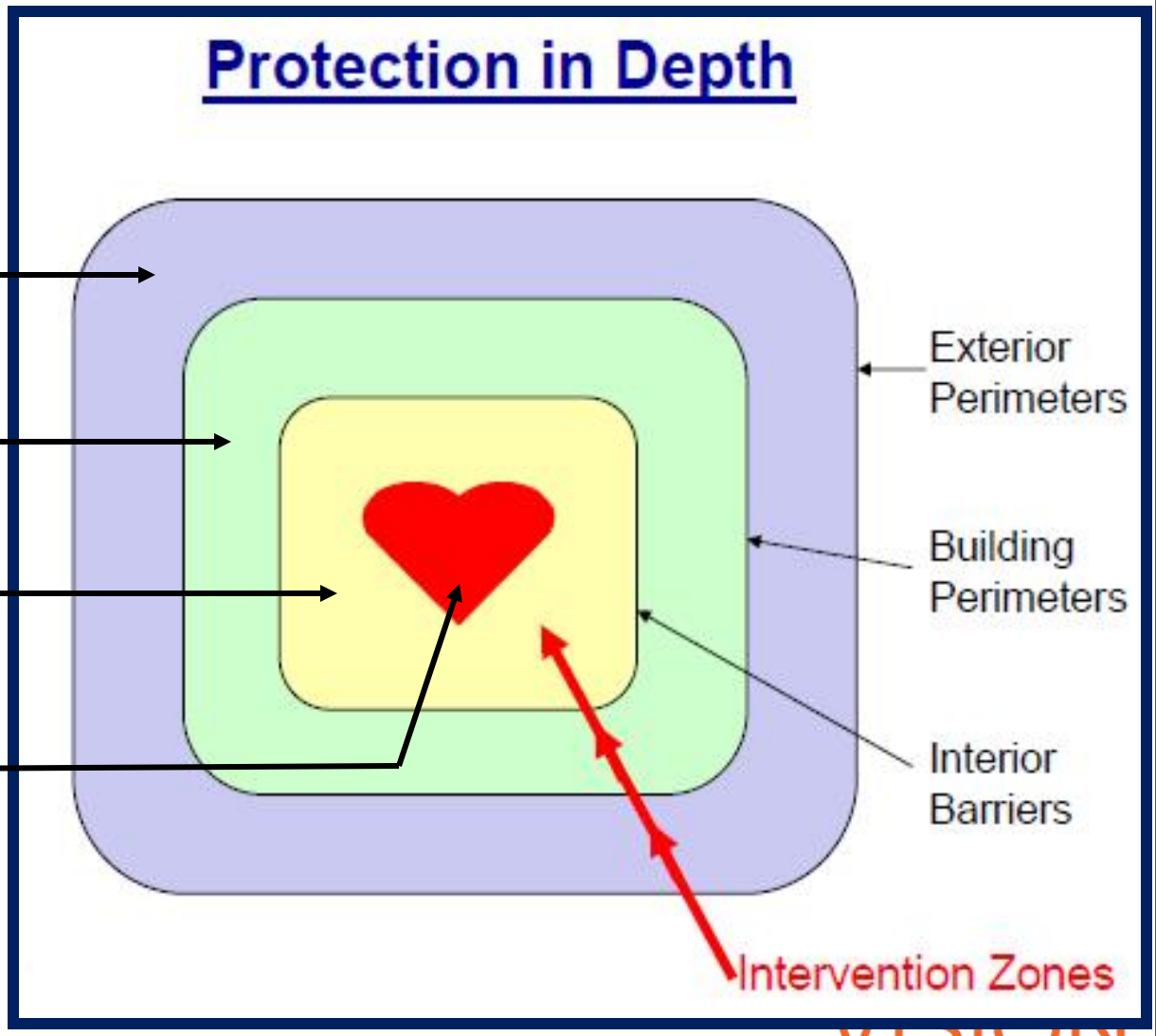
**Building Interior**
Security office, key card access, video surveillance, digital recording and archiving

**Building Perimeter**
Private parking, security patrols

**Site Perimeter**
Perimeter fence, security check-in

VISION COLLEGE

# L A Y E R E D  S E C U R I T Y



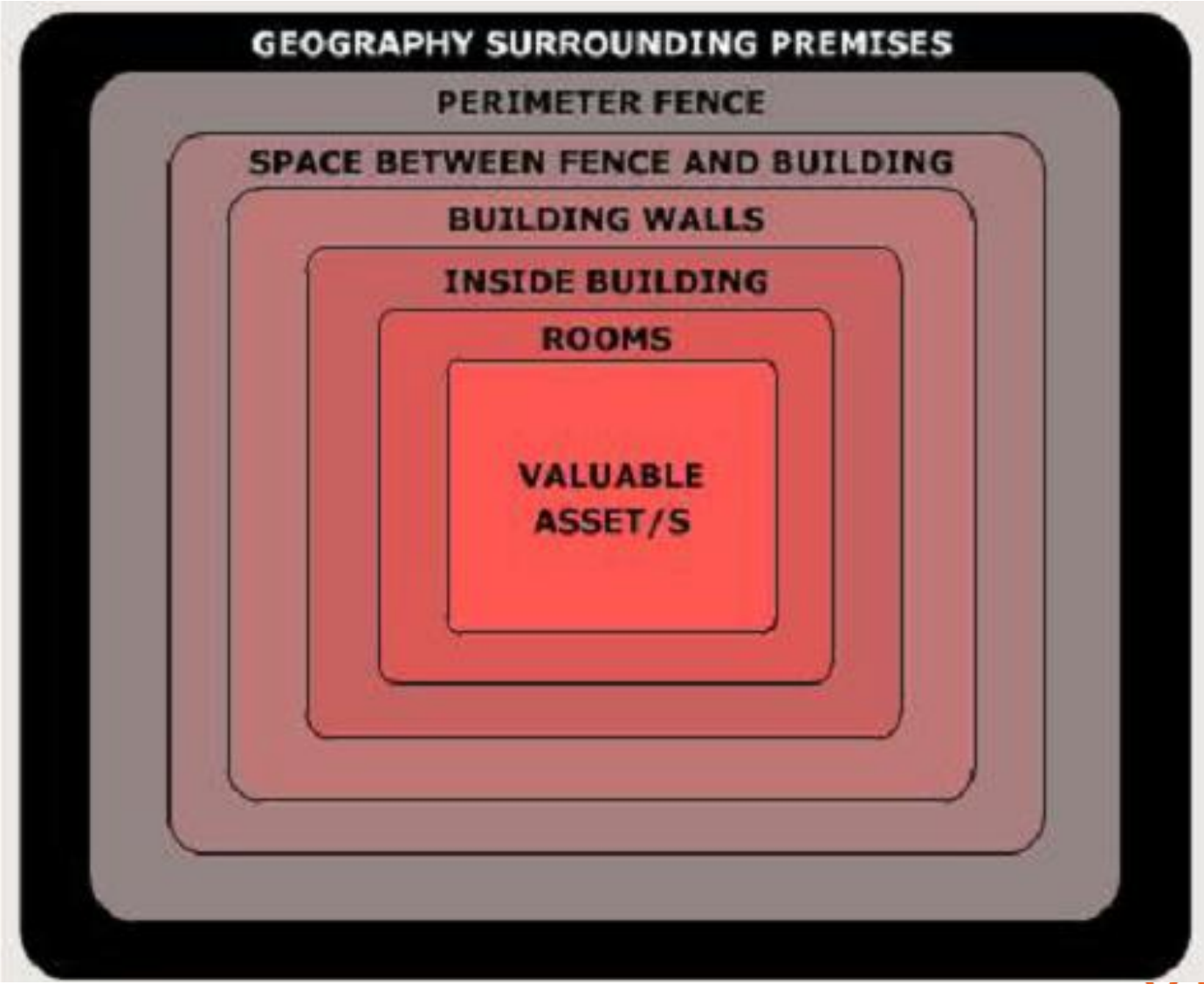

**Public Zone**

**Semi-Public Zone**

**Semi-Private Zone**

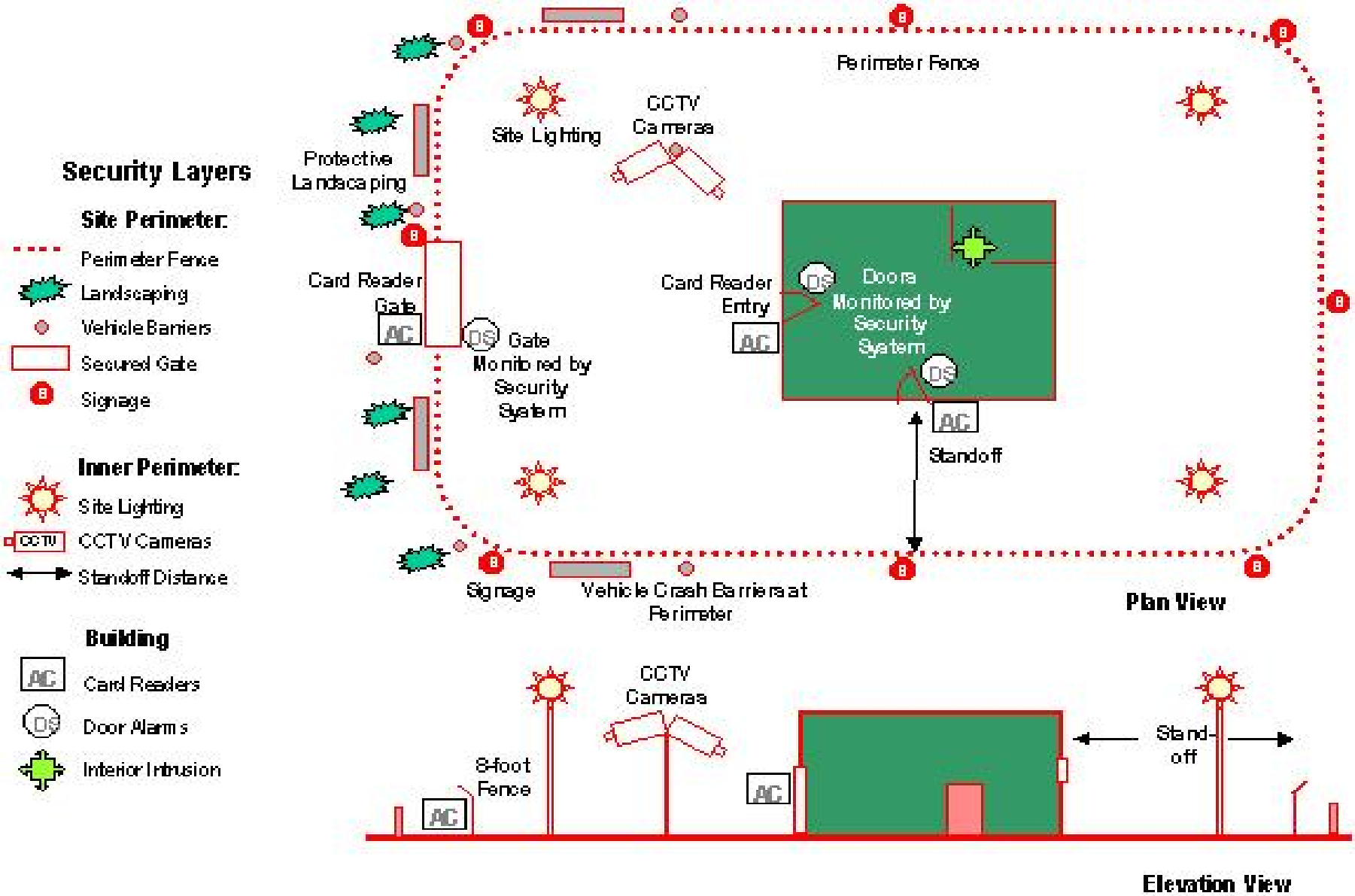
**Private/Exclusive Zone**

# L A Y E R E D  S E C U R I T Y




VISION COLLEGE

# Defense in depth



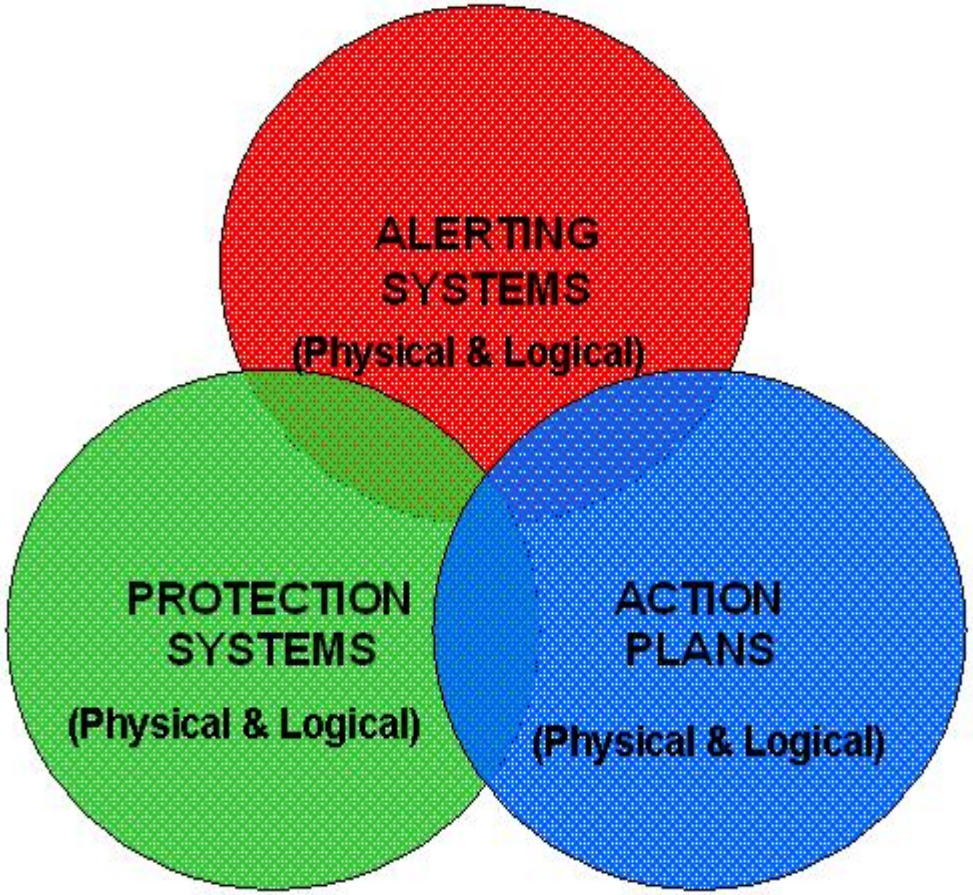
# Security program based on defense in depth concept for warehouse or factory

VISION COLLEGE

# Proposed American Embassy in London


VISION
COLLEGE

# COMPONENTS OF SECURITY PROGRAM




VISION COLLEGE

# COMPONENTS OF SECURITY PROGRAM

## Components of a Typical Security Program

Protection Systems

### Physical Security System

**Architectural features**

- location
- design
- layout

**Physical / Mechanical Systems**

- guardforce ( contract / proprietary
- barrier/lighting
- signages
- canine

Alerting Systems

**Electronic Systems**

- intruder detection system
- surveillance system
- identification credential system
- RFID system

### Logical Security Systems

### Administrative System

**Policies & Procedures**

- administrative controls
- personnel controls
- process controls
- technical controls

**Operational Methodologies (Line Operations)**

- Planning
- Organizing
- Implementing
- Controlling
- Review

Action Plans

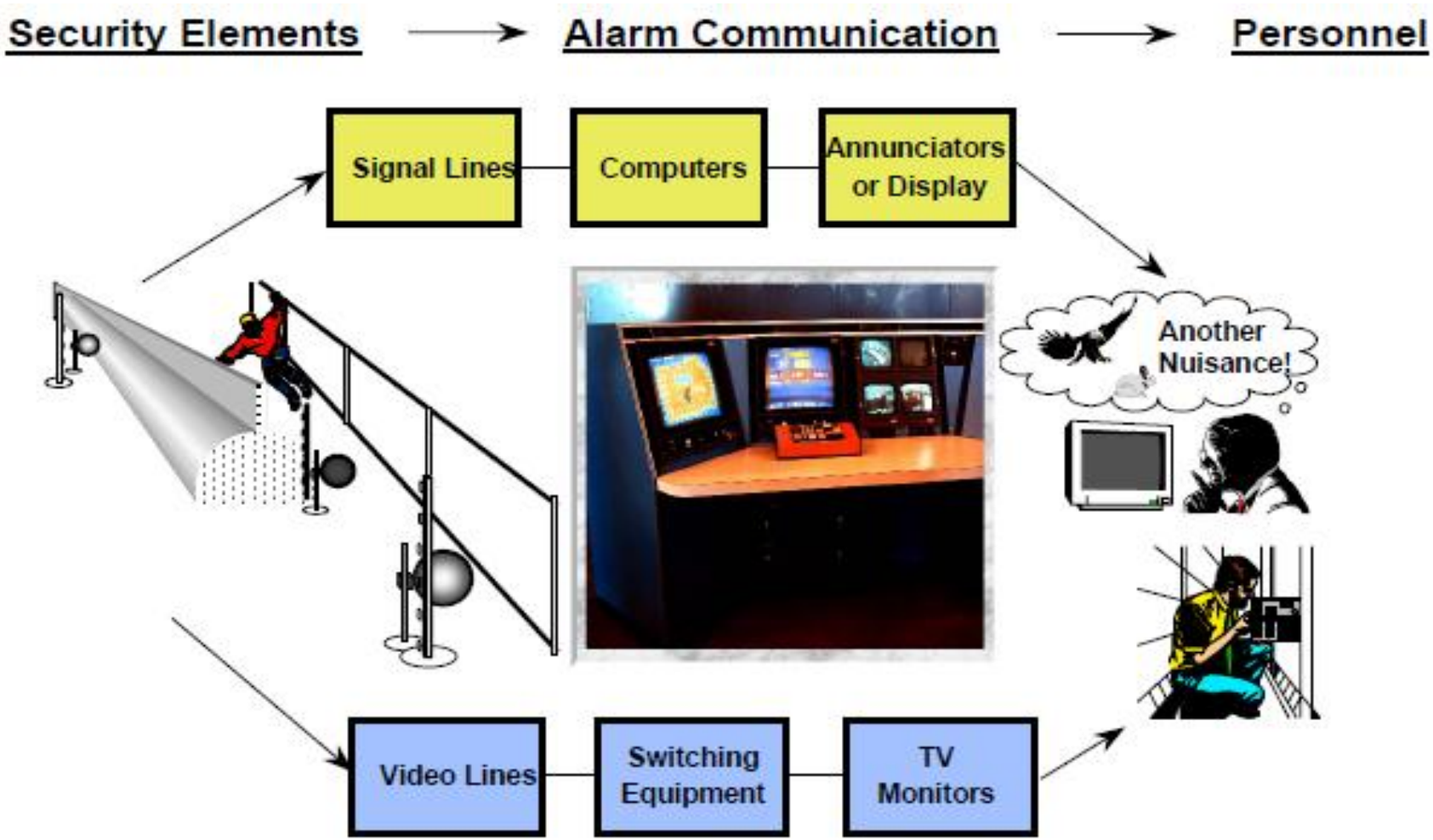
VISION COLLEGE

# Protection Systems

## Physical Security Controls

VISION COLLEGE

# Alerting Systems




VISION COLLEGE

# Action Plans

## A Security Plan: Management Policies

- Steps in developing a security plan:
  - Perform risk assessment – assessment of risks and points of vulnerability
  - Develop security policy – set of statements prioritizing information risks, identifying acceptable risk targets and identifying mechanisms for achieving targets
  - [illegible] nplementation plan – action steps needed to achieve security plan goals
  - Create security organization – in charge of security; educates and trains users, keeps management aware of security issues; administers access controls, authentication procedures and authorization policies
  - Perform security audit – review of security practices and procedures

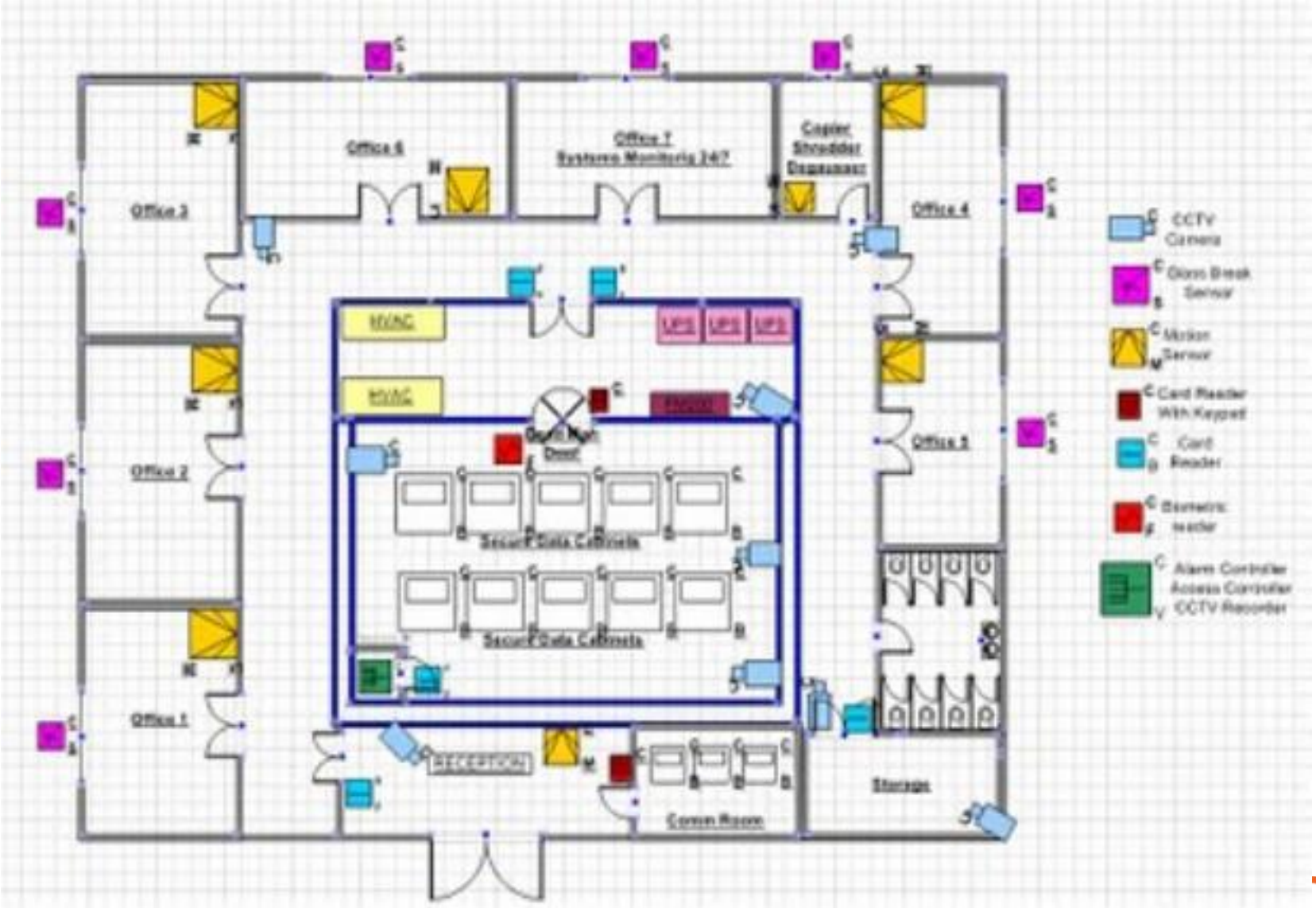
VISION COLLEGE

# Action Plan

- To effectively implement policy guidelines in organizations. There must be appropriate procedures and action plans made available in the organizations.
- Example: Patrolling procedures

VISION COLLEGE

# Protective and Alarm Systems Layout Plan for a Typical Facility




VISION COLLEGE