

Date _____

Day _____

— CHAPTER #14 —

→ IT Security management answers three basic questions

- ① What assets need protection?
- ② What threats exist to those assets?
- ③ How can those threats be countered?

• IT SECURITY MANAGEMENT

↳ A formal process to protect an organization's IT assets

↳ Ensure protection is effective & cost-efficient

↳ Focuses on:

↳ Confidentiality ↳ Availability ↳ Authenticity
↳ Integrity ↳ Accountability ↳ Reliability

→ Main Steps in IT Security Management

① Define security objectives, strategies & policies

② Perform IT Security Risk Assessment

③ Identify threats, & resulting risks

④ Select appropriate security controls

⑤ Write plans & procedure

⑥ Implement controls & provide training

⑦ Monitor & maintain controls

⑧ Detect & respond to security incidents

Date _____

Day _____

→ Risk Assessment Purpose

- Evaluate assets, threats and vulnerabilities
- Determines acceptable vs unacceptable risks
- Helps decide whether to:
 - ↳ Reduce risk
 - ↳ Accept risk

See Fig 14.1

→ IT security management is cyclic

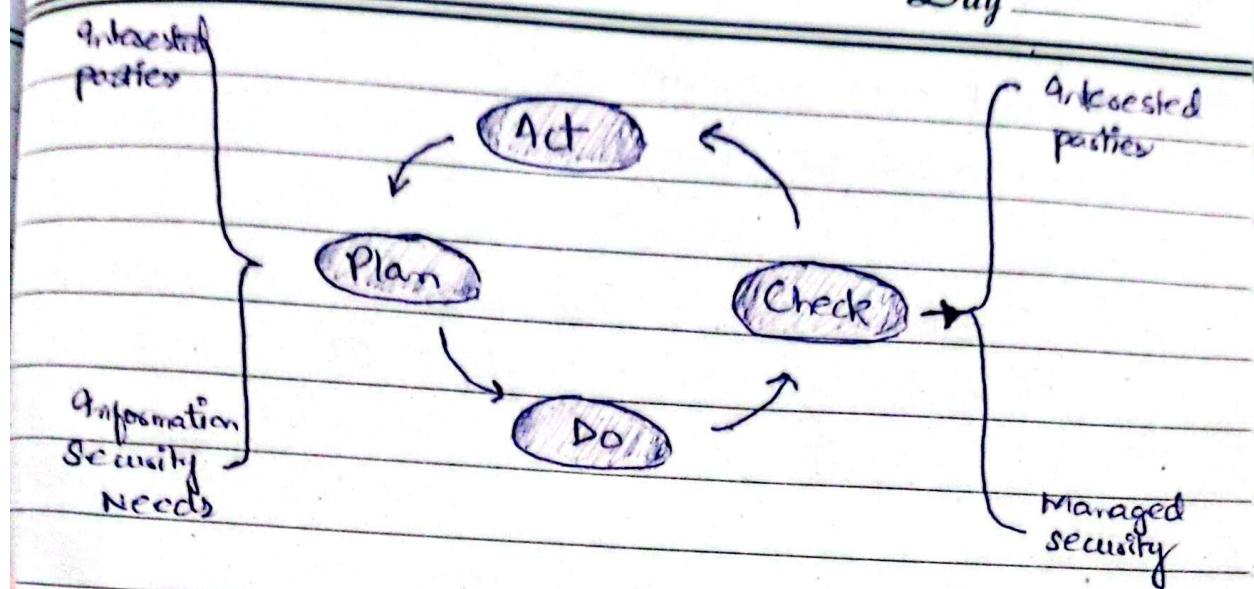
- ↳ Not a one-time task
- ↳ Must be continuously updated
- ↳ Needed due to changing technology & evolving threats

→ Risk Management Cycle

- Plan — Establish security policy, objectives, processes and procedures; perform risk assessment; develop risk treatment plan with appropriate selection of controls or acceptance of risk
- Do — Implement the risk treatment plan.
- Check — Monitor & maintain the risk treatment plan
- Act — Improve based on incident & changes

Date _____

Day _____



- ORGANIZATIONAL CONTEXT & SECURITY POLICY

- Organizational Security Objective

- ↳ Define what security outcome must be achieved
 - ↳ Must address:

- Individual Rights
 - Legal & Regulatory requirements
 - Applicable Standards

- ↳ Support the overall business objective

- Identifying Security Objective

- ↳ Analyze the role & importance of IT systems

- ↳ Focus on business value, not just cost

- ↳ Key questions include:

- Which organizational functions depend on IT?
 - Which tasks require IT support
 - Which decisions rely on accurate & available data?

Date

Day

- What data needs protection?
- What are the consequences of IT security failure?

↳ q) answers to some questions emphasize the need of IT in the business then risk to them should also be identified

→ Organizational Security Strategy

↳ High-level statements describing how objectives will be achieved

↳ Must be consistent across the organization

↳ Depends on:

- Security Objective
- Organization size
- Importance of IT Systems

↳ Defines the approach to manage IT Systems

→ Organizational Security Policy

↳ Describes security objectives, strategies & implementation process

↳ Addresses the following

- Scope & purpose
- Legal, regulatory & business alignment
- Security requirements ↗
 - Confidentiality
 - Availability
 - Accountability
 - Integrity
 - Authenticity
 - Reliability

Date _____

Day _____

- Assignment of responsibilities
- Risk management approach
- Security awareness & training
- Personnel issues of people in authority
- Legal sanctions & violation
- Security sys development & procurement
- Information classification scheme
- Incident detection & planning
- Policy review & change control

↳ IT security policy must be supported by senior management to maintain seriousness among other levels of staff.

• SECURITY RISK ASSESSMENT

↳ Without risk assessment

- Some risk remain unaddressed
- Some controls to mitigate risk are unjustified

↳ waste of resources

↳ Evaluating every asset & every risk is impractical

↳ Time, cost & rapid technology change make full analysis impossible

↳ Resources should be spent proportionally to:

- Potential impact of the risk
- Likelihood of the occurrence

Date _____

Day _____

→ Risk Assessment Approaches

↳ The below mentioned risk assessment approaches choice depends on the

- available resources
- value & criticality of IT Systems
- Legal & regulatory requirements

① Baseline Approach

↳ Implement general security controls using best practices

↳ ADVANTAGES:

- No additional risk assessment cost
- Easy to replicate across systems

↳ DISADVANTAGES:

- Ignores organization specific risk
- Controls may be:

↳ Too strong — unnecessary cost

↳ Too weak — insufficient protection

↳ Characteristics:

- Protect against common threats
- Uses industry best practices
- Forms a foundation for further controls

↳ Recommended for

- Small Orgs
- Limited Resources

Date _____ Regular system patching on a fixed schedule.
Basic access control using user accounts & role. Day _____

↳ Examples

- ① A small office installs antivirus
- ② Default security configuration are replaced with recommended best practice

(2) Informal Approach

↳ Non-structured analysis

↳ Uses expert judgement (internal/external)

↳ ADVANTAGES:

- Fast & low costs
- No special skills req
- More tailored than baseline

↳ DISADVANTAGE:

- Risks may be overlooked
- Results influenced by personal bias
- Weak justification for cost
- Inconsistent results overtime

↳ Recommended for

- Small to medium orgs
- IT sys not critical to business obj
- Limited budget

↳ Example:

- A security consultant informally identifies weak passwords & enables MFA.
- Restrict DB access after analyzing sensitive data
- Increase logging
- Page No. add extra firewall to sys exposed to internet

Date _____

Day _____

③ Detailed Risk Analysis

- ↳ Formal, structured & a comprehensive process
- ↳ Stages include

- ① Asset identification
- ② Threat & vulnerability identification
- ③ Likelihood estimation
- ④ Impact Analysis
- ⑤ Risk determination
- ⑥ Control Selection

↳ ADVANTAGES:

- Most thorough risk identification
- Strong justification for security spending
- Best support for ongoing security management

↳ DISADVANTAGE:

- High cost in time, expertise and resources
- Potential delays in protection

↳ Recommended for

- Gov. Orgs
- Critical Infra
- Large orgs with mission critical IT-systems

↳ Examples

- ① Encrypt customer DB due to high confidentiality
- ② Implement IDS for critical server
- ③ Apply strict RBAC
- ④ Conduct regular penetration testing assessments

Date _____

Day _____

④ Combined Approach

↳ Integrate all the previous three approaches

↳ Process

① Apply baseline controls to all systems

② Identify high-risk or critical sys

③ Perform informal analysis on key sys

④ Gradually perform detailed analysis

↳ ADVANTAGES

- Faster initial Protection

- Cost-effective resource allocation

- Strategic view of risks

↳ DISADVANTAGE

- Inaccurate high-level analysis may delay protection

- Some sys may remain vulnerable temporarily

↳ Examples:

① All sys gets standard controls, while payment sys recvs detailed analysis

② Informal reviews are done quickly, followed by formal assessments over time

③ Add backups for all sys, but real time replication for critical ones

④ Enforce basic pswd policy company-wide, but MPA for finance system only.