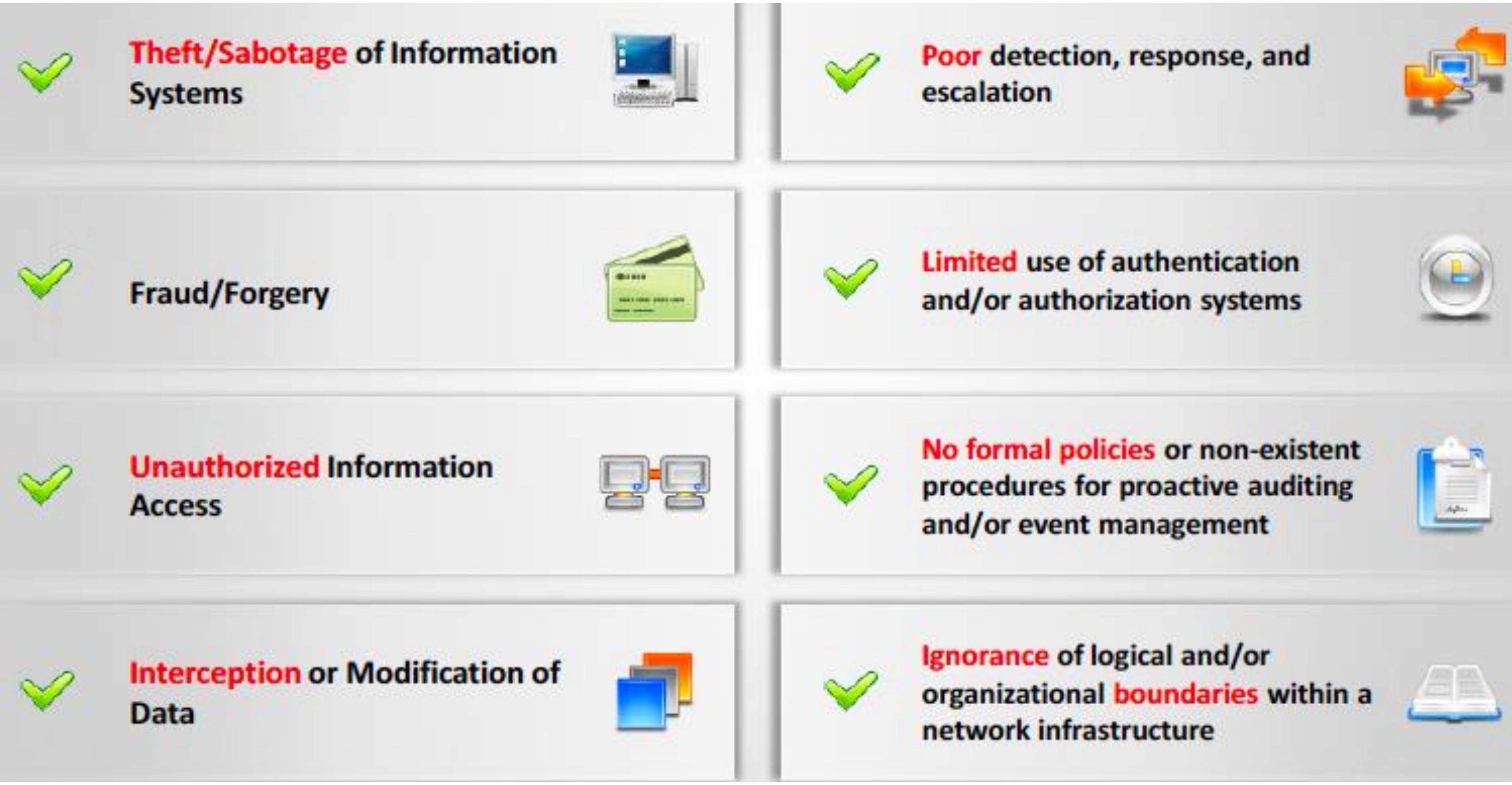
Penetration Test

Erick Dazki M.Kom

Muhammad S.Kom

Security Concerns

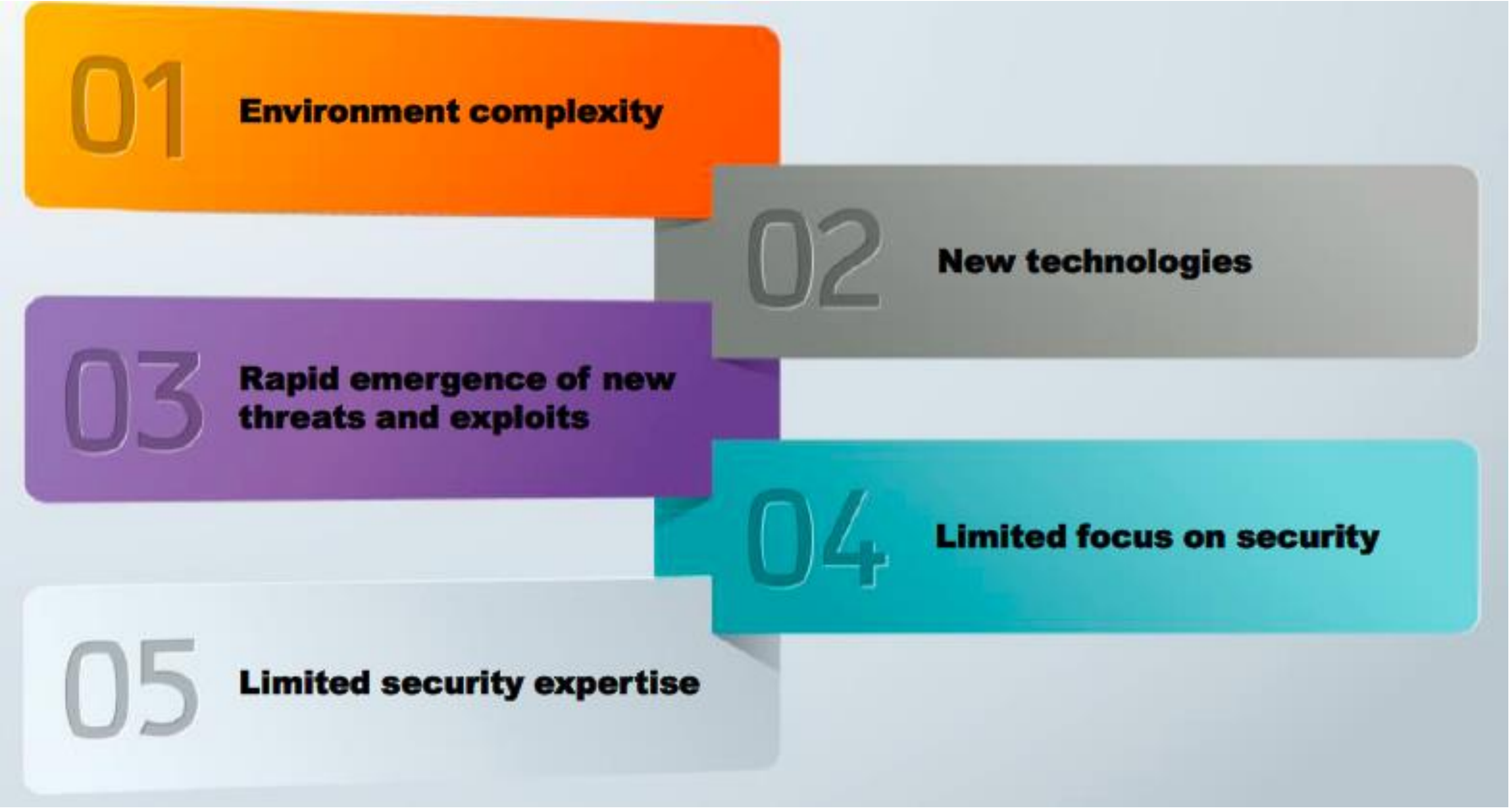


- ✓ Theft/Sabotage of Information Systems
- ✓ Fraud/Forgery
- ✓ Unauthorized Information Access
- ✓ Interception or Modification of Data
- ✓ Poor detection, response, and escalation
- ✓ Limited use of authentication and/or authorization systems
- ✓ No formal policies or non-existent procedures for proactive auditing and/or event management
- ✓ Ignorance of logical and/or organizational boundaries within a network infrastructure

Sumber: © Copyright by EC-Council

❖ Kita harus mengenali masalah-masalah kemanan yang sering dihadapi, bisa dari lingkungan eksternal maupun internal.

Greatest Challenges of Security



01 Environment complexity

02 New technologies

03 Rapid emergence of new threats and exploits

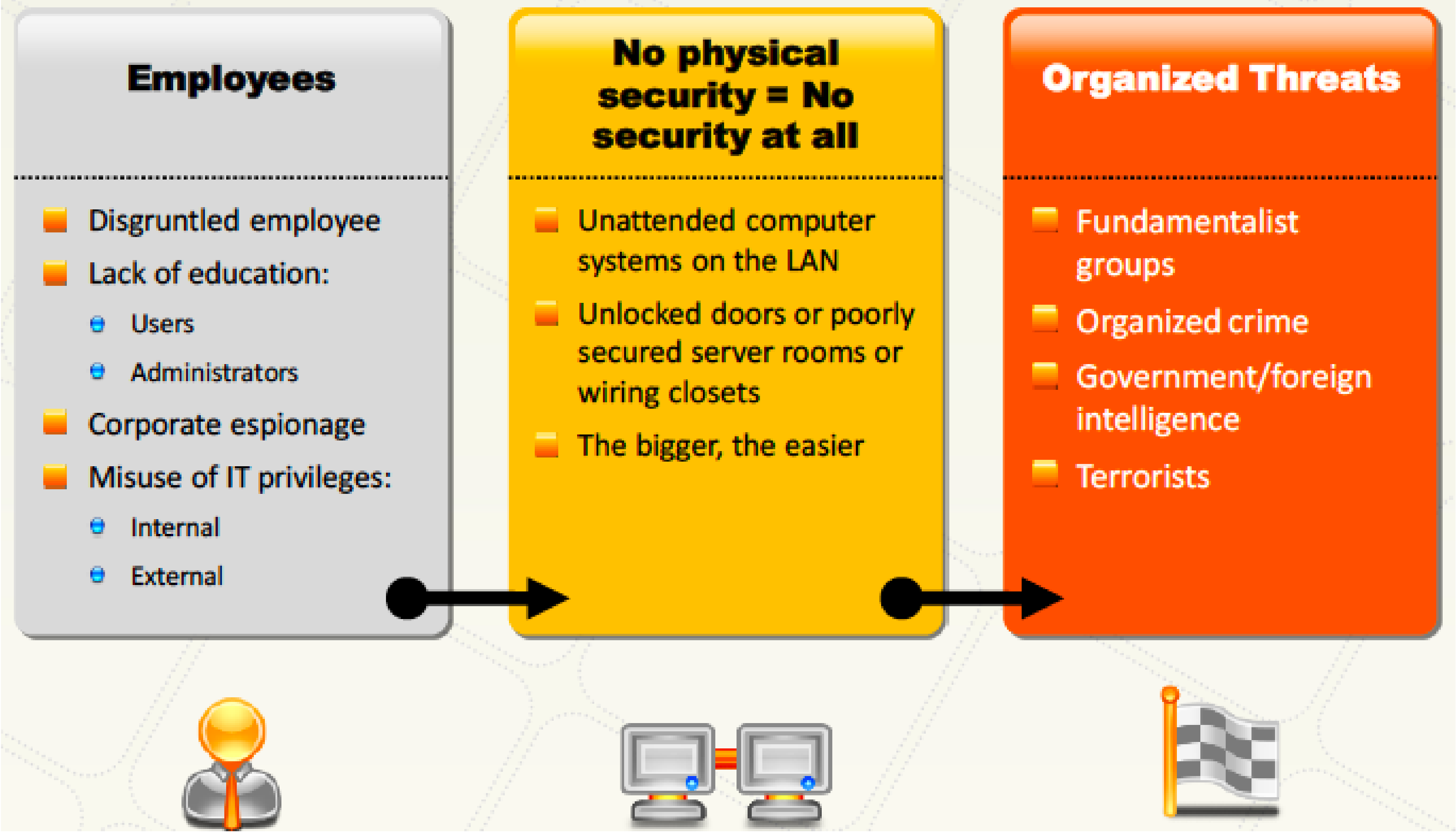
04 Limited focus on security

05 Limited security expertise

Sumber: © Copyright by EC-Council

❖ Tantangan besar pada keamanan sering sekali diabaikan oleh organisasi yang menggunakan Teknologi Informasi di setiap aktifitas nya.

Threat Agents



Employees

- Disgruntled employee
- Lack of education:
  - Users
  - Administrators
- Corporate espionage
- Misuse of IT privileges:
  - Internal
  - External

No physical security = No security at all

- Unattended computer systems on the LAN
- Unlocked doors or poorly secured server rooms or wiring closets
- The bigger, the easier

Organized Threats

- Fundamentalist groups
- Organized crime
- Government/foreign intelligence
- Terrorists

Sumber: © Copyright by EC-Council

❖ Threat Agents atau titik keamanan yang sering menjadi kelemahan setiap organisasi yang terkadang tidak terpikirkan.

Protect Information

01 Your Information Systems

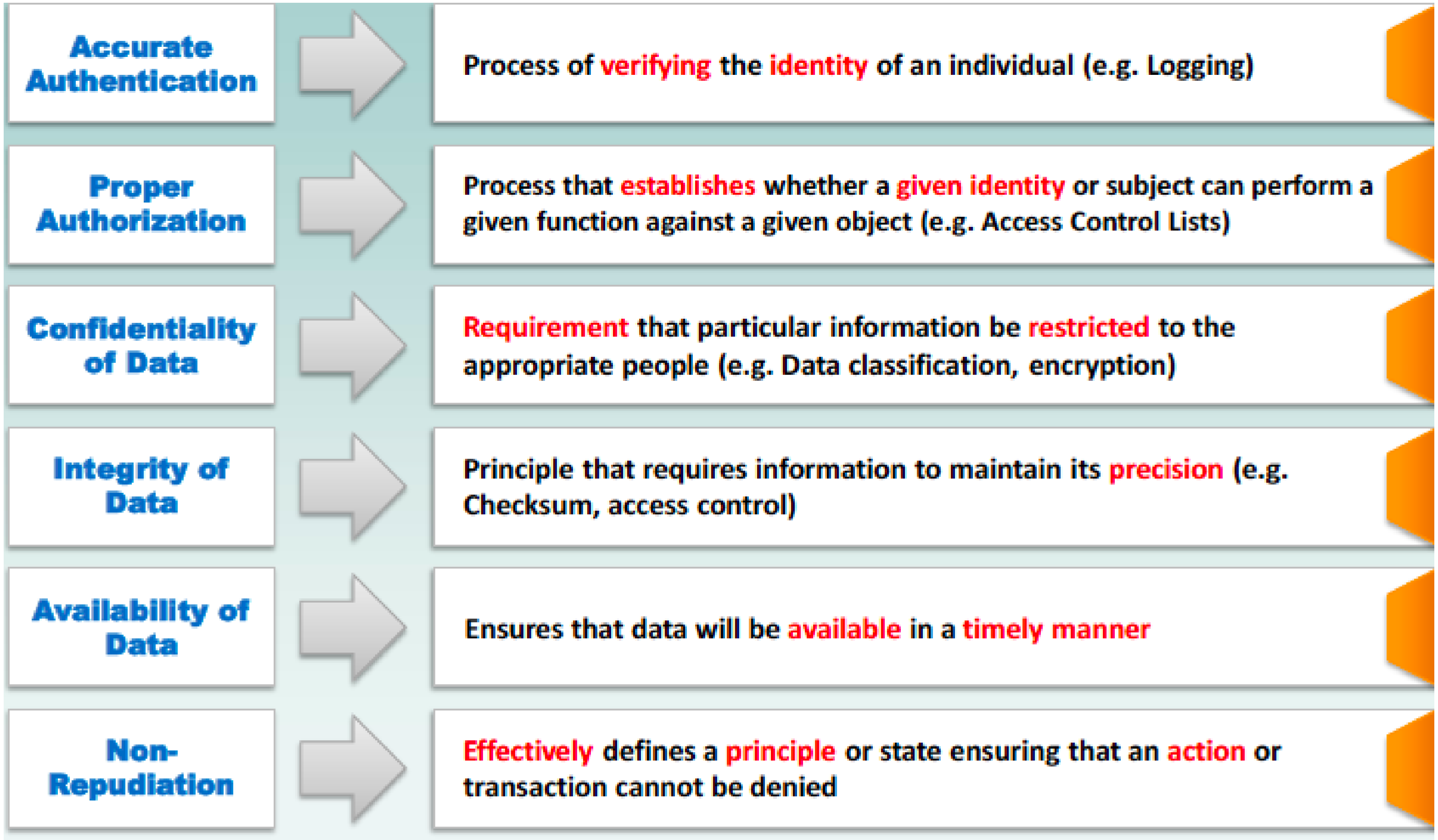
02 Your Network Infrastructure

03 Confidential Personal Data

04 Availability of Your Network

- ❖ Informasi menjadi suatu hal yang sangat penting bagi sebuah perusahaan/organisasi dengan aktifitasnya selalu berkaitan dengan Teknologi Informasi.

Data Security Measures

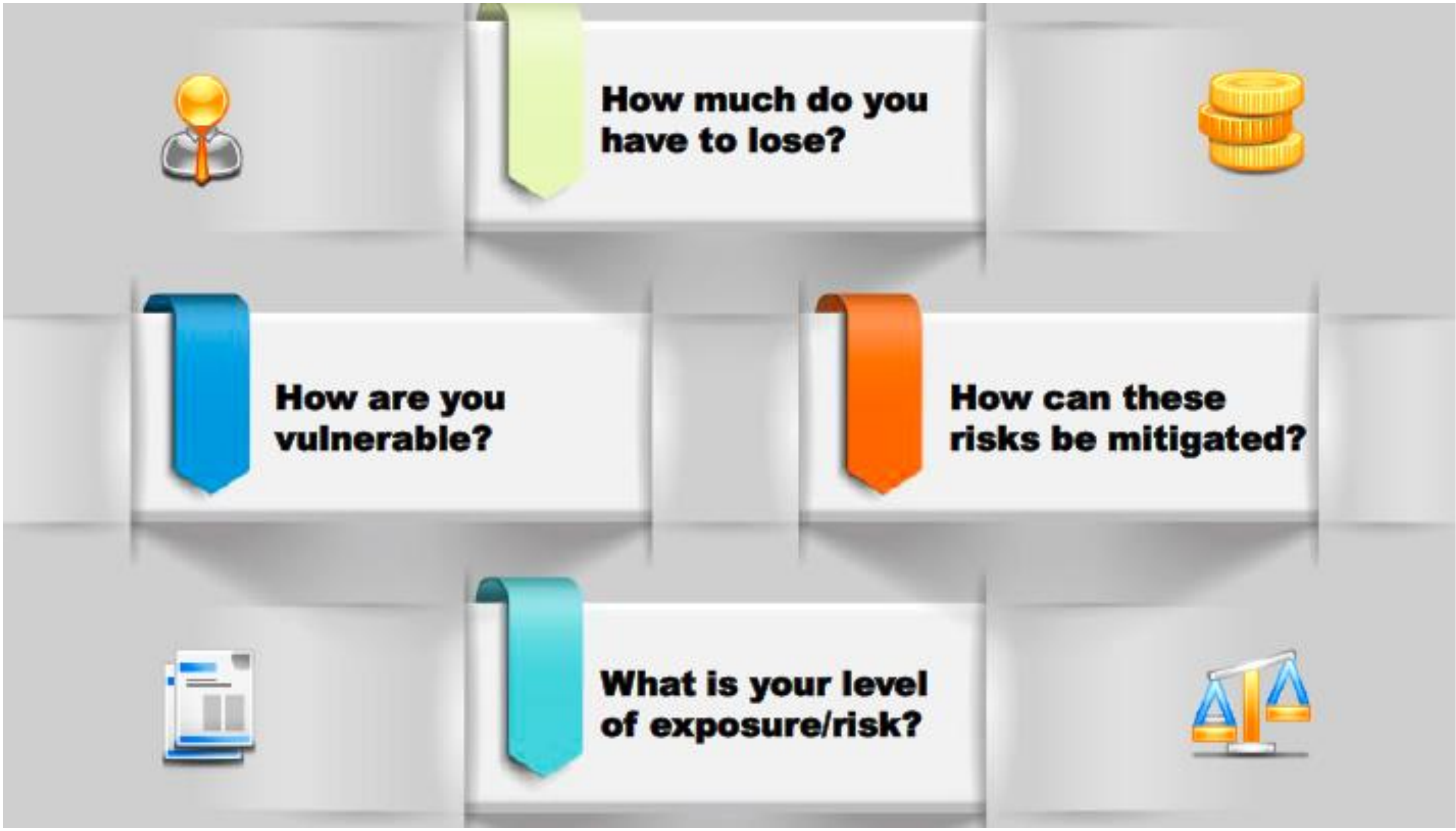


Accurate Authentication	Process of verifying the identity of an individual (e.g. Logging)
Proper Authorization	Process that establishes whether a given identity or subject can perform a given function against a given object (e.g. Access Control Lists)
Confidentiality of Data	Requirement that particular information be restricted to the appropriate people (e.g. Data classification, encryption)
Integrity of Data	Principle that requires information to maintain its precision (e.g. Checksum, access control)
Availability of Data	Ensures that data will be available in a timely manner
Non-Repudiation	Effectively defines a principle or state ensuring that an action or transaction cannot be denied

Sumber: © Copyright by EC-Council

- ❖ Kita harus memperhatikan langkah-langkah untuk keamanan data agar selalu terhindar dari ancaman-ancaman luar maupun dalam.

Understand the Risk



How much do you have to lose?

How are you vulnerable?

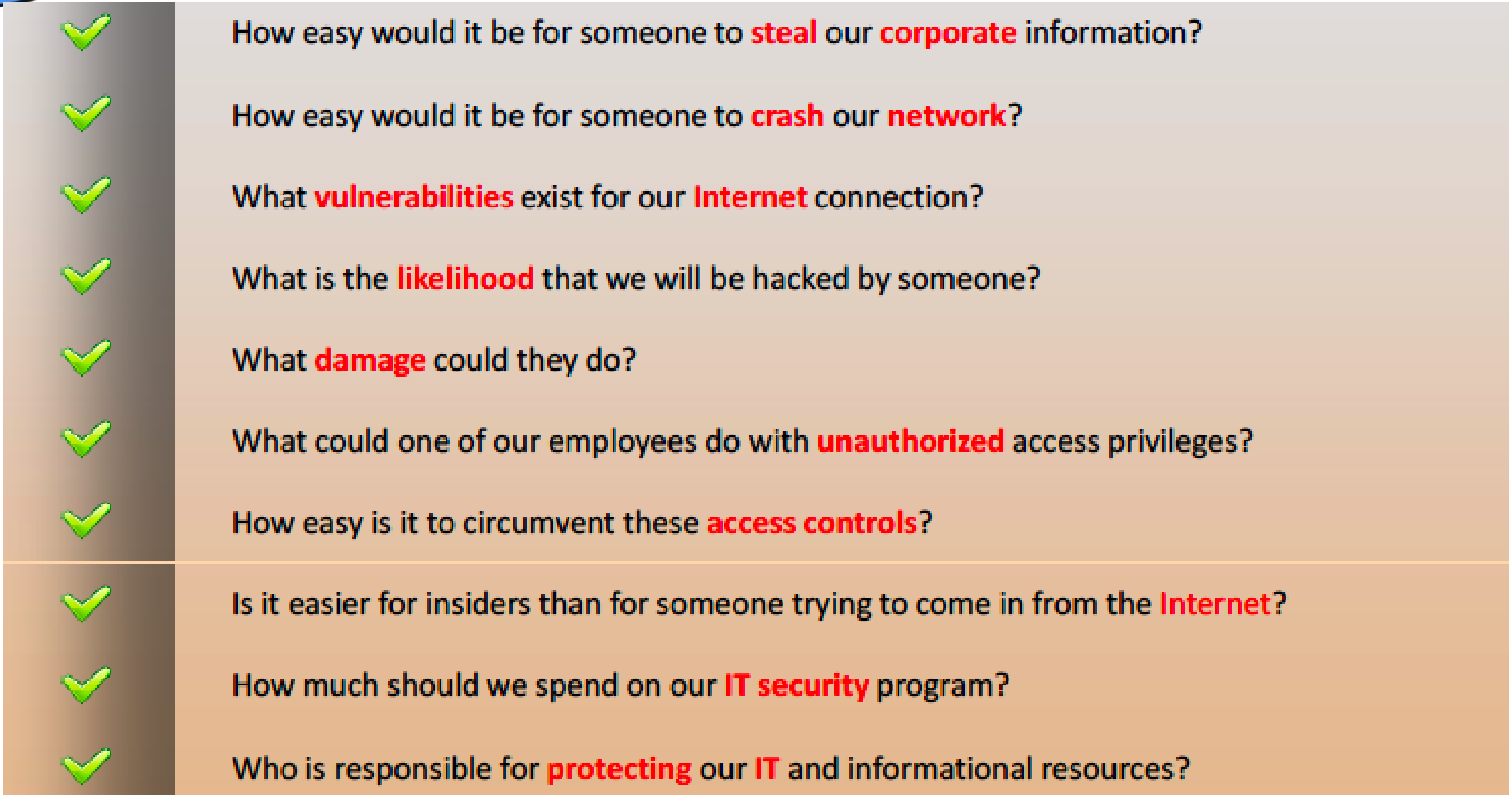
How can these risks be mitigated?

What is your level of exposure/risk?

Sumber: © Copyright by EC-Council

- ❖ Jika kita berbicara ancaman, pasti ada resiko yang datang. Kita harus pahami resiko apa saja yang datang dan apa yang harus dilakukan untuk penanganan resiko.

Assessment Questions

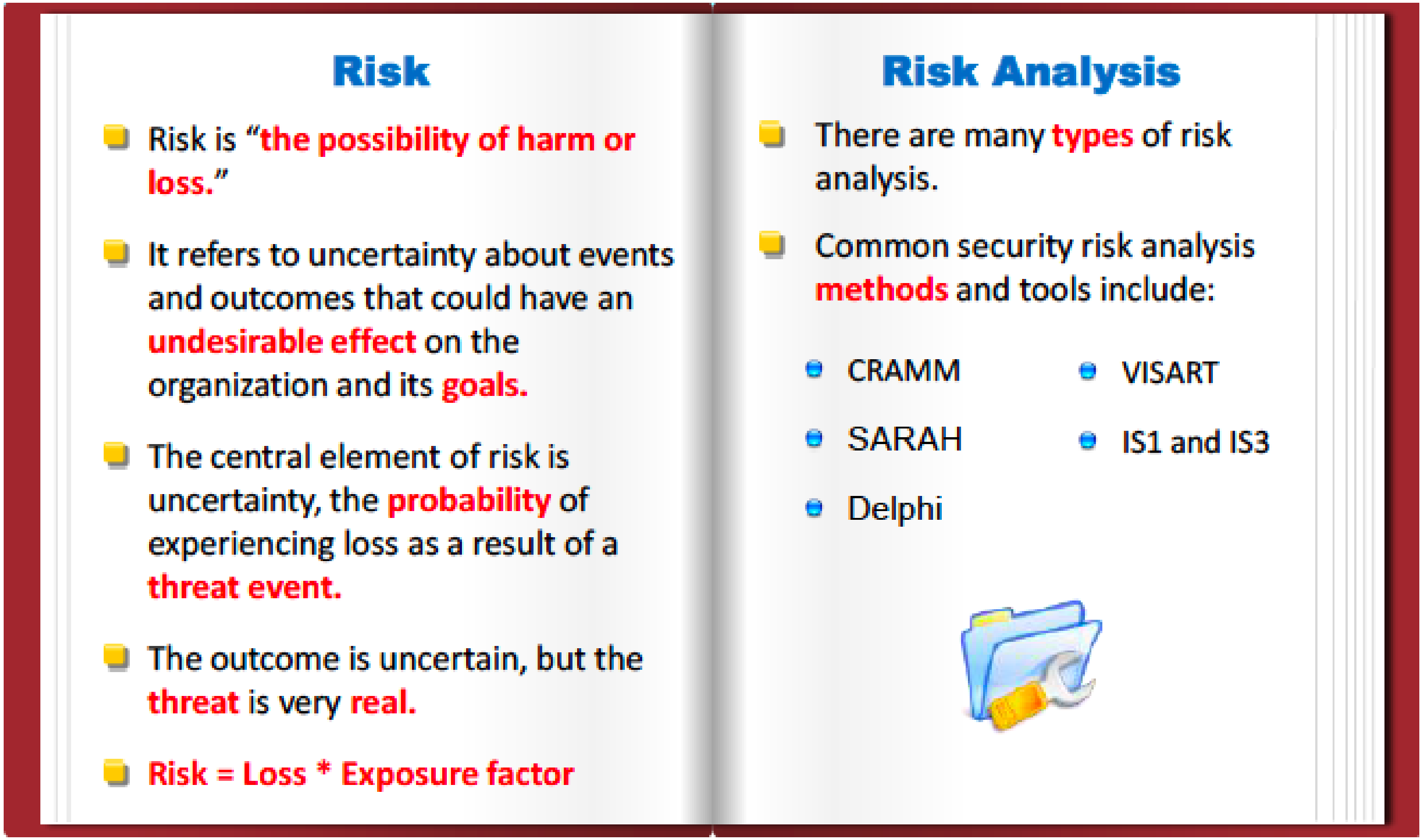


- ✓ How easy would it be for someone to **steal** our **corporate** information?
- ✓ How easy would it be for someone to **crash** our **network**?
- ✓ What **vulnerabilities** exist for our **Internet** connection?
- ✓ What is the **likelihood** that we will be hacked by someone?
- ✓ What **damage** could they do?
- ✓ What could one of our employees do with **unauthorized** access privileges?
- ✓ How easy is it to circumvent these **access controls**?
- ✓ Is it easier for insiders than for someone trying to come in from the **Internet**?
- ✓ How much should we spend on our **IT security** program?
- ✓ Who is responsible for **protecting** our **IT** and informational resources?

Sumber: © Copyright by EC-Council

❖ Sebuah ancaman harus dilakukan sebuah Assessment (penilaian) maka dari itu kita harus mempersiapkan pertanyaan-pertanyaan tentang Penilaian Resiko.

Risk Analysis



Risk

- Risk is “the possibility of harm or loss.”
- It refers to uncertainty about events and outcomes that could have an undesirable effect on the organization and its goals.
- The central element of risk is uncertainty, the probability of experiencing loss as a result of a threat event.
- The outcome is uncertain, but the threat is very real.
- Risk = Loss * Exposure factor

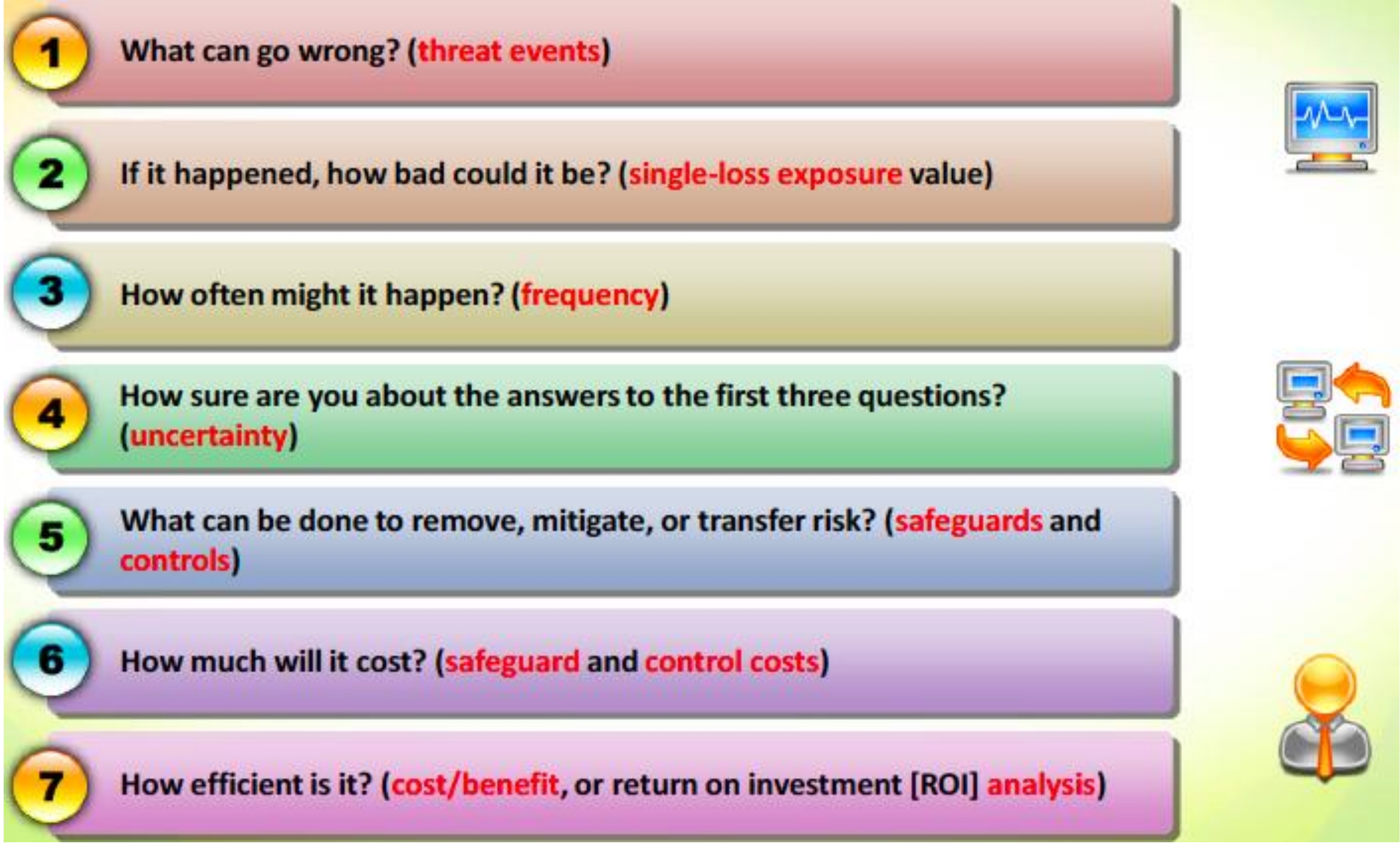
Risk Analysis

- There are many types of risk analysis.
- Common security risk analysis methods and tools include:
  - CRAMM
  - SARAH
  - Delphi
  - VISART
  - IS1 and IS3

Sumber: © Copyright by EC-Council

❖ Setiap adanya resiko kita harus menganalisa resiko tersebut. Kita bisa lihan resiko tersebut supaya bisa menanggulanginya.

Risk Assessment Answer Seven Questions



1 What can go wrong? (threat events)

2 If it happened, how bad could it be? (single-loss exposure value)

3 How often might it happen? (frequency)

4 How sure are you about the answers to the first three questions? (uncertainty)

5 What can be done to remove, mitigate, or transfer risk? (safeguards and controls)

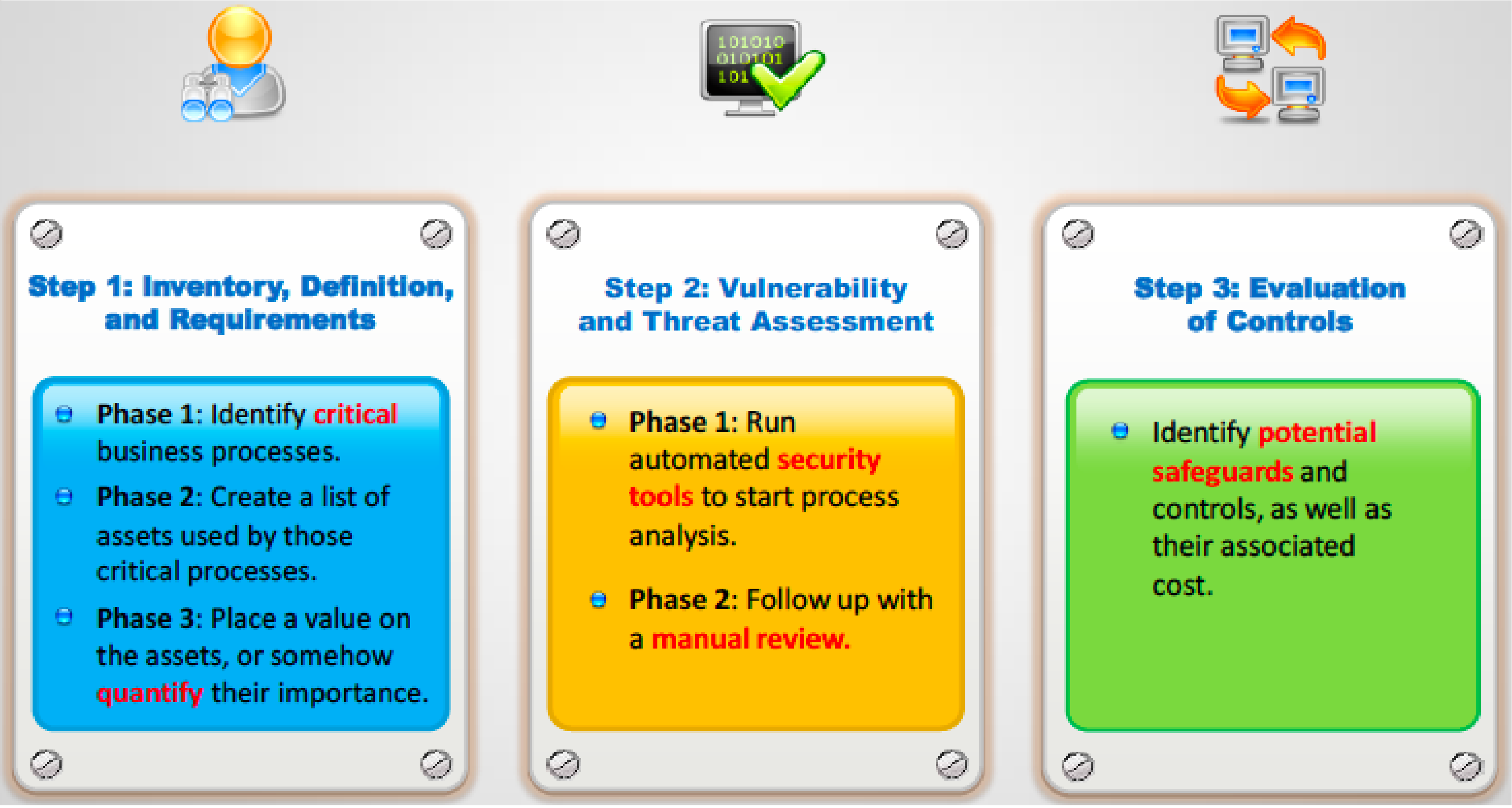
6 How much will it cost? (safeguard and control costs)

7 How efficient is it? (cost/benefit, or return on investment [ROI] analysis)

Sumber: © Copyright by EC-Council

- ❖ Penilaian Resiko menjawab 7 pertanyaan terkait dengan ancaman, biaya, kerusakan bahkan dampak dari resiko tersebut.

Risk Assessment Steps



Step 1: Inventory, Definition, and Requirements

- **Phase 1**: Identify critical business processes.
- **Phase 2**: Create a list of assets used by those critical processes.
- **Phase 3**: Place a value on the assets, or somehow quantify their importance.

Step 2: Vulnerability and Threat Assessment

- **Phase 1**: Run automated security tools to start process analysis.
- **Phase 2**: Follow up with a **manual review.**

Step 3: Evaluation of Controls

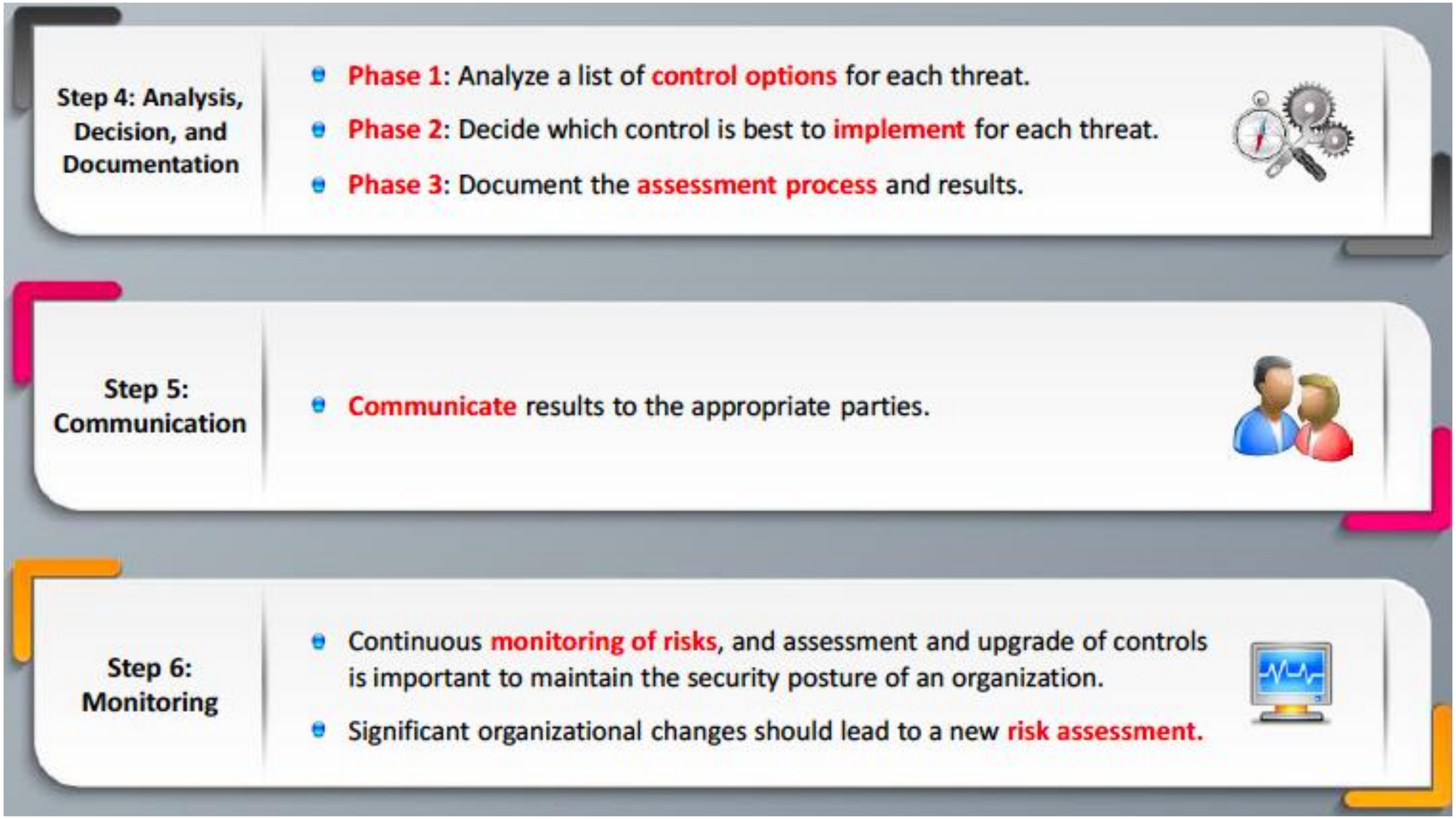
- Identify potential safeguards and controls, as well as their associated cost.

Sumber: © Copyright by EC-Council

- Langkah-langkah penilaian resiko yang harus diperhatikan

Cyber Computer Security

Risk Assessment Steps (Lanjutan)



Step 4: Analysis, Decision, and Documentation

- **Phase 1**: Analyze a list of **control options** for each threat.
- **Phase 2**: Decide which control is best to **implement** for each threat.
- **Phase 3**: Document the **assessment process** and results.

Step 5: Communication

- **Communicate** results to the appropriate parties.

Step 6: Monitoring

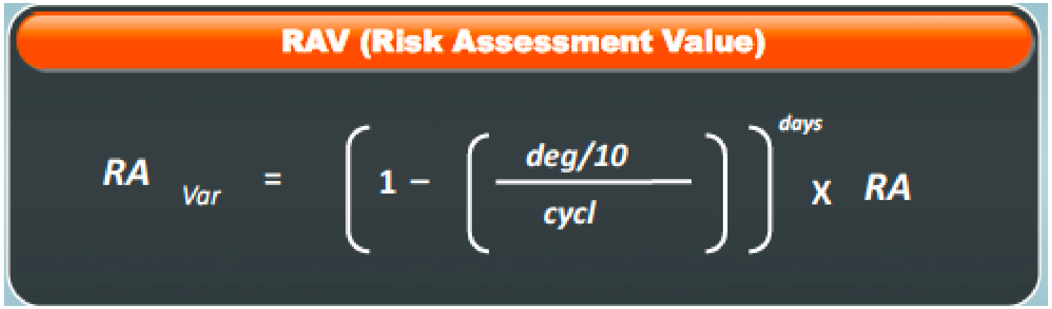
- Continuous **monitoring of risks**, and assessment and upgrade of controls is important to maintain the security posture of an organization.
- Significant organizational changes should lead to a new **risk assessment.**

Sumber: © Copyright by EC-Council

❖ Langkah-langkah penilaian resiko yang harus diperhatikan

Risk Assessment Values

Risk Assessment Values (RAV) adalah Degragasi keamanan (eskalasi risiko) selama siklus hidup tertentu berdasarkan *best practices* untuk pengujian secara periodik.



RAV (Risk Assessment Value)

$$RA_{Var} = \left(1 - \left(\frac{deg/10}{cycl}\right)\right)^{days} \times RA$$

Sumber: © Copyright by EC-Council

- ❖ Eskalasi resiko selama proses siklus penilaian berdasarkan *Best Practice* untuk pengujian secara periodik.

Information Security Awareness

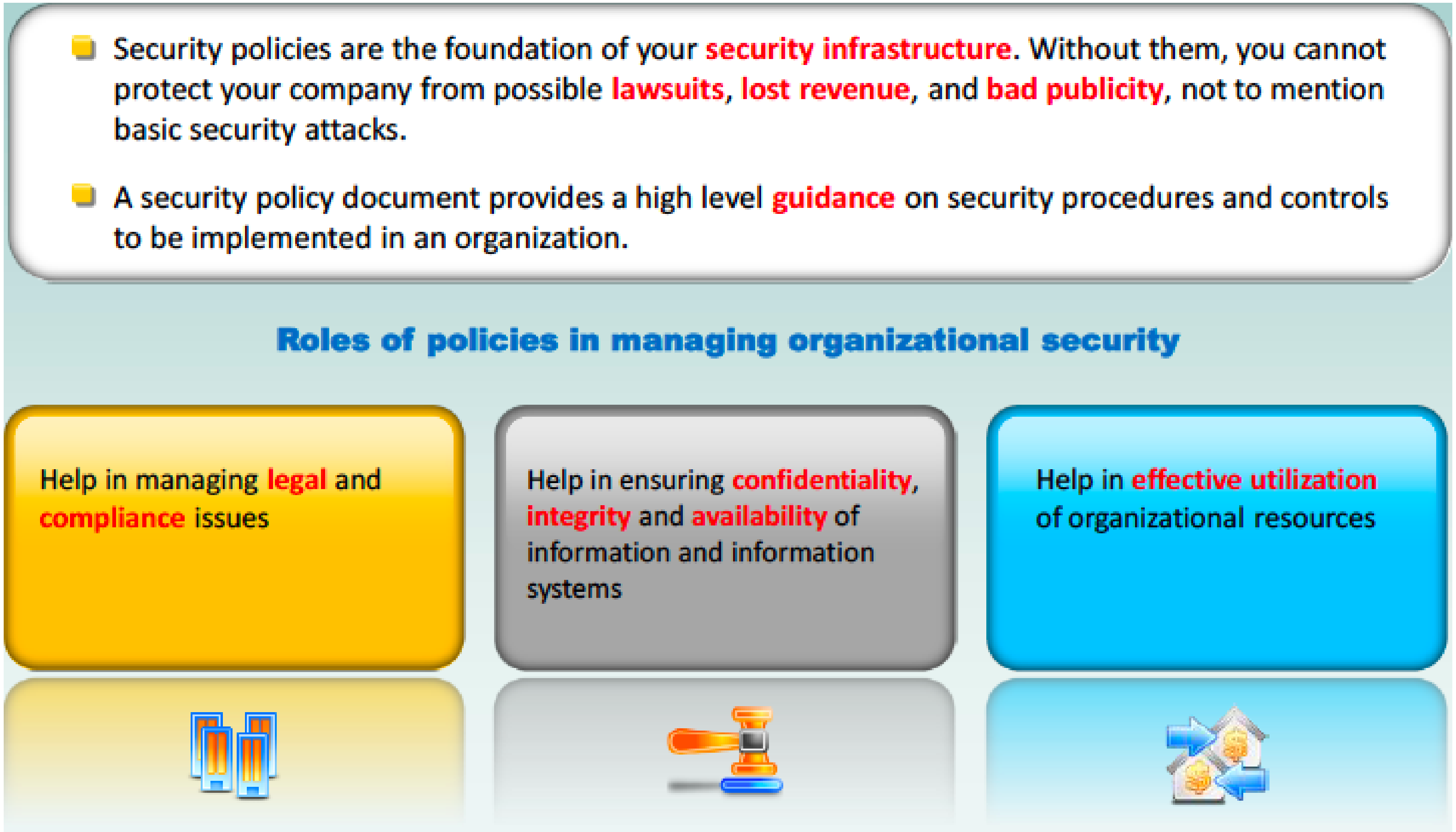
Information security is all about people.

If people understand and appreciate the dangers and risks associated with mismanaging information, the potential for exposure to risk becomes measurably reduced.

Sumber: © Copyright by EC-Council

❖ Kesadaran terhadap keamanan informasi sering sekali diabaikan oleh perusahaan/organisasi. Karena bisa saja ancaman datang dari dalam organisasi itu sendiri.

Security Policies



- Security policies are the foundation of your security infrastructure. Without them, you cannot protect your company from possible lawsuits, lost revenue, and bad publicity, not to mention basic security attacks.
- A security policy document provides a high level guidance on security procedures and controls to be implemented in an organization.

Roles of policies in managing organizational security

Help in managing legal and compliance issues

Help in ensuring confidentiality, integrity and availability of information and information systems

Help in effective utilization of organizational resources

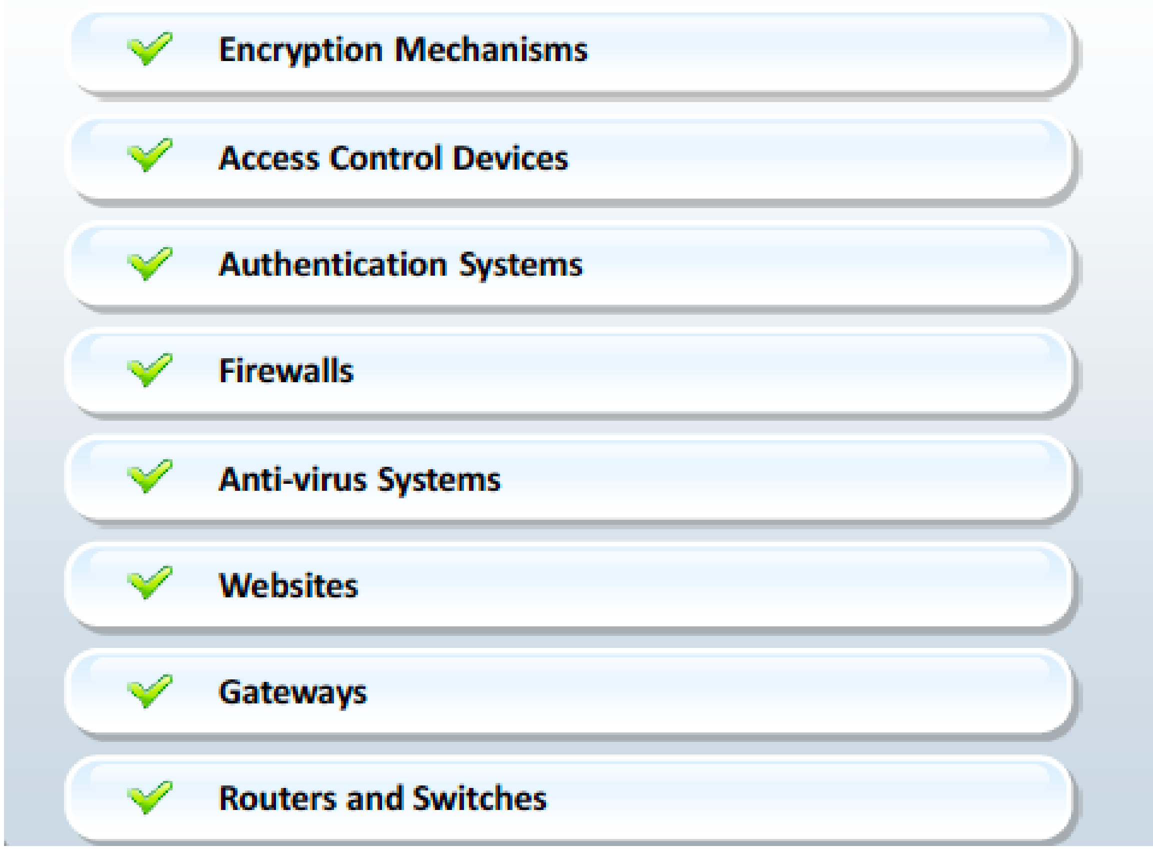
Sumber: © Copyright by EC-Council

- ❖ Suatu kebijakan keamanan sangat diperlukan untuk membentengi kemungkinan-kemungkinan yang akan terjadi. Kebijakan Keamanan berperan sebagai pedoman tingkat tinggi tentang prosedur keamanan dan kontrol pada organisasi.

Cyber Computer Security

Security Policy Basics

A security policy should determine the rules and regulations for the following systems:



- ✓ Encryption Mechanisms
- ✓ Access Control Devices
- ✓ Authentication Systems
- ✓ Firewalls
- ✓ Anti-virus Systems
- ✓ Websites
- ✓ Gateways
- ✓ Routers and Switches

Sumber: © Copyright by EC-Council

❖ Suatu kebijakan keamanan harus menentukan aturan dan peraturan dasar pada sistem agar proteksi lebih ketat dan kuat.

Security Policy Basics (Lanjutan)

There are two types of basic security policies:

- **Technical Security Policies**: Include how technology should be configured and used.
- **Administrative Security Policies**: Include how people (both end users and management) should behave/respond to security.

Persons responsible for the implementation of the security policies are:

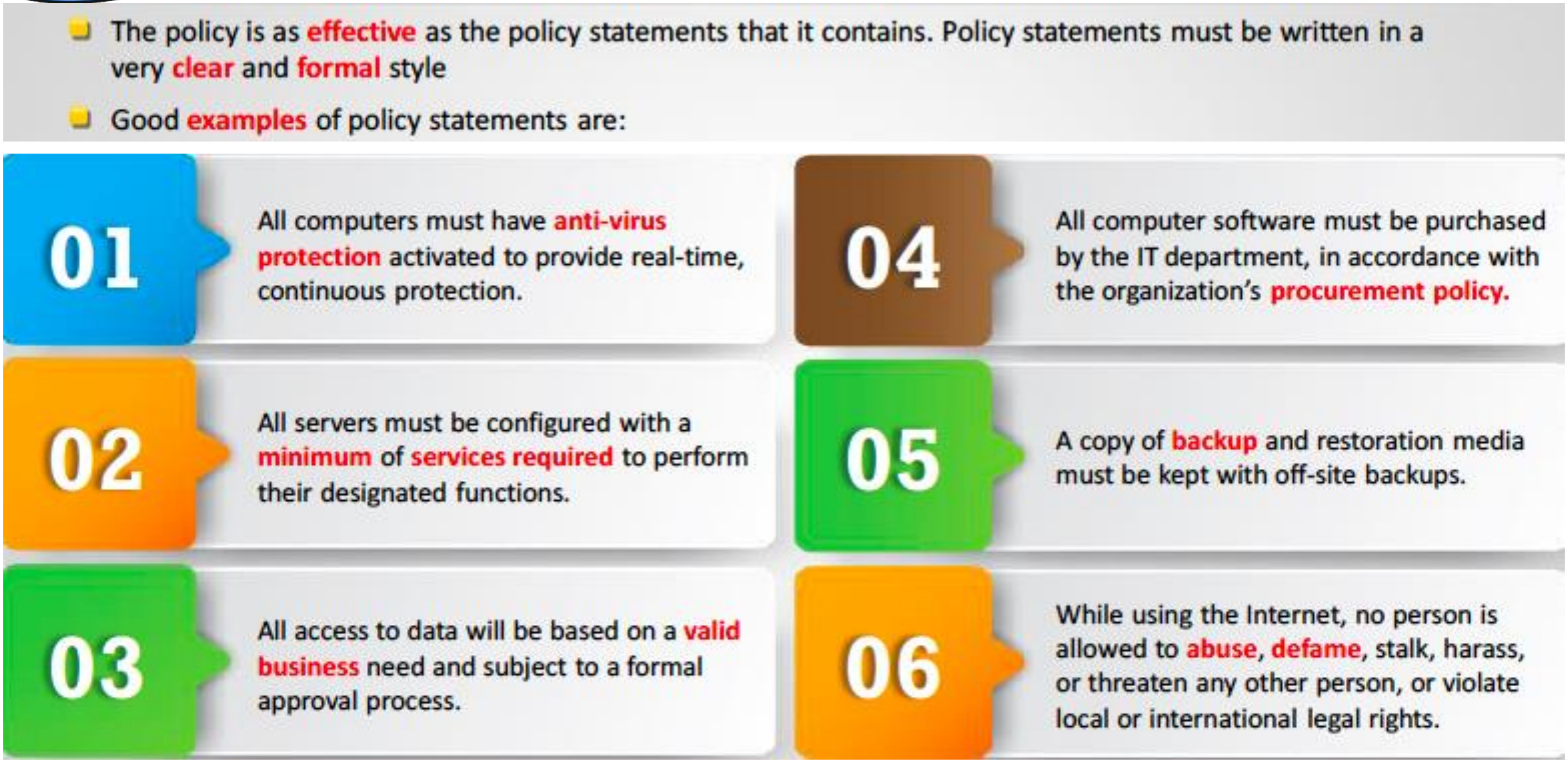
- Director of Information Security
- Chief Security Officer
- Director of Information Technology
- Chief Information Officer

Sumber: © Copyright by EC-Council

❖ Suatu kebijakan keamanan harus menentukan aturan dan peraturan dasar pada sistem agar proteksi lebih ketat dan kuat.

Cyber Computer Security

Policy Statements



- The policy is as effective as the policy statements that it contains. Policy statements must be written in a very clear and formal style
- Good examples of policy statements are:

01 All computers must have anti-virus protection activated to provide real-time, continuous protection.

02 All servers must be configured with a minimum of services required to perform their designated functions.

03 All access to data will be based on a valid business need and subject to a formal approval process.

04 All computer software must be purchased by the IT department, in accordance with the organization's procurement policy.

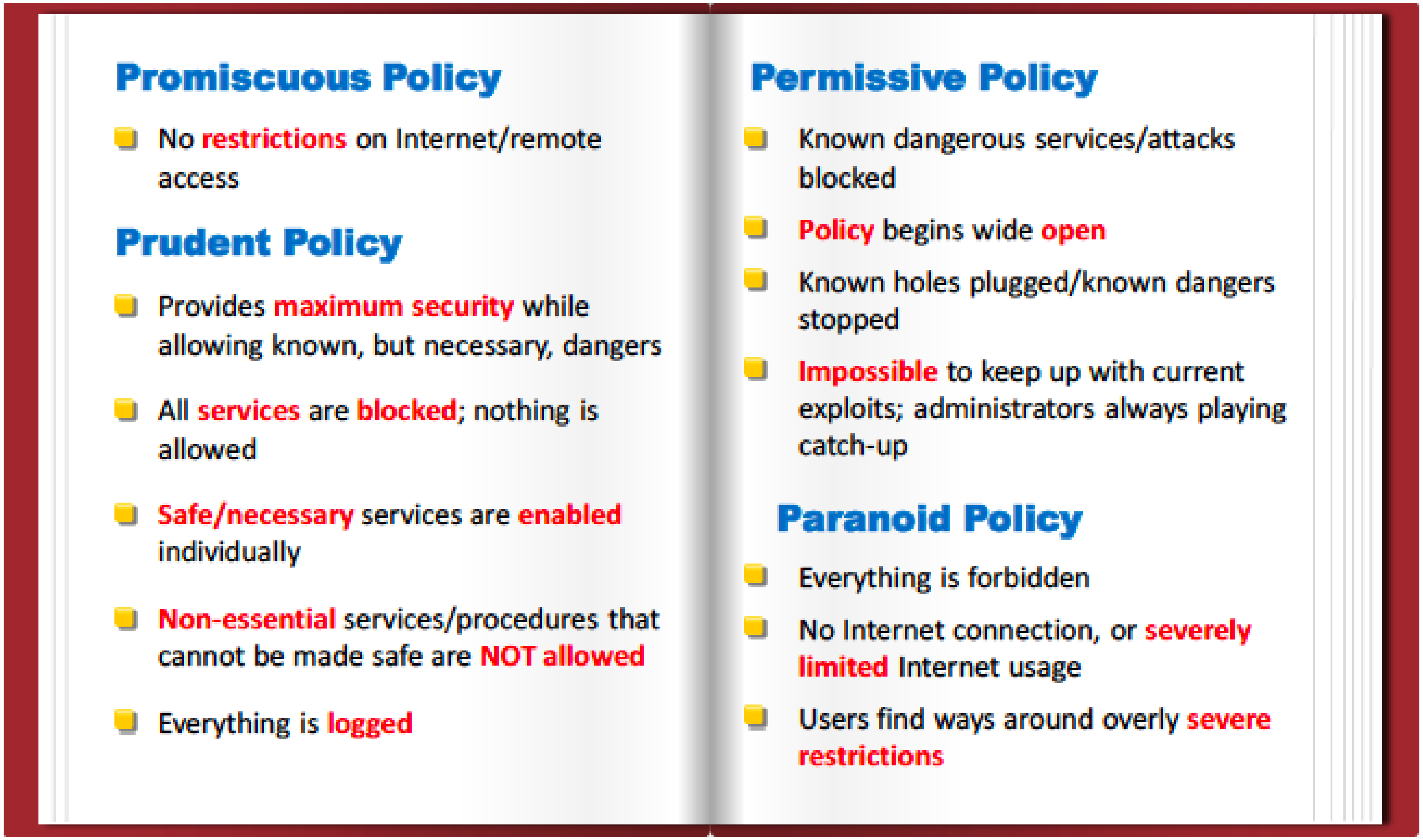
05 A copy of backup and restoration media must be kept with off-site backups.

06 While using the Internet, no person is allowed to abuse, defame, stalk, harass, or threaten any other person, or violate local or international legal rights.

Sumber: © Copyright by EC-Council

❖ Suatu Kebijakan baiknya harus dibuat secara tertulis, jelas dan formal. Agar semua aktifitas yang dilakukan oleh user maupun admin menjadi aman.

Types of Security Policies



Promiscuous Policy

- No **restrictions** on Internet/remote access

Prudent Policy

- Provides **maximum security** while allowing known, but necessary, dangers
- All **services** are **blocked**; nothing is allowed
- **Safe/necessary** services are **enabled** individually
- **Non-essential** services/procedures that cannot be made safe are **NOT allowed**
- Everything is **logged**

Permissive Policy

- Known dangerous services/attacks blocked
- **Policy** begins wide **open**
- Known holes plugged/known dangers stopped
- **Impossible** to keep up with current exploits; administrators always playing catch-up

Paranoid Policy

- Everything is forbidden
- No Internet connection, or **severely limited** Internet usage
- Users find ways around overly **severe restrictions**

Sumber: © Copyright by EC-Council

❖ Berikut adalah tipe-tipe dari kebijakan keamanan, ada kebijakan yang menerapkan kelonggaran terhadap akses internet dan ada yang super ketat.

An Organization’s Security Policies

1. Acceptable-use policy
2. Remote-access policy
3. Information-protection policy
4. Wireless security policy
5. Email security policy
6. Email and Internet use policy
7. Personal computer acceptable use policy
8. Firewall-management policy
9. Internet acceptable use policy
10. User identification and password policy
11. Software license policy
12. User account policy

Sumber: © Copyright by EC-Council

❖ Apa saja yang termasuk dalam kebijakan keamanan yang harus diterapkan pada sisitem, yaitu mencakup semua aktifitas yang terkait dengan internet.

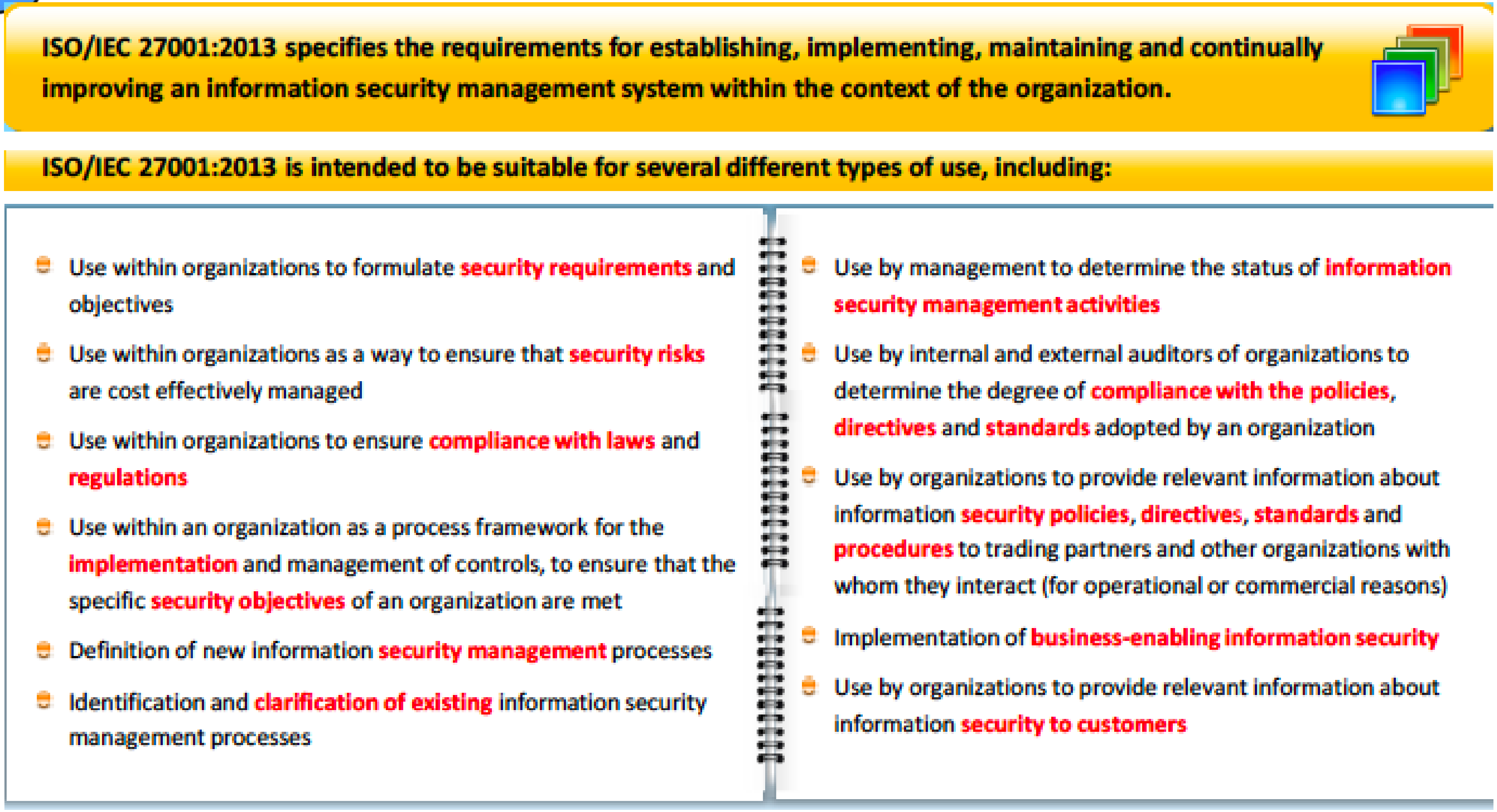
An Organization’s Security Policies

13. Information-protection policy
14. Special-access policy
15. Network-connection policy
16. Business-partner policy
17. Data classification policy
18. Intrusion detection policy
19. Virus prevention policy
20. Laptop security policy
21. Personal security policy
22. Cryptography policy

Sumber: © Copyright by EC-Council

- Apa saja yang termasuk dalam kebijakan keamanan yang harus diterapkan pada sisitem, yaitu mencakup semua aktifitas yang terkait dengan internet.

Information Security Standars: ISO/IEC 27001:2013



ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

ISO/IEC 27001:2013 is intended to be suitable for several different types of use, including:

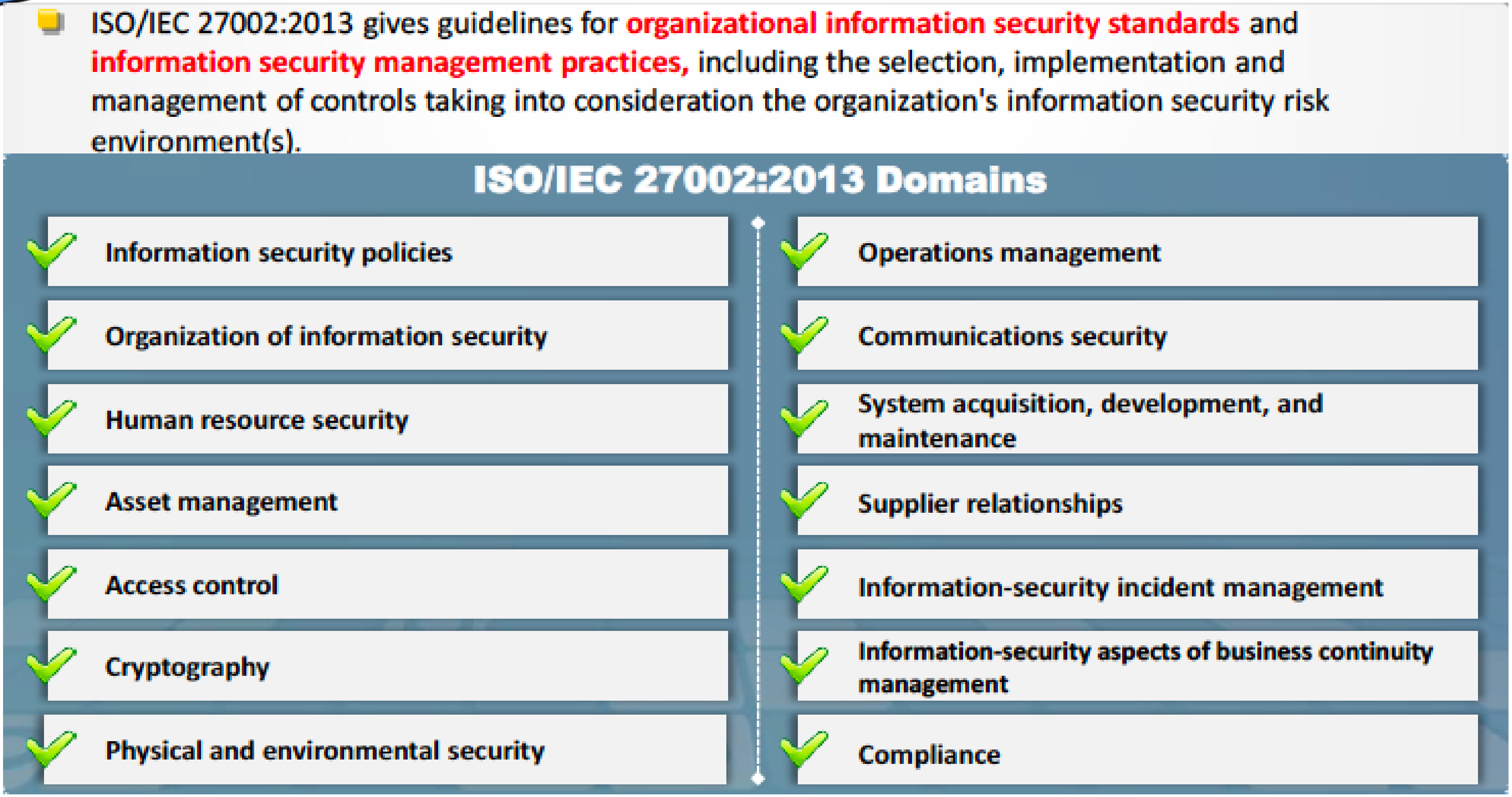
- Use within organizations to formulate **security requirements** and objectives
- Use within organizations as a way to ensure that **security risks** are cost effectively managed
- Use within organizations to ensure **compliance with laws** and **regulations**
- Use within an organization as a process framework for the **implementation** and management of controls, to ensure that the specific **security objectives** of an organization are met
- Definition of new information **security management** processes
- Identification and **clarification of existing** information security management processes
- Use by management to determine the status of **information security management activities**
- Use by internal and external auditors of organizations to determine the degree of **compliance with the policies, directives** and **standards** adopted by an organization
- Use by organizations to provide relevant information about information **security policies, directives, standards** and **procedures** to trading partners and other organizations with whom they interact (for operational or commercial reasons)
- Implementation of **business-enabling information security**
- Use by organizations to provide relevant information about information **security to customers**

Sumber: © Copyright by EC-Council

- ❖ Selain kebijakan keamanan ada juga best practice yang menjadi sebuah strandar keamanan informasi, seperti ISO/IEC 27001:2013

Cyber Computer Security

Information Security Standards: ISO/IEC 27002:2013



- ISO/IEC 27002:2013 gives guidelines for **organizational information security standards** and **information security management practices,** including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

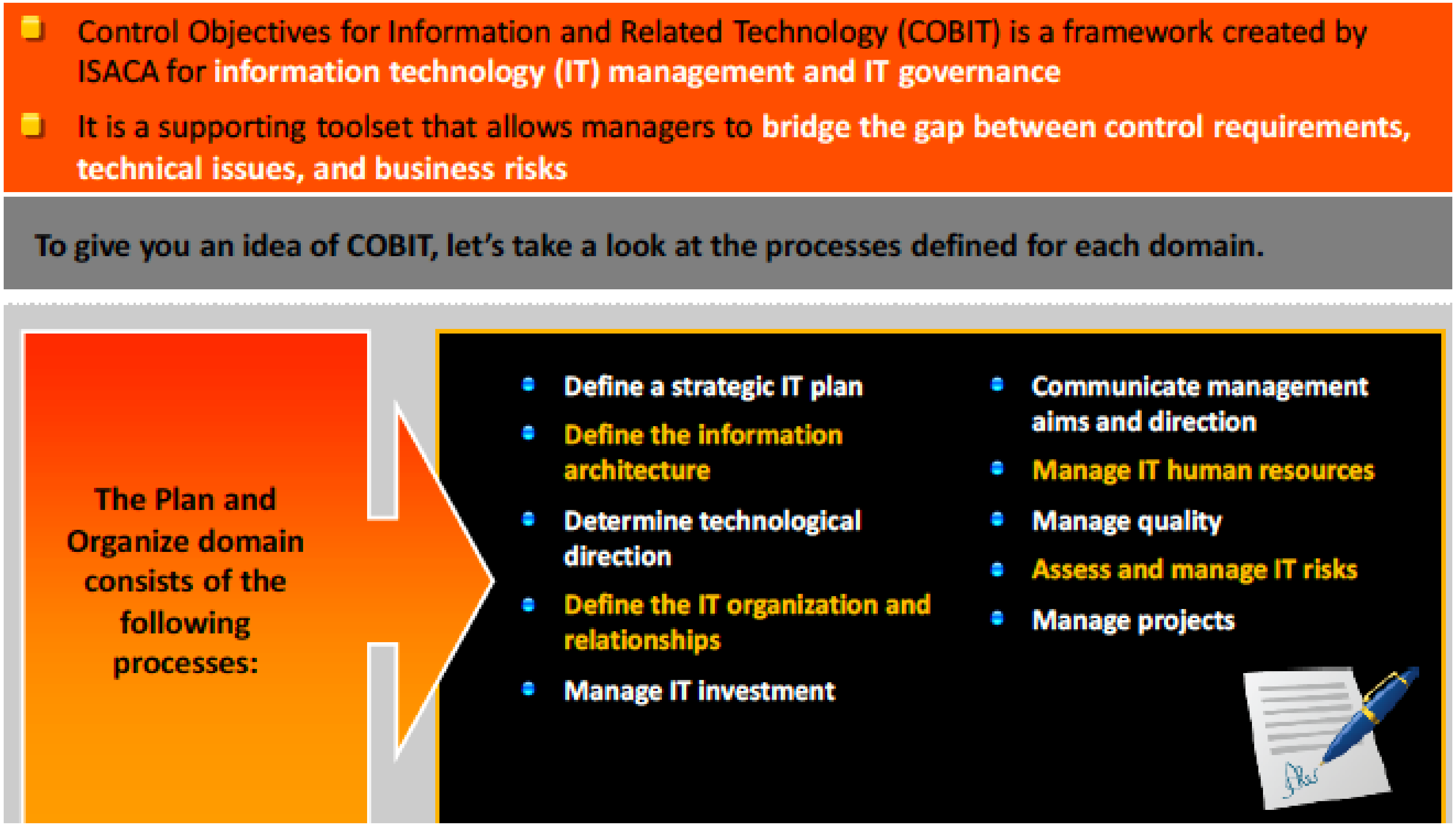
ISO/IEC 27002:2013 Domains

- ✓ Information security policies
- ✓ Organization of information security
- ✓ Human resource security
- ✓ Asset management
- ✓ Access control
- ✓ Cryptography
- ✓ Physical and environmental security
- ✓ Operations management
- ✓ Communications security
- ✓ System acquisition, development, and maintenance
- ✓ Supplier relationships
- ✓ Information-security incident management
- ✓ Information-security aspects of business continuity management
- ✓ Compliance

Sumber: © Copyright by EC-Council

❖ Selain kebijakan keamanan ada juga best practice yang menjadi sebuah strandar keamanan informasi, seperti ISO/IEC 27002:2013

COBIT



- Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance
- It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks

To give you an idea of COBIT, let's take a look at the processes defined for each domain.

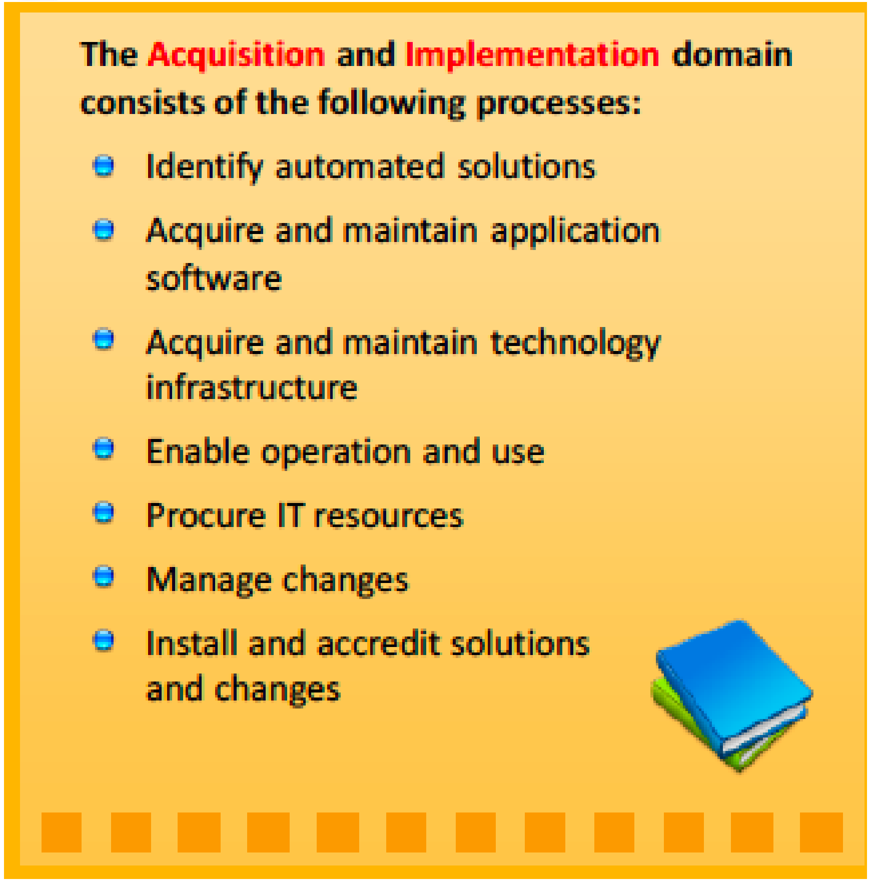
The Plan and Organize domain consists of the following processes:

- Define a strategic IT plan
- Define the information architecture
- Determine technological direction
- Define the IT organization and relationships
- Manage IT investment
- Communicate management aims and direction
- Manage IT human resources
- Manage quality
- Assess and manage IT risks
- Manage projects

Sumber: © Copyright by EC-Council

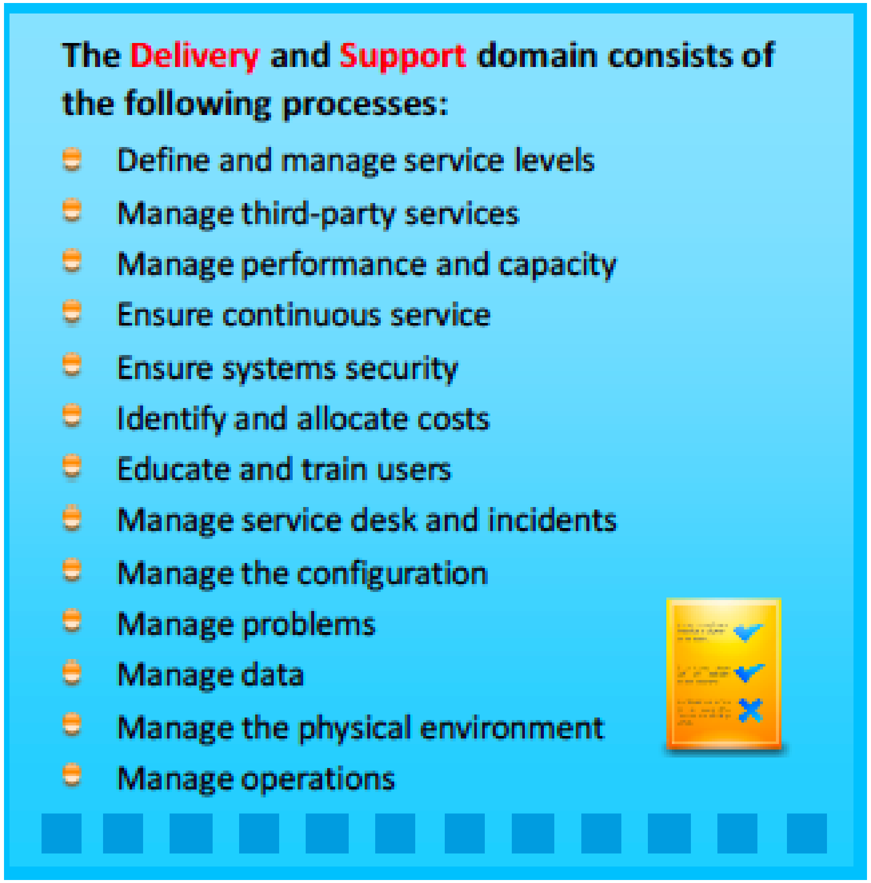
❖ COBIT dapat mendukung yang memungkinkan pengelola menjembatani kesenjangan antara kebutuhan kontrol, masalah teknis, dan resiko bisnis.

COBIT (lanjutan)



The Acquisition and Implementation domain consists of the following processes:

- Identify automated solutions
- Acquire and maintain application software
- Acquire and maintain technology infrastructure
- Enable operation and use
- Procure IT resources
- Manage changes
- Install and accredit solutions and changes



The Delivery and Support domain consists of the following processes:

- Define and manage service levels
- Manage third-party services
- Manage performance and capacity
- Ensure continuous service
- Ensure systems security
- Identify and allocate costs
- Educate and train users
- Manage service desk and incidents
- Manage the configuration
- Manage problems
- Manage data
- Manage the physical environment
- Manage operations

Sumber: © Copyright by EC-Council

❖ Pada domain COBIT meliputi Acquisition and Implementasi, Delivery and Support yang harus diperhatikan pada Keamanan Informasi sistem.