ISO27001:2022 Lec9

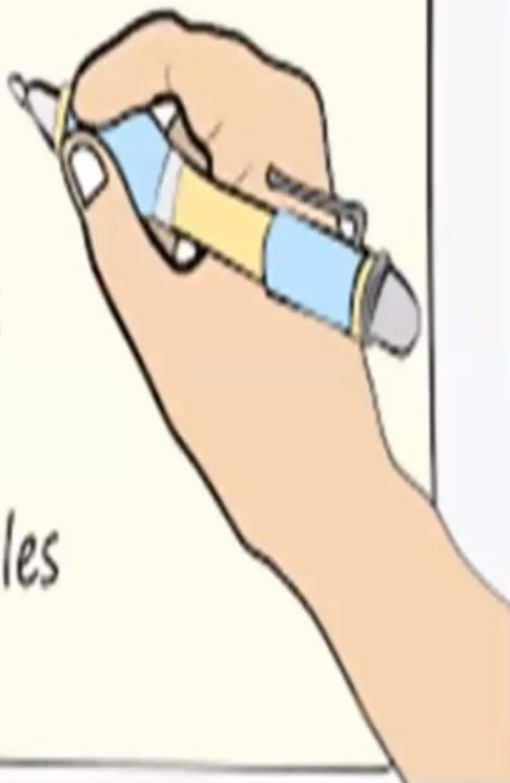**How to achieve this control ?**

Prepare a business case to **convince** the management and take their commitment on the ISO 27001 Implementation
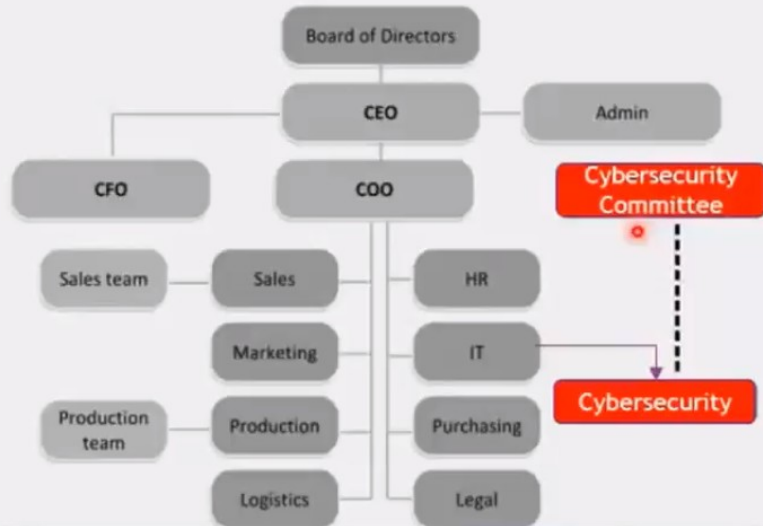
Business case
- Reasons
- Options
- Benefits
- Costs
- Timescales
- Risks
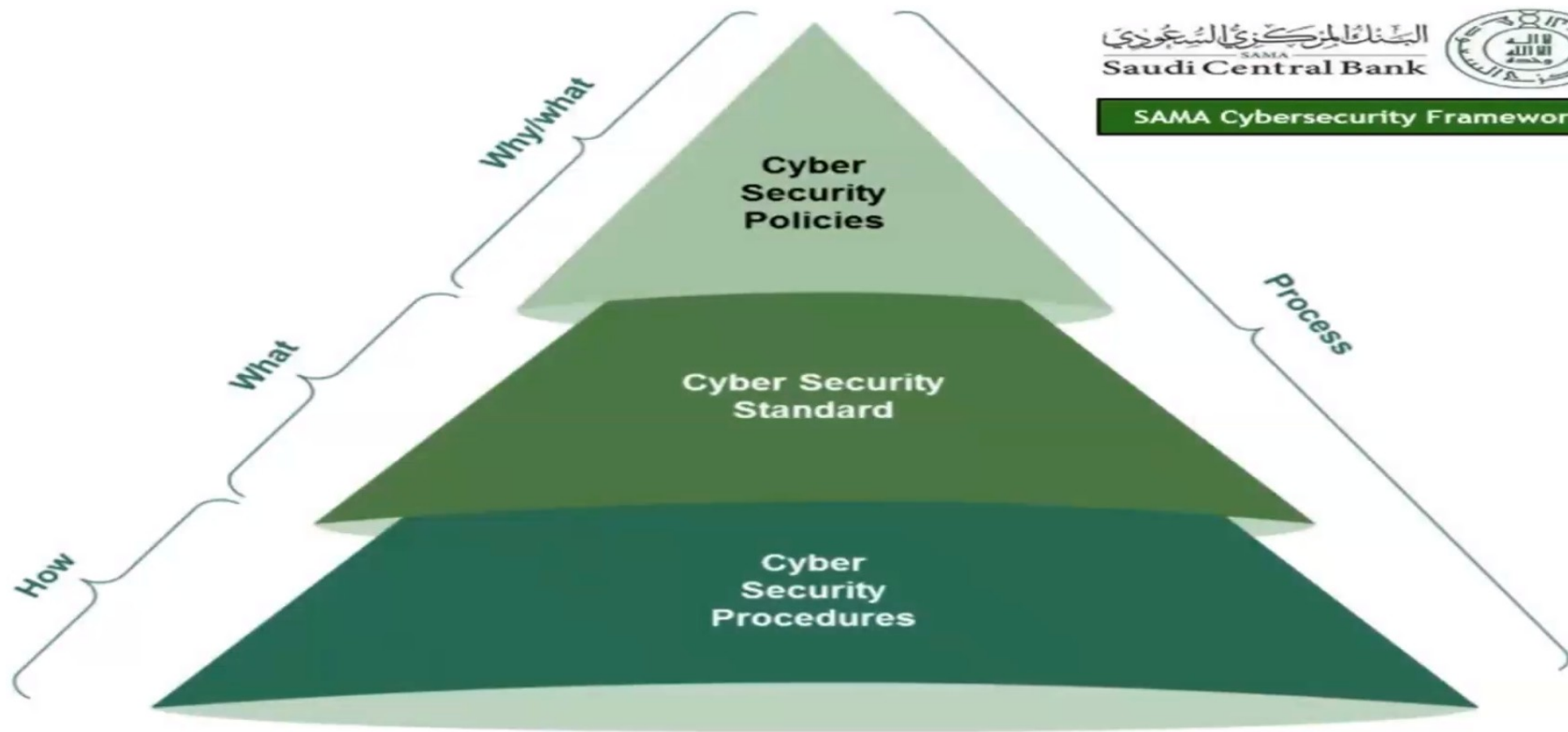
Figure 3 - Cyber Security Documentation Pyramid

1-2	Cybersecurity Management
Objective	To ensure Authorizing Official's support in implementing and managing cybersecurity programs within the organization as per related laws and regulations
Controls	
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This function must be independent from the Information Technology/Information Communication and Technology (IT/ICT) functions (as per the Royal Decree number 37140 dated 14/8/1438H). It is highly recommended that this cybersecurity function reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, must be filled with full-time and experienced Saudi cybersecurity professionals.
1-2-3	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, and governance framework must be defined, documented and approved. The committee must include the head of the cybersecurity function as one of its members. It is highly recommended that the committee reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.

3.1.1 Cyber Security Governance

Principle

A cyber security governance structure should be defined and implemented, and should be endorsed by the board.

Objective

To direct and control the overall approach to cyber security within the Member Organization.

Control considerations

1. A cyber security committee should be established and be mandated by the board.
2. The cyber security committee should be headed by an independent senior manager from a control function.
3. The following positions should be represented in the cyber security committee:
   a. senior managers from all relevant departments (e.g., COO, CIO, compliance officer, heads of relevant business departments);
   b. Chief information security officer (CISO);
   c. Internal audit may attend as an "observer.
4. A cyber security committee charter should be developed, approved and reflect:
   a. committee objectives;
   b. roles and responsibilities;
   c. minimum number of meeting participants;
   d. meeting frequency (minimum on quarterly basis).
5. A cyber security function should be established.
6. The cyber security function should be independent from the information technology function. To avoid any conflict of interest, the cyber security function and information technology function should have separate reporting lines, budgets and staff evaluations.
7. The cyber security function should report directly to the CEO/managing director of the Member Organization or general manager of a control function.
8. A full-time senior manager for the cyber security function, referred to as CISO, should be appointed at senior management level.
9. The Member Organization should :
   a. ensure the CISO has a Saudi nationality;
   b. ensure the CISO is sufficiently qualified;
   c. obtain no objection from SAMA to assign the CISO.
10. The board of the Member Organization should allocate sufficient budget to execute the required cyber security activities.

Relationships Between Information Security Elements

1. Assets and controls can present vulnerabilities that can be exploited by threats.

2. It is the combination of threats and vulnerabilities that can increase the potential effect of the risk.

3. Controls allow the reduction of vulnerabilities. An organization has few alternatives to act against threats. For example, controls can be implemented to provide protection against system intrusions, but it is difficult for an organization to take action to reduce the number of hackers on the internet.
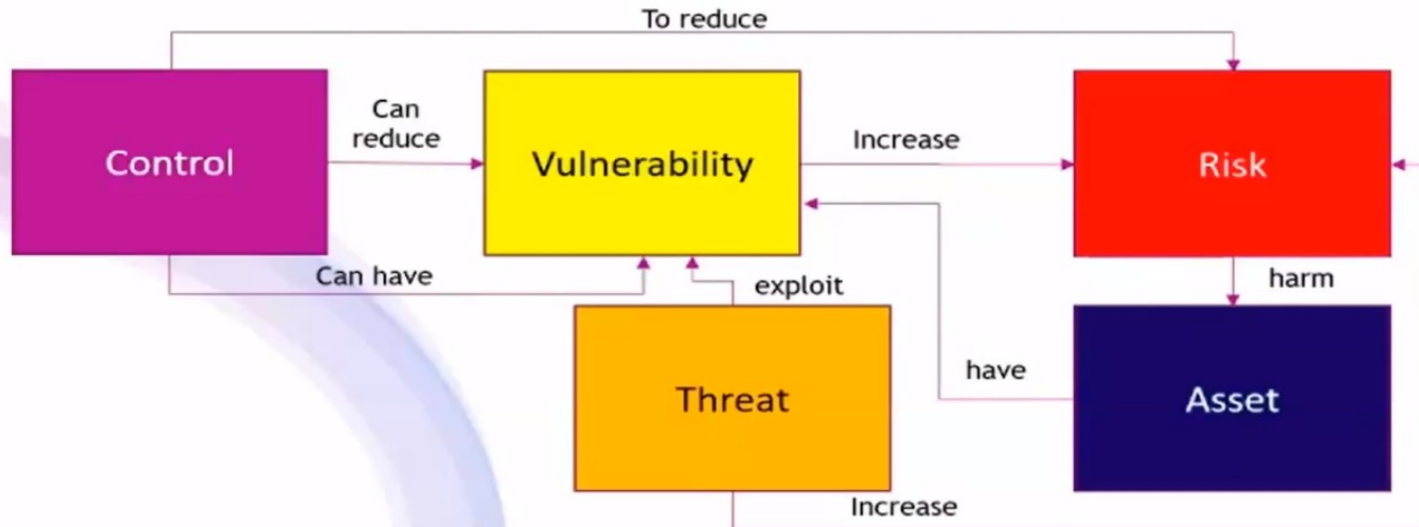
The ISO/IEC 27001 standard classifies security controls in three categories:

Preventive Control	Detective Control	Corrective Control
• Discourage or prevent the appearance of problems	• Search for, detect and identify problems	• Solve problems found and prevent the recurrence

Preventive Control

Examples:
- Publish an information security policy
- Have a confidentiality agreement signed
- Hire only qualified personnel
- Identify risks coming from third parties
- Segregation of duties

Detective Control

Examples:
- Monitor and review third-party services
- Monitor the resources used by systems
- Alarm triggers e.g. when sensing fire
- Review of user access rights
- Analysis of audit logs

Corrective Control

Examples:
- Technical and legal investigation(forensics) following a security incident
- Activating the business continuity plan after the occurrence of a disaster
- Implementation of patches following the identification of technical vulnerabilities

Risk Management Methodology

You shall have an Enterprise Risk Management Methodology

The information security risk criteria should be established considering the context of the organization and requirements of interested parties and should be defined in accordance with Enterprise Risk Management

Appendix 5: Risk tolerance/treatment table

The table below outlines the level of risk tolerance and treatment depending on the overall level of risk rating:

Risk Ratings	Risk Tolerance / Treatment Required
Extreme Risk	**Unacceptable/No Tolerance** Immediate/Urgent action required Escalate to the Vice-Chancellor and President/Senior Executive Group
High Risk	**Highly Cautious** Within 4 months/Action plan required Requires escalation to Senior Managers and/or applicable Senior Executive member
Medium Risk	**Tolerable/Conservative** Assess the risk and determine if current controls are adequate Management responsibility must be specified
Low Risk	**Acceptable** Manage through routine procedures Unlikely to need specific application of resources.

Appendix 4: Risk rating matrix

All risks within the University are rated using a common scale that assesses:

- The **likelihood** of the University being impacted in that way, and
- the potential **consequences** if the risk were to occur.

The risk rating is determined by combining the consequence and likelihood as shown as follows:

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Extreme
Almost certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	High	Extreme
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

What should Statement of Applicability Include?

- Control objectives identified
- Control objectives and control mapping
- Justification for exclusions
- Implementation status
- Supporting documents

1. Identify security controls to be included in the ISMS.

2. Justify the choice of selected and unselected security controls.

3. Obtain formal approval from the management before the implementation of ISMS.

The choice of applying a security control should be justified by the conducted information security risk assessment.

Statement of Applicability (SOA) - Example

Security Control#	Security Control name	Control Description	Included /Excluded	Justification for Inclusion or exclusion
A.13.2.3	Electronic Messaging	Information involved in electronic messaging shall be appropriately protected		
A.14.2.1	Secure development Policy	Rules for the development of software and systems shall be established and applied to developments within the organization		

Treatment of problems and nonconformities

Process: Access Management	clause number: A.9.2.1	Site: Bahrain	Type: Minor
Audit criteria:	A formal user registration and de-registration process should be implemented to enable assignment of access rights.		
Description of the observed nonconformity:	In a sample of 10 user registration and revoking requests that have been extracted from the company service hub portal, there are 6 requests have been correctly gone through the whole identity and access management procedure and took the required approvals, and the rest requests have been created without following the procedure and taking the required approvals		
Root Cause:			
Recommendation:	Ensure all user registration and revoking requests are taken the appropriate approvals and following the identity and access management procedure		

	A	B	C	D	E
1	**A6**	**Organization of information security**			
2	A6.1	**Internal organization**	**Current Level**	**Description**	**Desired Level**
3		A6.1.1 Information security roles and responsibilities	Initial	ABC will define information security related roles and responsibilities through personnel job descriptions and documented procedures, which will be communicated to all concerned.	Managed
4		A6.1.2 Segregation of duties	Nonexistent	ABC will ensure that job descriptions and procedures are communicated to all concerned, to avoid conflicts and to ensure that access to critical information assets and services are clearly divided among authorized personnel.	Defined
5		A6.1.3 Contact with authorities	Initial	In case of emergency, escalation and reporting procedures will be define to ensure communication with relevant Designations as well as contact with local authorities.	Managed

TIP:
Use Spreadsheet to
conduct GAP Analysis

THANKS!