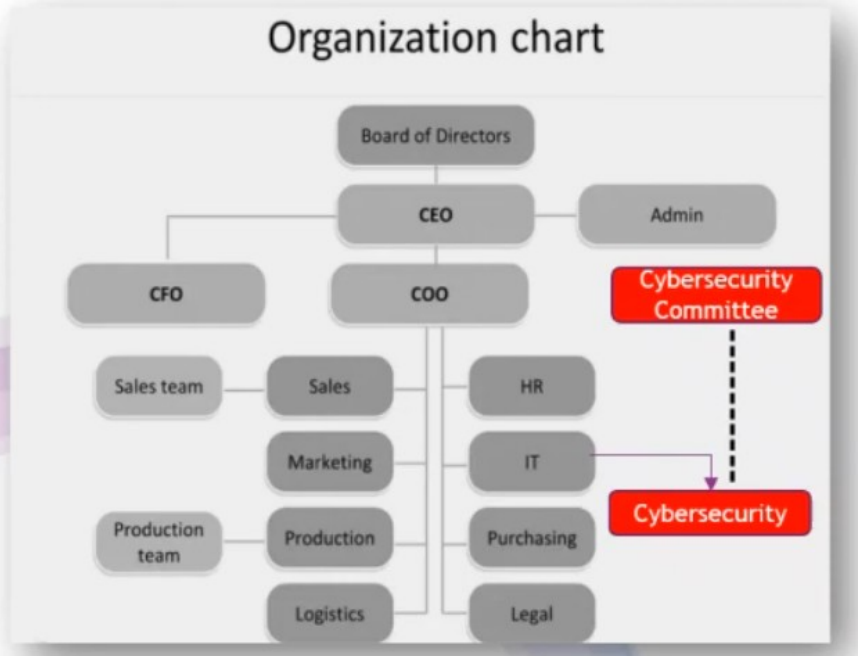
ISO27001:2022
Lec9

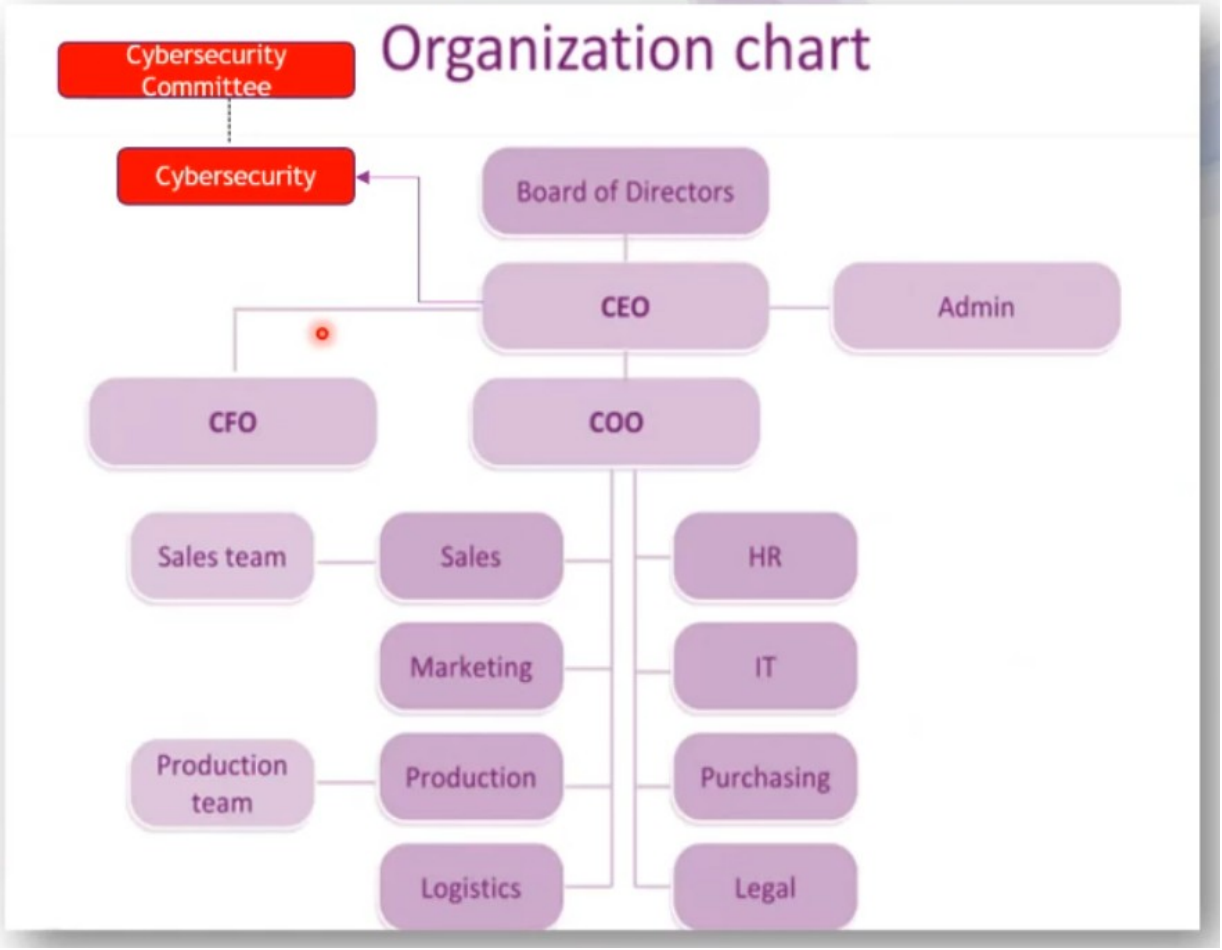
How to achieve this control ?

Prepare a business case to convince the management and take their commitment on the ISO 27001 Implementation

Old School



New School

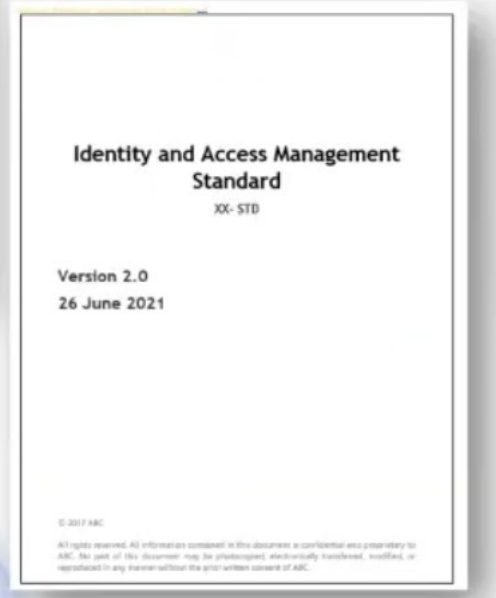


Identity and Access Management Policy

XX- PL

Version 4.0

26 June 2021



Identity and Access Management Standard

XX- STD

Version 2.0

26 June 2021

Identity and Access Management Procedures

XX-PR

Version 2.0

26 June 2021

User Profile Request Form (UPR)

Form ID: XX-FRM

User Details:

☐ Permanent ☐ Temporary

First Name: ..... Last Name: .....

Staff ID: ..... Department: .....

Joining Date: .....

HR Manager Approval/Respective Manager Approval:

Purpose:

☐ User Registration

Access Gained:

☐ Network Account	☐ ERP System
☐ Email Account	
☐ Internet Access	☐ Accounting System
☐ Direct Telephone line	

Asset Received:

.....

.....

Department Head Approval:

☐ User Access Changes

Access Changed:

☐ Network Account	☐ CRM
☐ Email Account	☐ HR/PAYROLL
☐ Internet Access	

How many policies should you developed ?

It is based on your organization !

How many Standards should you developed ?

It is based on your organization !

How many Procedure should you developed ?

It is based on your organization !

How many Forms should you developed ?

It is based on your organization !

The result of implementing the policies, procedures and standards shall produce records and logs (Evidence)

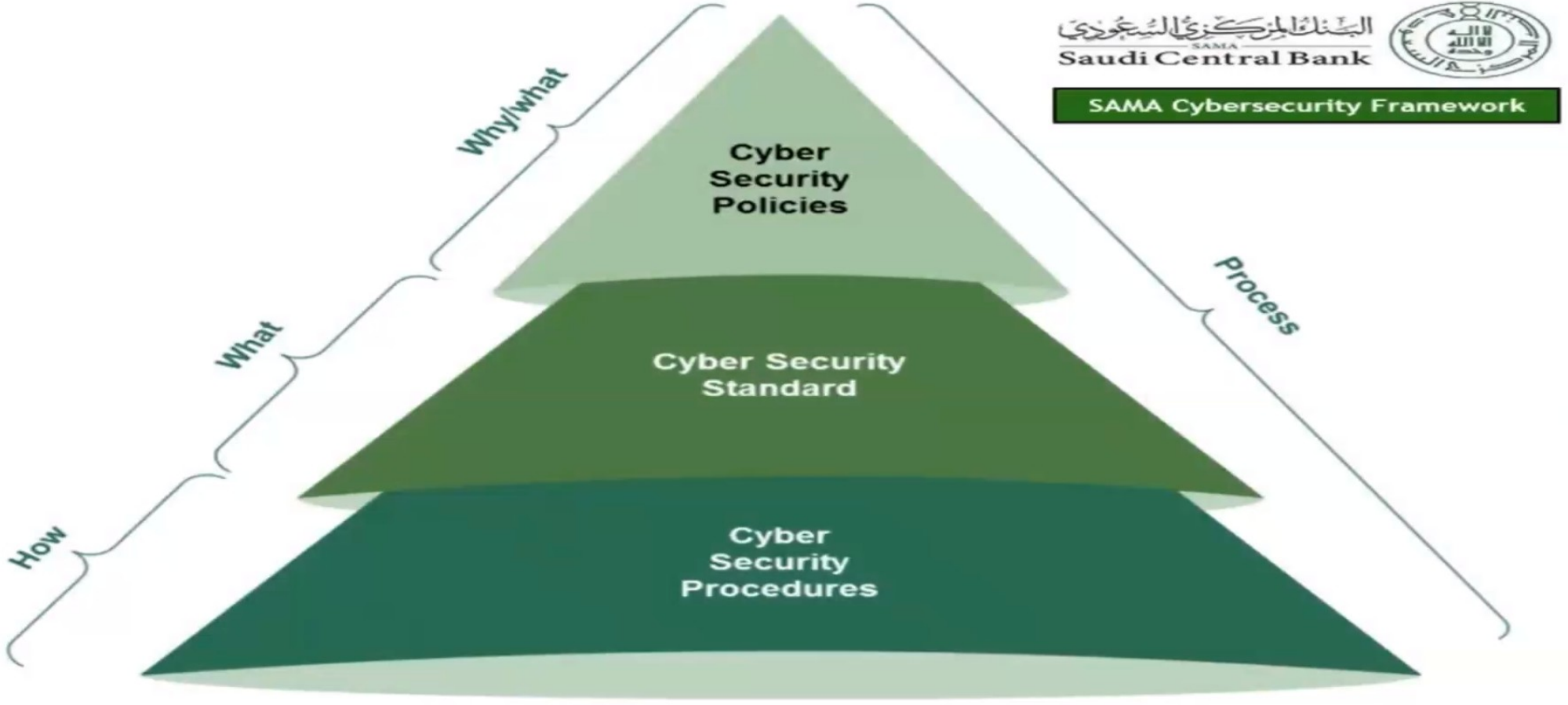


Figure 3 - Cyber Security Documentation Pyramid

NCA - ECC CONTROLS

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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.

SAMA - CYBERSECURITY FRAMEWORK

البنك المركزي السعودي
SAMA
Saudi Central Bank

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.

3.1.4 Cyber Security Roles and Responsibilities

Principle

Responsibilities to implement, maintain, support and promote cyber security should be defined throughout the Member Organization. Additionally, all parties involved in cyber security should understand and take their role and responsibilities.

Objective

To ensure that relevant stakeholders are aware of the responsibilities with regard to cyber security and apply cyber security controls throughout the Member Organization.

Control considerations

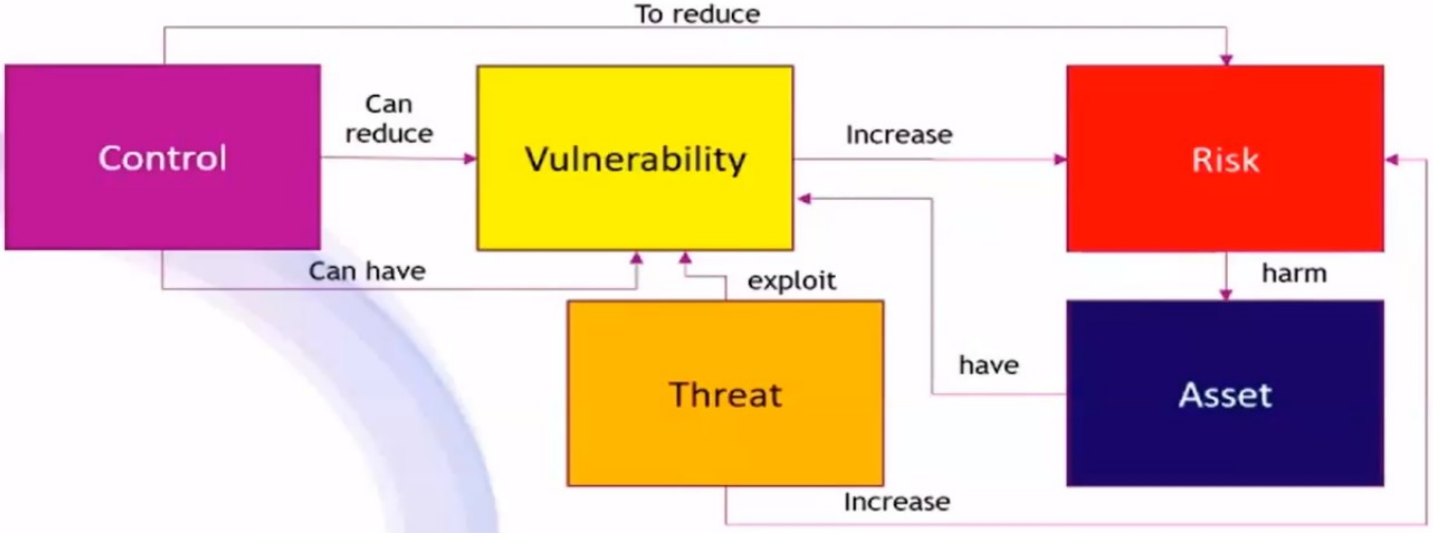
1. The Board of Directors has the ultimate responsibility for cyber security, including:
   a. ensuring that sufficient budget for cyber security is allocated;
   b. approving the cyber security committee charter;
   c. endorsing (after being approved by the cyber security committee):
      1. the cyber security governance;
      2. the cyber security strategy;
      3. the cyber security policy.
2. The cyber security committee should be responsible for:
   a. monitoring, reviewing and communicating the Member Organization's cyber security risk appetite periodically or upon a material change in the risk appetite;
   b. reviewing the cyber security strategy to ensure that it supports the Member Organization objectives;
   c. approving, communicating, supporting and monitoring:
      1. the cyber security governance;
      2. the cyber security strategy;
      3. the cyber security policy;
      4. cyber security programs (e.g., awareness program, data classification program, data privacy, data leakage prevention, key cyber security improvements);
      5. cyber security risk management process;
      6. the key risk indicators (KRIs) and key performance indicators (KPIs) for cyber security.
3. The senior management should be responsible for:
   a. ensuring that standards, processes and procedures reflect security requirements (if applicable);
   b. ensuring that individuals accept and comply with the cyber security policy, supporting standards and procedures when they are issued and updated;
   c. ensuring that cyber security responsibilities are incorporated in the job descriptions of key positions and cyber security staff.
4. The CISO should be responsible for:
   a. developing and maintaining:
      1. cyber security strategy;
      2. cyber security policy;
      3. cyber security architecture;
      4. cyber security risk management process;
   b. ensuring that detailed security standards and procedures are established, approved and implemented;
   c. delivering risk-based cyber security solutions that address people, process and technology;
   d. developing the cyber security staff to deliver cyber security solutions in a business context;
   e. the cyber security activities across the Member Organization, including:
      1. monitoring of the cyber security activities (SOC monitoring);
      2. monitoring of compliance with cyber security regulations, policies, standards and procedures;
      3. overseeing the investigation of cyber security incidents;
      4. gathering and analyzing threat intelligence from internal and external sources;
      5. performing cyber security reviews;
   f. conducting cyber security risk assessments on the Members Organization's information assets;
   g. proactively supporting other functions on cyber security, including:
      1. performing information and system classifications;
      2. determining cyber security requirements for important projects;
      3. performing cyber security reviews.
   h. defining and conducting the cyber security awareness programs;
   i. measuring and reporting the KRIs and KPIs on:
      1. cyber security strategy;
      2. cyber security policy compliance;
      3. cyber security standards and procedures;
      4. cyber security programs (e.g., awareness program, data classification program, key cyber security improvements).
5. The internal audit function should be responsible for:
   a. performing cyber security audits.
6. All Member Organization's staff should be responsible for:
   a. complying with cyber security policy, standards and procedures.

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

- Discourage or prevent the appearance of problems

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

- Search for, detect and identify problems

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

- Solve problems found and prevent the recurrence

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

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

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.


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.

Bureau Veritas Certification

AEON THANA SINSAP (THAILAND) PUBLIC COMPANY LIMITED

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013

Scope of certification

The following site is part of the Management System of the above organization

HEAD OFFICE

388 EXCHANGE TOWER, 26TH - 27TH &33RD - 34TH FLOOR, SUKHUMVIT ROAD, KHWAENG KLONGTOEY, KHET KLONGTOEY, BANGKOK 10110 THAILAND

RETAIL FINANCE BUSINESS COMPRISING CREDIT CARD, LOAN, HIRE PURCHASE MOTORCYCLE, WEB BUSINESS SERVICE AND USED CAR HIRE PURCHASE COVERING THE FOLLOWING DEPARTMENTS: FINANCE & ACCOUNTING SHARED SERVICE CENTER, SYSTEM PLANNING, I.T., SYSTEM DEVELOPMENT, MARKETING, CORPORATE GOVERNANCE & CONTROL, BUSINESS CONTROL MANAGEMENT AND LEGAL

STATEMENT OF APPLICABILITY (SOA), VERSION 2.0, EFFECTIVE DATE: NOVEMBER 03, 2014

Certificate No.: TH015313-001 Version: 01 Issue Date: 18-06-2020

The validity of this certificate depends on the validity of the main certificate

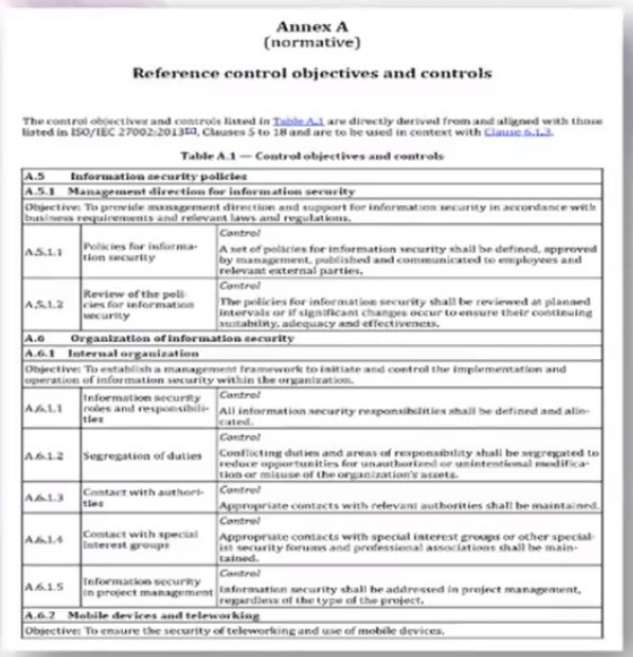
UKAS

Certification Body Address: 5th Floor , 66 Prescot Street, London, E1 8HG, United Kingdom

Local office: Bureau Veritas Certification (Thailand) Ltd. 16th Floor, Bangkok Tower, 2170 New Petchburi Road, Bangkapi, Huaykwang, Bangkok 10310, Thailand

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.

To check this certificate validity please call: +662 670 4800



Annex A
(normative)

Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

A.5	**Information security policies**	
A.5.1	**Management direction for information security**	
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6	**Organization of information security**	
A.6.1	**Internal organization**	
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.5	Information security in project management	*Control* Information security shall be addressed in project management, regardless of the type of the project.
A.6.2	**Mobile devices and teleworking**	
Objective: To ensure the security of teleworking and use of mobile devices.		

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

Exercise: Determine the proper root cause of the following nonconformity and edit the existing recommendation

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		

1. Prepare all the controls with the all justifications
2. Prepare the Information security risk assessment report with treatment plan
3. Grant Approvals form Management

ABC Company	DOCUMENT NUMBER: ABC-03
SUBJECT: ISMS STATEMENT OF APPLICABILITY	VERSION:2.0
CLASSIFICATION: INTERNAL	ISSUED: 06/01/2021
PAGE (1 OF 18)	NEXT REVISION: 06/01/2022

ISMS Statement of Applicability

REVISION HISTORY

Revision Date	List of Changes	Version	Author	Approved By
Jan, 2020	First Release	1.0	Head of Cybersecurity	GCS-SC
Jan, 2021	Review	2.0	Cybersecurity Department	GCS-SC

DISTRIBUTION TABLE

Title	Access Type
Head of Cybersecurity	View / Modify
Head of IT	View Only
GCS-SC	View Only

	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!