King AbdulAziz University
Cyber-Security Center

Cyber-Security Strategy

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022	
Reviewer	The Strategic Center for Realizing the Kingdom’s Vision		

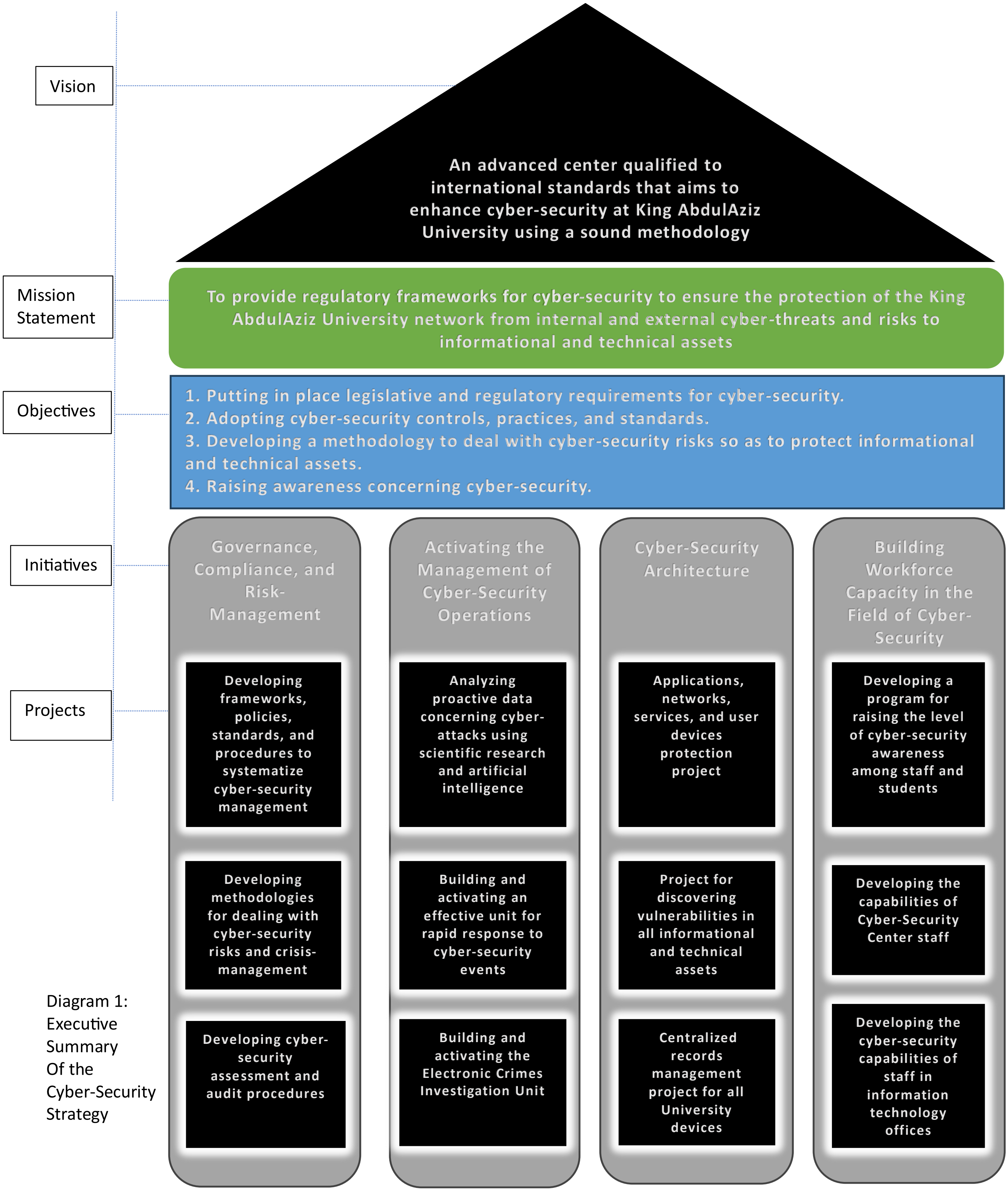
Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	30/10/2022 CE	Daniyal ibn Muhammad al-Ghazzawi	

Table of Contents

Executive Summary

King AbdulAziz University seeks to develop its capabilities in the field of cyber-security, to maintain and enhance cyber-security at King AbdulAziz University, and to protect the University from internal and external cyber-security risks. King AbdulAziz University has prepared this Cyber-Security Strategy in order to confront and analyze threats, reduce cyber-risks, and to achieve between enhancing cyber-security, raising trust, and contributing to growth and prosperity.



Vision

An advanced center qualified to international standards that aims to enhance cyber-security at King AbdulAziz University using a sound methodology

Mission Statement

To provide regulatory frameworks for cyber-security to ensure the protection of the King AbdulAziz University network from internal and external cyber-threats and risks to informational and technical assets

Objectives

1. Putting in place legislative and regulatory requirements for cyber-security.
2. Adopting cyber-security controls, practices, and standards.
3. Developing a methodology to deal with cyber-security risks so as to protect informational and technical assets.
4. Raising awareness concerning cyber-security.

Initiatives

Projects

Governance, Compliance, and Risk-Management

- Developing frameworks, policies, standards, and procedures to systematize cyber-security management
- Developing methodologies for dealing with cyber-security risks and crisis-management
- Developing cyber-security assessment and audit procedures

Activating the Management of Cyber-Security Operations

- Analyzing proactive data concerning cyber-attacks using scientific research and artificial intelligence
- Building and activating an effective unit for rapid response to cyber-security events
- Building and activating the Electronic Crimes Investigation Unit

Cyber-Security Architecture

- Applications, networks, services, and user devices protection project
- Project for discovering vulnerabilities in all informational and technical assets
- Centralized records management project for all University devices

Building Workforce Capacity in the Field of Cyber-Security

- Developing a program for raising the level of cyber-security awareness among staff and students
- Developing the capabilities of Cyber-Security Center staff
- Developing the cyber-security capabilities of staff in information technology offices

Diagram 1: Executive Summary Of the Cyber-Security Strategy

Introduction

King AbdulAziz University seeks to achieve integrated governance of cyber-security at the University level to reduce risks, strengthen trust and confidence, and enable growth, as well as to develop its capabilities in the field of cyber-security, aiming to improve, maintain, and enhance the level of King AbdulAziz University's cyber-security and to protect the University from internal and external cyber-risks. Thus King AbdulAziz University has prepared this Cyber-Security Strategy to support King AbdulAziz University's operational strategy, to confront cyber-threats, and to reduce cyber-risks.

This Strategy is fundamentally intended for the Director of the Cyber-Security Center, members of the Supervisory Committee for Cyber-Security, consultants of the King AbdulAziz University Cyber-Security Center, and other specialists in this field. Cyber-security is the responsibility of all King AbdulAziz University employees, including external parties.

The Cyber-Security Strategy was developed to provide recommendations relating to cyber-security operations at King AbdulAziz University in a manner consistent with the nature of the work, so as to enable operational initiatives, and to provide a clear and unified vision in alignment with the Kingdom's Vision 2030. It is intended to be disseminated among all departments, divisions, and branches of King AbdulAziz University, as well as entities and companies affiliated to the University.

This document aims to comply with cyber-security requirements and related legislative and regulatory requirements, which is itself a legislative requirement expressed in Control 1-1-1 of the Essential Cyber-Security Controls promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

The Cyber-Security Strategy covers all of the work of King AbdulAziz University, and the University itself and its affiliated entities and companies will endeavor to implement it.

Cybersecurity Vision

1. The Cyber-Security Vision provides a brief description of the position that King AbdulAziz University aspires to reach as regards its cyber-security situation over the course of the next three years, and also describes the cyber-security situation targeted for the future of the University.
2. The University's Cyber-Security Center has taken into consideration the University's objectives to ensure their compatibility with the Cyber-Security Vision.

The Cyber-Security Vision

An advanced center qualified to international standards that aims to enhance cyber-security at King AbdulAziz University using a sound methodology.

Inputs into the Strategy

The vision and orientations of the Kingdom of Saudi Arabia in the field of cyber-security are among the fundamental inputs into the development of King AbdulAziz University's Cyber-Security Strategy. Following on from this, understanding the role of King AbdulAziz University in and contribution to the National Cyber-Security Strategy is important for alignment of the objectives of the University's Cyber-Security Strategy with the objectives of the National Strategy and the realization of Vision 2030.

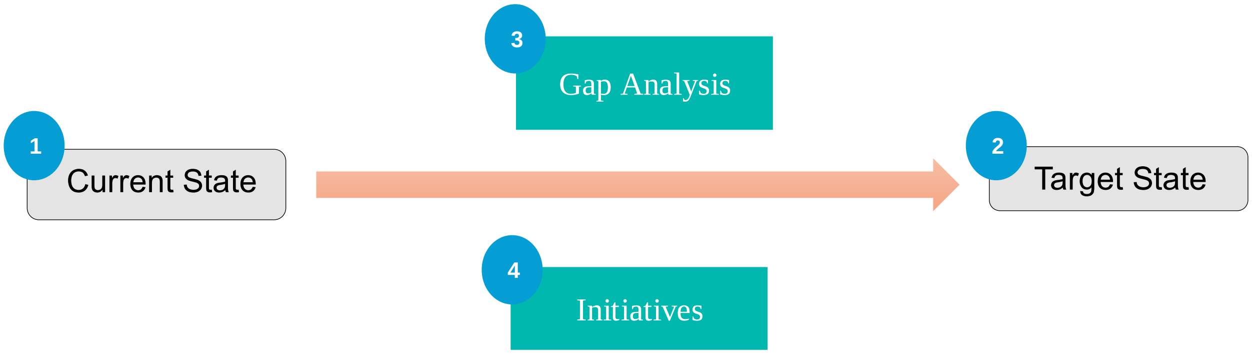


Diagram 2: Components of the Strategy

The Current Cyber-Security Situation

The operations set forth below present examples of the inputs that go into forming the Cyber-Security Strategy of King AbdulAziz University in accordance with the Cyber-Security Strategy. The objective of these operations is to define the target state of cyber-security in comparison to the current situation:

1. Assessment of the level of compliance with national regulatory and legislative requirements, such as the Essential Cyber-Security Controls (ECC).
2. Assessment of the level of compliance with the requirements of international information security management systems, such as ISO27001.
3. Cyber-Security Risk Assessment (CSRA).
4. Cyber-Security Maturity Assessment (CSMA).

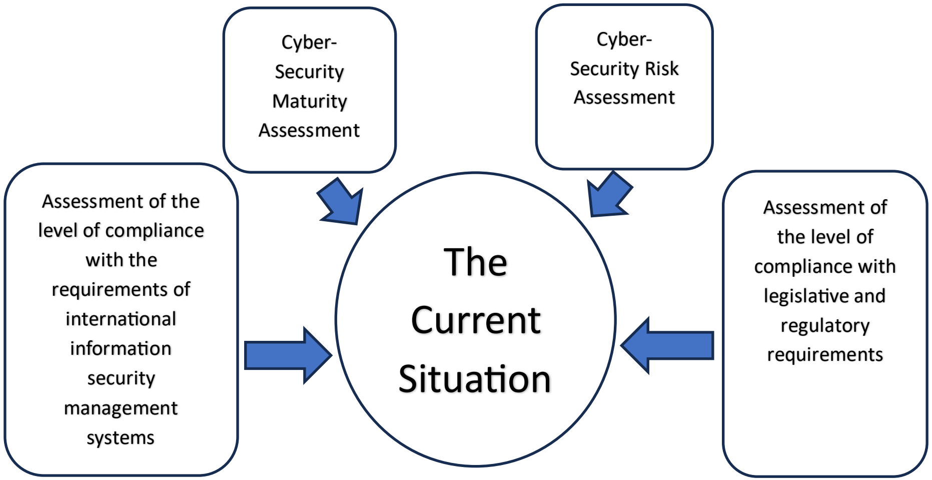

Cyber-Security Maturity Assessment
Cyber-Security Risk Assessment
Assessment of the level of compliance with the requirements of international information security management systems
The Current Situation
Assessment of the level of compliance with legislative and regulatory requirements

Diagram 3: Mechanism for Defining the Current Situation

Cyber-Security Objectives

The Cyber-Security Objectives are defined in accordance with the Cyber-Security Vision and the results of the assessments set forth in the Current Cyber-Security Situation section, above, as follows:

1. Supporting the Operations Strategy of King AbdulAziz University: Ensuring the contribution of cyber-security action plans, objectives, initiatives, and projects within King AbdulAziz University to achieve the relevant legislative and regulatory objectives and requirements.

2. Protecting Informational and Technical Assets at King AbdulAziz University: Providing the necessary technical solutions to protect informational and technical assets at King AbdulAziz University.

3. Promoting Engagement in Best Practices in the Field of Cyber-Security: Developing the skills and qualifications of employees in the field of cyber-security, promoting awareness of cyber-security through multiple channels, and building a positive culture of cyber-security.

Gap Analysis

Based on the results obtained from assessment of the level of compliance in the application of the Essential Cyber-Security Controls, the Cyber-Security Risk Assessment, analysis of operational impact, and the Cyber-Security Maturity Assessment, a SWOT-square analysis is conducted for King AbdulAziz University to analyze the gaps between the current situation and the target situation for cyber-security at the University. Such analysis demonstrates the University's strengths and weaknesses, the opportunities that the University may exploit, and the threats that it faces.

	Beneficial	Harmful
Internal	Strengths (Interior elements that distinguish the University) • The presence of an information security research group that includes Ph.D.-qualified experts in the field of cyber-security • The existence of specific, specialized academic programs in the fields of cyber-security and crisis management. • The presence of a system for administrative communications and electronic transactions that allows for the application of complete encryption solutions.	Weaknesses (Interior elements that negatively affect the University) • Lack of sufficient awareness concerning cyber-security and cyber-security threats and risks among employees. • Lack of solutions to protect against advanced and persistent threats. • University students are among the most important sources of internal threats. • Lack of adequate technologies for the protection of wireless networks.

External	Opportunities (External elements that may be exploited to the benefit of the University) • Many of the University’s talented and capable graduates work in the field of cyber-security. • The establishment of the National Authority for Cyber-Security, which supports entities in responding to cyber-security incidents. • The initiatives of the National Authority for Cyber-Security to train specialists in the field of cyber-security.	Threats (External elements that may cause some problems for the University) • The continuous development of cyber-security protection systems. • Rapid and continuous advancement in technology has caused current systems to be unable to support cyber-security applications. • The presence of sensitive systems within the University and the provision of its services abroad have caused University systems to be the target of cyber-attacks.

Cyber-Security Initiatives

The cyber-security initiatives comprise all projects and programs required to implement the objectives of the Cyber-Security Strategy. These initiatives are formed on the basis of the Cyber-Security Vision and Objectives, as follows:

- **Governance, Compliance, and Risk-Management:** The initiatives category includes projects and programs concerned with governance, risks, and compliance aimed at enhancing cyber-security at King AbdulAziz University and at constructing strategic plans for cyber-security.
- **Activating the Management of Cyber-Security Operations:** The initiatives category includes projects and programs that assist King AbdulAziz University in quickly recognizing and resolving internal and external threats.
- **Cyber-Security Architecture:** The initiatives category includes projects and programs that assist King AbdulAziz University to increase its level of maturity in cyber-security and to protect the University from cyber-risks.
- **Building Workforce Capacity in the Field of Cyber-Security:** The initiatives category includes projects and programs aimed at raising awareness of cyber-security, edifying employees of the Cyber-Security Center and the University with skills and qualifications in the field of cyber-security, and creating a vital environment for innovation in cyber-security.

The table below shows the relation between the Cyber-Security Objectives and the Cyber-Security Initiatives:

Initiatives Objectives	Governance, Compliance, and Risk-Management	Activating the Management of Cyber-Security Operations	Cyber-Security Architecture	Building Workforce Capacity in the Field of Cyber-Security
Putting in place legislative and regulatory requirements for cyber-security	√	–	–	–
Adopting cyber-security controls, practices, and standards.	√	–	–	–
Developing a methodology to deal with cyber-security risks so as to protect informational and technical assets.	√	√	√	–
Raising awareness concerning cyber-security	–	√	–	√

The Cyber-Security Initiatives can be measured using the following metrics:

Year 1

No.	Cyber-Security Initiative	Operational Cyber-Security Key Performance Indicator	Objective		
			Year 1	Year 2	Year 3
1	Governance, Compliance, and Risk-Management	Percentage Implementation of the Essential Cyber-Security Controls (ECC)	60%	75%	90%
		Number of new projects and technological changes for which a cyber-security risk assessment has been conducted	4	6	8
		Number of assessed policies	5	11	27
		Number of reports submitted to the Supervisory Committee regarding the University's Cyber-Security Performance Index	4	4	4
2	Activating Cyber-Security Management Operations	Number of research projects carried out on the basis of internal data using artificial intelligence	1	2	3
		Number of cyber-crimes investigated and addressed by the Center's team	3	4	5
		Number of cyber-incidents responded to and addressed	15/day	10/day	5/day
3	Cyber-Security Architecture	Development of a unified identity system for all University applications and networks	All applications	All network components and services	Linkage of the system with Employee Affairs
		Level of wireless network coverage of the Mobile Device Management system (MDM)	100% WLAN coverage	100% WLAN and wireless network coverage in branches	Complete, 100% wireless network coverage on the Main Campus and in branches
		Level of device and application coverage in the Records Management System	100% coverage for all servers	100% coverage for all network devices	100% coverage for all user devices
4	Building Workforce Capabilities in the Field of Cyber-Security	Number of awareness cards sent to raise awareness regarding cyber-security	21	21	21
		Number of training and awareness workshops concerning cyber-security held for employees in information technology departments	4	6	8
		Number of specialized training courses held for employees of the Cyber-Security Center to develop their skills	5	10	15

Cyber-Security Budget

The purpose of the cyber-security budget is to determine the budget necessary for the implementation of the Cyber-Security Strategy and Initiatives, and to obtain the funds necessary for its allocation by the relevant offices at the University.

Budget Characteristics

1. The Cyber-Security Center is responsible for preparing the Cyber-Security Budget so as to ensure the provision of cyber-security technologies and tools in the best way possible. The Director of the Cyber-Security Center is also responsible for submitting a summary of expenditures related to the Cyber-Security Budget to the President of the University.
2. The Cyber-Security Budget must be consistent with relevant policies, legislative and regulatory requirements, orders, and decisions.
3. The Cyber-Security Budget is determined based on the annual budget cycle of King AbdulAziz University.
4. The Cyber-Security Budget is subjected to annual review in accordance with the policies and procedures adopted by King AbdulAziz University.

Components of the Budget

The Cyber-Security Budget is comprised of the following components:

1. The Operations Budget of the Cyber-Security Center, which includes the cost of consulting services, the costs of technical services, and other costs.
2. The Initiatives Budget of the Cyber-Security Center, which includes non-recurring costs incurred for the construction of the Center and operations related to the implementation of the Cyber-Security Strategy, as well as recurring costs that cover cyber-security measures and programs for specialized skills development and necessary training for the Center’s employees, such as training courses and conferences.

Calculating the Cyber-Security Budget

1. The budget of the Cyber-Security Center at King AbdulAziz University is calculated in accordance with the research activity conducted by the Deanship of Information Technology over recent years.
2. The budget of the Cyber-Security Center, as allocated by King AbdulAziz University for the Cyber-Security Strategy over the course of the next three years, is as follows: 45,000,000 Saudi riyals for the first year, 56,000,000 Saudi riyals for the second year, and 67,000,000 Saudi riyals for the third year.

Roles and Responsibilities

–Responsible Party and Owner of the Document: Director of the Cyber-Security Center.
–Updating and Review of the Document: The Cyber-Security Center.
–Implementation and Application of the Document: The Cyber-Security Center.