


King AbdulAziz University
Cyber-Security Center

Cyber-Security Assessment and Audit Policy

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022 CE	

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	15/11/2021 CE	Shuruq bint Khalid Banafi	
1.1	14/11/2022 CE	Maram bint Khalid Hambishi	In accordance with the requirements of the Authority

Table of Contents

<i>Objectives</i>	4
<i>Scope and Applicability of the Work</i>	4
<i>Policy Clauses</i>	4
<i>Roles and Responsibilities</i>	5
<i>Compliance with the Policy</i>	5

Objectives

This policy aims to define, based on best practices and standards, the cyber-security requirements for assessment and audit of cyber-security controls at King AbdulAziz University, and to ensure their implementation and operation in accordance with the regulatory policies and procedures of King AbdulAziz University, as well as with the relevant national legislative and regulatory requirements, and with international requirements regulatorily approved by King AbdulAziz University.

This policy follows the relevant national legislative and regulatory requirements and international best practices, which is itself a legislative requirement expressed in Control 1-8-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

This policy covers all cyber-security controls at King AbdulAziz University, and applies to all King AbdulAziz University employees.

Policy Clauses

1-1 The Cyber-Security center must review the implementation of the Cyber-Security Controls on a periodic basis, as well as the extent of compliance with the Essential Cyber-Security Controls (ECC:1-2018) and the Cyber-Security Controls for Critical Systems (CSCC-1:2019) promulgated by the National Cyber-Security Authority.

1-2 Assessment and audit of the application of the Cyber-Security Controls must be carried out on a periodic basis by parties independent from the Cyber-Security Center, such as the Deanship of Quality and Academic Accreditation or external parties.

1-3 Review of the application of the Cyber-Security Controls for Critical Systems must be carried out at least once every three years by parties within King AbdulAziz University independent from the Cyber-Security Center.

1-4 The application of the Cyber-Security Controls must be ensured periodically, and at least once annually for critical systems, to ensure their alignment with the Essential Cyber-Security Controls (ECC:1-2018) and the Cyber-Security Controls for Critical Systems (CSCC-1:2019).

1-5 Cyber-security assessment and audit procedures must be defined and documented.

1-6 Cyber-security assessment and audit results must be documented and discussed with the offices concerned.

1-7 Results must be presented to the Supervisory Committee for Cyber-Security and the responsible authority. Results must also include the scope of assessment and audit, observations detected, recommendations and corrective procedures, risk assessments, and plans for addressing observations.

1-8 The following Responsibility Assignment Matrix (RACI chart) must be relied upon in the implementation of cyber-security audit and assessment processes:

	Deanship of Quality and Academic Excellence	Governance, Risk, and Compliance Office	Cyber-Security Center	Director of the Cyber-Security Center	Director of the Cyber-Security Center	President of the University
Cyber-Security Assessment	R		R	A	I	I
Cyber-Security Audit	R	R	I	I	A	I
Implementing Corrective Procedures	C/I	C/I	R	R	A	I

2- Other Requirements

2-1 The Cyber-Security Center must take proactive and corrective measures in response to assessment and audit results.

2-2 The Cyber-Security Center must identify the factors that led to the observations detected, analyze them, understand what caused them, and limit their recurrence.

2-3 The Cyber-Security Assessment and Audit Policy must be reviewed annually, and changes to it must be documented and approved.

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 Governance, Risk, and Compliance Office with the Cyber-Security Center.

Compliance with the Policy

1- The Director of the Cyber-Security Center must ensure the compliance of King AbdulAziz University with this policy periodically.

2- All employees of King AbdulAziz University must comply with this policy.

3- Any violation of this policy may subject the offender to disciplinary action, in accordance with the procedures followed by King AbdulAziz University.