INTERNAL AUDIT PROCEDURE

KING SAUD UNIVERSITY

DEANSHIP OF E-TRANSACTIONS & COMMUNICATION

VERSION 1.1

INTERNAL USE ONLY

PREPARED BY	REVIEWED BY	APPROVED BY
ALTAMASH SAYED	NASSER A. AMMAR	DR. MOHAMMED A ALNUEM

REVISION HISTORY

Sr. No.	Date of Revision	Ver.	Validity	Description of change	Reviewed By	Approved By
1	18/03/12	1.0	One Year	Initialization	Nasser A. Ammar	Dr. Mohammed A Alnuem
2	02/03/13	1.1	One Year	Department Ownership Changed	Mr. Toqeer Ahmad	Mr. Mohammed A. Alsarkhi
3	05/03/13	1.1	One Year	No Change	Mr. Toqeer Ahmad	Mr. Mohammed A. Alsarkhi
4						
5						
6						
7						
8						
9						
10						

DISTRIBUTION LIST

Sr. No	Version Number	Name	Designation	Department
1				
2				
3				

TABLE OF CONTENTS

1. PURPOSE

To provide a formal, precise, complete and detailed plan on which the ISMS audit will be carried out. The objective of the audit is to check over a specified regular audit period that all aspects of the ISMS are functioning as intended and the compliance of the ISMS to the ISO 27001 standard is maintained at an acceptable level.

2. SCOPE

This procedure applies to King Saud University (KSU) - eTransactions & Communication (ETC) Deanship and all parties, its affiliated partners or subsidiaries, including data processing and process control systems, that are in possession of or using information and/or facilities owned by KSU-ETC Deanship.

This procedure applies to all staff/ users that are directly or indirectly employed by KSU-ETC Deanship, subsidiaries or any entity conducting work on behalf of KSU that involves the use of information assets owned by ETC Deanship.

3. RELATED POLICIES AND PROCEDURES

- Compliance Policy.

4. PROCEDURE ENFORCEMENT / COMPLIANCE

Compliance with this procedure is mandatory and ETC Deanship managers shall ensure continuous compliance monitoring within their departments. Compliance with the statements of this procedure is a matter of periodic review by Risk & Information Security Department and any violation of the procedure will result in corrective action by the ISMS Steering Committee.

Disciplinary action will be depending on the severity of the violation which will be determined by the investigations. Actions such as termination or others as deemed appropriate by ETC Management and Human Resources Department will be taken.

5. DOCUMENT OWNER

- ISMS Manager

6. ROLES & RESPONSIBILITY

Each role involved in this procedure shall have main responsibilities as follows:

1. **ISMS Manager**
   - *Approves the Annual Audit Plan and ensures that all steps within this procedure are executed correctly and timely.*
   - *Reports Non-compliance to ISMS Management Steering Committee.*
   - *Develops, maintains, updates and implements the procedure.*
   - *If an audit produces findings, the ISMS Manager and the ISMS Audit Team, must develop an action plan and schedule a follow up audit.*

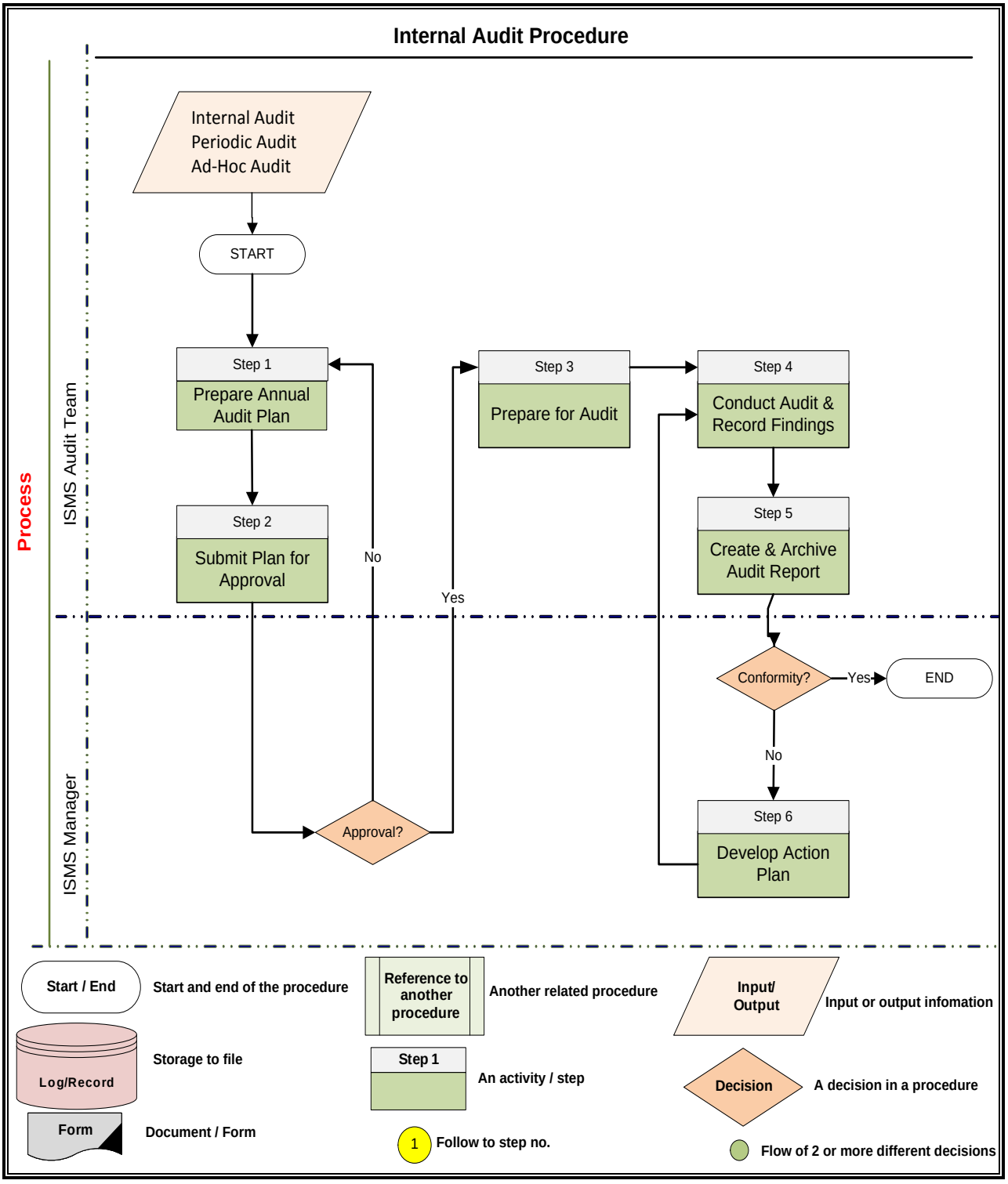
2. **ISMS Audit Team**
   - *The ISMS Audit Team is responsible for ensuring compliance with the information security practices, policies and procedures.*
   - *Manage all information security auditing activities.*
   - *Develop the annual audit plan.*
   - *Monitor the compliance with the information security policies, procedures, guidelines and standards along with external chosen standards.*
   - *Report audit findings to the ISMS Manager.*
   - *If an audit produces findings, the ISMS Manager and the ISMS Audit Team, must develop an action plan and schedule a follow up audit.*

7. INVOCATION

This procedure shall be followed whenever there is:

- ***Annual Audit Plan***

8. PROCESS FLOWCHART



9. PROCEDURE DETAILS

This section reflects the broad activities/steps to be carried out in the procedure.

STEP 1 : PREPARE ANNUAL AUDIT PLAN	
Responsibility	ISMS Audit Team
Input	• Security related incidents that have occurred since last audit. • Security related personnel issues that have arisen since last audit. • Results of any risk assessment undertaken since the last audit and discussion of the proposed controls. • Designation of people or processes to manage risks (e.g. insurance). • Proposed changes to the Security Policy. • Implementation progress reports of previously decided actions.
Actions	• The ISMS Audit Team prepares the Annual Audit Plan covering the type of audits as well as the frequency and methods of audit. The annual audit plan takes into consideration the status and importance of the processes and areas to be audited, the Risk Assessment report, as well as the results of previous audits.
Output	Annual Audit Plan

STEP 2 : SUBMIT PLAN FOR APPROVAL	
Responsibility	ISMS Audit Team
Input	• Annual Audit Plan
Actions	• The ISMS Audit Team submits the plan to the ISMS Manager for approval. Upon approval of the annual audit plan, the ISMS Audit Team communicates the plan to the interested parties (Audittees)
Output	Annual Audit Plan: • If Approved : Proceed to step 3 • If not Approved: Proceed to step 1

STEP 3 : PREPARE FOR AUDIT	
Responsibility	ISMS Audit Team
Input	• Annual Audit Plan • Periodic audit • Ad-hoc audit
Actions	• The ISMS Audit Team collects and studies previous audit findings and possible outstanding issues. Additionally, the team prepares all relevant documents that will be needed for the realization of the audit (e.g. ISMS Audit Checklist). Checklists or work-programs are instrumental in aiding an audit that is thorough, effective and uniform. • Periodic audit checklists / work-programs must be in-depth and based on ISO 27001 (using the template ISMS Audit Checklist), following a predefined path and checking for compliance with controls. Follow-up audit checklists/ work-programs must be limited to include only the relative audit findings. Ad-hoc audit checklists/ work-programs must always be focused on the trigger event. Therefore ad-hoc audit checklists must be created anew prior to each ad-hoc audit.
Output	ISMS Audit Checklist

STEP 4 : CONDUCT AUDIT & RECORD FINDINGS	
Responsibility	ISMS Audit Team
Input	• ISMS Audit Checklist • Annual Audit Plan
Actions	The ISMS Audit Team performs the audit and completes the pre-defined audit report. During the course of the audit the ISMS Audit Team tries to find adequate evidence to ascertain that: • The information security policy is still an accurate reflection of the business requirements. • An appropriate risk assessment methodology is being used. • The documented procedures are being followed (i.e. within the scope of the ISMS) and are meeting their desired objectives. • Technical controls (e.g. firewalls, physical access controls) are in place, are correctly configured and working as intended. • The residual risks have been assessed correctly and are still acceptable to the management of the company. • The agreed actions from previous audits and reviews have been implemented. • The ISMS is compliant with ISO 27001.
Output	Audit Findings (if any)

STEP 5 : CREATE & ARCHIVE AUDIT REPORT	
Responsibility	ISMS Audit Team
Input	Audit Findings
Actions	• Based on the audit findings, the ISMS Audit Team prepares the audit report. This is a report referring to non-compliance, unresolved issues, high residual risks, etc. Any audit finding must be labeled according to its priority level • Audit findings that are characterized as Priority 1 are major non-conformities and must be planned for resolution in a period of 2 weeks and a follow up audit must be scheduled at the end of that period. Note that if considered critical, the resolution of certain audit findings may be required ASAP • Audit findings that are characterized as Priority 2 are minor non-conformities and must be planned for resolution in a period of 3 months and a follow up audit must be scheduled at the end of that period • Audit findings that are characterized as Observation must be planned for resolution in a period of 6 months and their progress must be monitored in all of the following periodic audits until resolution • Audit findings and their corresponding non-conformance must be communicated to the ISMS Manager at the end of each audit
Output	Audit Report

STEP 6 : DEVELOP ACTION PLAN	
Responsibility	ISMS Manager
Input	• Annual Report
Actions	• According to the audit findings and the non-conformance level, an action plan and follow up audit must be developed. Follow-up audits are scheduled and performed when a previous audit has found critical non-conformances. The scope of follow-up audits is limited to the non-conformance and the same audit mechanisms that produced the finding are used.
Output	• Action Plan • Follow up Audit

10. OUTPUTS

The following activity will be an output of the process.

- ISMS Annual Audit Plan
- ISMS Audit Report
- Action Plan

11. RECORDS

The following are the list of all applicable records that are the evidence of implementation of the Process.

The records are maintained in hard and soft copy.

- ISMS Annual Audit Plan
- ISMS Audit Check List

12. ANNEXURE

INTERNAL AUDIT TEMPLATE										
Sr. No.	Department Audited	Non Conformity (NC) / Opportunity for Improvement (OI) / Noteworthy Effort (NE)	Description / Findings	ISO 27001 Clause No.	Planned Closure date	Responsibility	Root Cause Analysis	Corrective / Preventive Action	Evidence (Mention the specific record generated)	Status