**Republic of the Sudan**

**The National Audit Chamber (NAC)**

**History of SAIs**

It is established in 1920 as an audit department under the finance secretary.

An independent audit department headed by an auditor general was established in 1933 when the first Audit Act was adopted.

The temporary constitution of 1955 set aside special part for the Auditor General and guaranteed its independence and subordination to the Parliament and the Supreme Council.

1970’s Auditor General Act, replaced and updated the 1933 Act, defining the rights and duties of the Chamber incorporating the economic and administrative development of the state.

The1986 Act replaced and updated the1970 Act and introduced performance audit in addition to financial audit.Then it replaced in 2007 Act.

The last update was the 2015 Act that widely embowered the Chamber in terms of mandate and independence.

More emphasis placed upon performance audit, IT audit and Forensic audit.

* **Our SAI Sudan Experience on some of the topics specified for the IT Security Seminar:**

**Security Management:**

Our SAI focuses more on security management in auditing and the following are sample of the questionnaire questions used by our auditors on this area:

**PHYSICAL SECURITY**

1. Does the entity maintain written procedures to controls over the physical security of the computer equipment?

2. Is the physical location of the computer/server/storage/training rooms appropriate to ensure security?

3. Are physical access devices (i.e., card-key or combination lock systems) used to restrict entrance to the computer room?

4. Obtain documentation listing all individuals with access to the computer room.

5. Does the entity have any policies for temporary access by employees, visitors, or outside vendors? (e.g., are these individuals escorted during their activities, or are ID badges or sign-in logs used?)

6. Does the entity utilize monitoring software linked to the physical access device to electronically monitor computer room entrances?

a. Are access reports generated?

b. Are these reports reviewed by appropriate IT management?

7. Does the entity use plate glass or other techniques (e.g. surveillance cameras) to visually monitor computer room access?

8. Does the entity utilize procedures and devices to secure sensitive equipment and storage media from the risk of environmental damage, such as:

- Halon, CO¬¬2, or dry-piped water suppression systems?

- Hand held fire extinguishers?

- Smoke and heat sensors?

- Water detectors and humidity controls?

- Temperature controls and dedicated air conditioning units?

- An uninterruptible power supply (UPS), diesel or gas generators, or power generators?

9. For any other sensitive areas, are access controls to these areas adequate? Examples of sensitive areas (besides the computer room) would include communications closets, any UPS equipment, and tape libraries.

**LOGICAL ACCESS**

10. Does the entity maintain written policies or procedures related to the security controls over access to the system?

11. Does the entity utilize various levels of security products (e.g., security software, application and database security)?

12. Determine the types of controls that are in place over the issuance, maintenance, and termination of passwords. Do such controls include:

a. A security administrator designated to control password security?

b. Informing employees of proper password security throughtraining or signed security statements?

c. Unique passwords?

d. Passwords changed on a periodic basis?

e. Passwords cancelled or access rights modified in a timelymanner upon an employee's termination or transfer?

13. Are reports generated by the system's security software?

a. Are these reports regularly reviewed by the security administrator?

b. Are procedures in place to follow up on these reports?

14. Is sensitive data protected by restricted access or other controls?

**Cyber Security:**

Our SAI Sudan has started to focus on Cyber Security Audit as a specialized audit and made use of cyber security maturity assessment and the tools available for calculating cyber security maturity to measure the maturity of the auditee's cyber security capabilities, moreover the Information system audit department has started developing Cyber Security Audit manual to improve the audit process on this area and improve its deliverables consequently.

**Capacity Building:**

As a part of the mission Statement of SAI Sudan IS Audit Department Strategic Plan the IS Audit Department is committed to the implementation of the ISACA IS Audit and Assurance Standards and Guidelines & to the ISACA Code of professional ethics, one of the core competency of the SAI Sudan IS audit team and members are:

* Support the implementation, encourage compliance with, appropriate standards, procedures, for effective governance and management of enterprise information systems and technology, audit, control, security and risk management. .

Our SAI is also Developing IT audit Core groups; Cyber security core group is one of them. And two of this core group members participated in AFROSAI-E capacity building workshop on Cyber security last November.

**Role of SAIs in promoting and audit of IT Security:**

Our SAI Sudan has general controls working paper that contain a part for evaluating IT Security controls which include:

1. Level of IT Administration in the structure.
2. IT steering committee.
3. Access Controls (Physical Security – Logical Access).

Also SAI Sudan has risk assessment working papers to evaluate the risk in audited entities by making risk register and detecting inherent risks, including a part for assessing the cyber security risks.

Our information System Audit Department has developed audit universe application and Procedures used to know all critical information about our auditable entities in our country; some of the audit universe elements are about IT security since it is considered as critical indicator that gives some entities higher priority in planning audits.