

**MINISTRY OF EDUCATION**

**REPUBLIC OF KENYA**

**KENYA EDUCATION MANAGEMENT INSTITUTE**

**ICT INFRASTRUCTURE AUDIT REPORT**

**MAY 2019**

**Audit Team**:

Agnes Keli

Allan Kamau

Charles Waithiru

**Table of Contents**

[**ABBREVIATIONS** 3](#_Toc9444649)

[**EXECUTIVE SUMMARY** 4](#_Toc9444650)

[**Objective and Scope** 4](#_Toc9444651)

[**1.1 AUDIT SCOPE** 5](#_Toc9444652)

[**1.2 AUDIT OBJECTIVES** 6](#_Toc9444653)

[**1.3 AUDIT METHODOLOGY** 6](#_Toc9444654)

[**2. AUDIT FINDINGS AND RECOMMENDATIONS** 6](#_Toc9444655)

[**2.1 Management of ICT assets** 6](#_Toc9444656)

[**2.2 Network Security Management** ……..8](#_Toc9444657)

[**2.3 Physical and Environmental Security** 8](#_Toc9444658)

[**2.4 Structured Cabling** 9](#_Toc9444659)

[**2.5 Cabling security** 10](#_Toc9444660)

[**3. ANNEX** 10](#_Toc9444661)

# **ABBREVIATIONS**

|  |  |
| --- | --- |
| CCTV | * Closed-Circuit Television |
| COBIT | * Control Objectives for Information and related Technology |
| GOK | * Government of Kenya |
| ICT | * Information Communication Technology |
| IS | * Information System |
| ISACA | * Information Systems Audit and Control Association |
| IT | * Information Technology |
| KEMI | * Kenya Education Management Institute |

# **EXECUTIVE SUMMARY**

# **Objective and Scope**

The objective of the audit was;

* To provide management with an independent assessment relating to the effectiveness of the network infrastructure and identify opportunities for improvement.
* To determine whether adequate and effective IT asset management processes

and controls are in place

The scope of our audit was limited to KEMI offices in Nairobi and consisted of;

* An evaluation of the network design, current configuration set up and the general security review of the network infrastructure.
* Information technology hardware and software inventories, including IT asset management practices in place.

**Key Findings and Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Area** | **Key findings** | **Recommendations** |
| 1 | Management of ICT assets | The audit found that some ICT equipment had tags while some did not have. | Ensure that all equipment received through purchase are tagged appropriately |
| There was no software inventory to show a listing of installed software | The institution should have inventories for both hardware and software assets. |
| The ICT inventory was in hard copy records and in excel document. | KEMI should endeavor to automate the end user equipment inventory. |
| 2 | Physical and Environmental Security | There was no documentation to show that the fire suppression system had been inspected and tested. | Ensure that the fire suppression system is tested in compliance with industry and insurance standards and guidelines. |
| The air conditioner was not maintaining the required temperatures for the server room | Ensure that appropriate repair and maintenance procedures are carried out on the air conditioners. |
| The server room was found to be having combustible materials | Remove all the combustible materials form the server room |
| The server room was not fitted with biometric access system and there was also no CCTV monitoring system. | The management should ensure that the server room is fitted with biometric system as a best way of authenticating user access to the server room. The Perimeter of the server room site should be monitored by visible or infrared Closed Circuit Television System. |
| 3 | Network Security management | KEMI has no firewall system in place and hence lacked a security measure when establishing a connection from a local network to the internet. | Ensure that a firewall system is deployed to provide for adequate controls that will ensure prevention, detection, removal and reporting of the malicious code on all ICT assets. |
| 4 | Structured Cabling | Structured cabling had not been done in some building blocks and network cables were terminating to a network device in other blocks. | Ensure that structured cabling is implemented in all building blocks so as to have a complete Local Area Network in the institution. |

# **1.1 AUDIT SCOPE**

In accordance with the engagement letter, we performed an audit of KEMI ICT infrastructure, for the period of February, 2019.

The scope of our audit was limited to KEMI offices in Nairobi and consisted of;

* An evaluation of the network design, current configuration set up and the general security review of the network infrastructure.
* Information technology hardware and software inventories, including IT asset management practices in place.

**Audit Review Standards**

Our Scope was developed incorporating GOK ICT networks and end user devices standards.

This approach allowed us to review the network infrastructure and ICT assets management, as well as providing a standardized methodology for the audit processes.

# **1.2 AUDIT OBJECTIVES**

* To provide management with an independent assessment relating to the effectiveness of the network infrastructure and identify opportunities for improvement.
* To determine whether adequate and effective IT asset management processes and controls are in place

# **1.3 AUDIT METHODOLOGY**

Our review procedures included:

* Review of available documentation (such as the information technology and other related organizational policies and procedures)
* Inquiry and observation
* Review of the network architecture
* Inspection of ICT assets

**Conducting the Audit**

Our audit was conducted in accordance with IS Audit and Assurance Standards and IS Audit and Assurance Guidelines issued by ISACA, Government of Kenya ICT standards, and generally accepted industry practices. The audit criteria that was used in the audit included management policies and procedures, Government of Kenya ICT standards, and management control guidelines, which are outlined in COBIT® 5, as issued by ISACA.

# **2. AUDIT FINDINGS AND RECOMMENDATIONS**

The purpose of this section is to provide a detailed explanation of the audit findings and recommendations.

# **2.1 Management of ICT assets**

The audit expected to find that KEMI has processes and systems in place to record, track, monitor, and safeguard the ICT assets inventory.

***Finding #1***

Employees exiting the institution filled clearance forms indicating surrender of ICT equipment in their possession to the ICT unit

***Finding #2***

The audit found that some ICT equipment had tags while some did not have. There is a risk that IT asset purchases are not properly recorded, and that assets could be misappropriated.

***Finding #3***

There was an up to date ICT inventory for hardware which contained details on serial number, model, department.

***Finding #4***

The audit team noted that there was no software inventory to show a listing of installed software. Without this list, KEMI is unable to efficiently manage the purchase of software licences.

***Finding #5***

The ICT inventory was in hard copy records and in excel document. With spreadsheets, there is no method of tracking the history and movement of the asset, and no method of tracking an asset when it is moved from one spreadsheet to another. Therefore, an asset could be removed accidently (or intentionally) from the spreadsheet without any audit trail in the system.

***Finding #6***

The audit found that ownership of ICT assets was only assigned for computers.

***Recommendation #1***

Ensure that all equipment received through purchase are tagged appropriately.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

***Recommendation #2***

The institution should have inventories for both hardware and software assets. The hardware asset register should contain details on tracking information, maintenance schedules and warranty information. The software asset register should contain details on software name, software purpose, scope of use and anticipated end of life.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

***Recommendation #3***

KEMI should endeavor to automate the end user equipment inventory. The institution should implement one tracking tool for hardware and software inventory, which would enable KEMI to efficiently track all IT assets.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

***Recommendation #4***

As an improvement there is need for each information asset to be assigned an owner. Some of these assets include printers, copiers and other devices.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

## **2.2 Network Security Management**

***Finding #7***

The networking devices had been configured with subnets to divide the network into different logical networks

***Finding #8***

KEMI has no firewall system in place and this meant that it lacked a security measure when establishing a connection from a local network to the internet.

***Recommendation #5***

The institution should ensure that a firewall system is deployed to provide for adequate controls that will ensure prevention, detection, removal and reporting of the malicious code on all ICT assets.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

# **2.3 Physical and Environmental Security**

***Finding #9***

There was no documentation to show that the fire suppression system had been inspected and tested.

***Recommendation #6***

Ensure that the fire suppression system is tested in compliance with industry and insurance standards and guidelines.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

***Finding #10***

The air conditioner was not maintaining the required temperatures for the server room

***Recommendation #7***

Ensure that appropriate repair and maintenance procedures are carried out on the air conditioners.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

***Finding #11***

The audit team noted that ICT Block A and B LABS did not have segregation of power cables and telecommunication cables.

***Recommendation #8***

The management should ensure that power cables are segregated from communications cables to prevent interference

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

***Finding #12***

The server room was found to be having combustible materials such as cartons which could increase the chances of fire igniting and spreading quickly.

***Recommendation #9***

Remove all the combustible materials form the server room

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

***Finding #13***

The server room was not fitted with biometric access system and there was also no CCTV monitoring system.

***Recommendation #10***

The management should ensure that the server room is fitted with biometric system as a best way of authenticating user access to the server room.

The Perimeter of the server room site should be monitored by visible or infrared Closed Circuit Television System.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

# **2.4 Structured Cabling**

**Finding #14**

The audit found that structured cabling had only been done for ICT block A and block B. Network cables were terminating to a network device in other blocks.

***Recommendation #11***

Ensure that structured cabling is implemented in all building blocks so as to have a complete Local Area Network in the institution.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

# **2.5 Cabling security**

***Finding #15***

The audit team observed that cables in the racks and network cabinets had not been clearly marked

***Recommendation #12***

The institution should ensure that there are clearly identifiable cable and equipment markings to minimize handling errors.

|  |  |
| --- | --- |
| **Management Response and Action Plan** | **Responsibility/deadlines** |
|  |  |

# **3. ANNEX**

**Asset management**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Finding** | **Remarks** |
| All equipment received through purchase or donation are tagged  appropriately. | partial | Needs to be redone to harmonize inventory. |
| All equipment and assets whether new, transferred and/or write-off  are recorded by the ICT Unit for audit and other asset managerial  purposes | Yes | Write off records to be availed. |
| The inventory of ICT assets indicated product details (product  number, serial number, part number, etc.), tracking information,  maintenance schedules and warranty information. | Serial number, model, department recorded. | Information on warranty is missing(avail records) |
| Officers exiting the institution are required to surrender all ICT equipment in their custody to the ICT unit. | Yes | They have clearance form(portable) |
| The institution has automated the end user equipment inventory | Yes | Both manual and automated |

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Finding** | **Remarks** |
| The institution has implemented and maintained an inventory of assets associated with information and information processing facilities | Yes |  |
| The asset inventory is accurate, up to date, and  consistent and aligned with other inventories. | Yes |  |
| For each of the identified assets, ownership of the asset is assigned and the classification identified | Yes | This area requires improvement for some equipment e.g printers, projectors, photocopiers. |
| The institution has assigned each information asset to an owner | Yes | The ownership is only done for computers needs to |
| Employees and external party users using or having  access to the organization’s assets are aware of the information security requirements of the organization’s assets associated with information and information processing facilities and resources. | OK | Users read and sign a confidentiality and data security agreements. |
| All employees and external party users return all  of the organizational assets in their possession upon  termination of their employment, contract or agreement. | Yes | Clearance form |
| The termination process is formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization. | Yes | Except portable gadgets (clearance form exists) |
| The institution has ensured storage of IT assets in accordance with manufacturers’ specifications; | Yes | Equipment purchased and stored as per technical specifications |

**Network Security Management**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Finding** | **Remarks** |
| The institution has divided large networks into separate network  domains based on trust either physically into different  networks or by using different logical networks (e.g. virtual private networking). | Yes | They have used subnets |

**Physical and Environmental Security**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Finding** | **Remarks** |
| Controls have been adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism; | Partial | The fire suppression system needs to be serviced so that it reads automatically in case of fire. |
| Environmental conditions, such as temperature and humidity, are monitored for conditions which could adversely affect the operation of information processing facilities; | No | Air conditioners needs repair and re-configuration. |
| Power and telecommunications lines into information processing facilities are underground, where possible, or subject to adequate alternative protection; | Yes |  |
| Power cables are segregated from communications cables to prevent interference | Partial | Only ICT Block A and B  LABS |

**Telecommunication/equipment room**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Finding** | **Remarks** |
| The door of Telecommunication room opens outwardly, slide sideways, or is removable. | No | It opens inwardly |
| Sufficient lighting is provided. The light switches are located near the entrance door; | Yes | One fluorescent tube needs replacement |
| These areas do not have false(drop) ceilings | No | Not existing |
| Have a raised floor of not less than 300 mm with provisions for future expansion. | Yes |  |
| The room is neat and devoid of any non-telecommunication related substances | Partial | Some items need to be removed e.g old ups, cartons, old switches and keyboards |
| The recommended temperature for  telecommunications and equipment rooms is  Cooling to a maximum temperature of 29 degrees  Celsius is required, and a minimum temperature of  24 degrees is preferred. The temperature should  not get colder than 10 degrees. | No | Air conditioning equipment needs to be repaired They are 2 in number. |
| Relative humidity is maintained in the range from 30 to 80%. | No | Air conditioners are not working. |
| The floor and walls are sealed to inhibit dust  ingress into the cabinets | No | There is an opening on the windows |
| Electrical power is supplied by a minimum of two dedicated 220V-240V nominal from different phases, non-switched, AC-duplex electrical outlets. Each outlet should be on separate branch circuits; | Ok | Its switched instead of non-switched. |
| Grounding is provided; | Ok |  |
| The equipment shall be supplied with clean power | Ok | 3KVA ups support |
| Equip all telecommunication rooms with electrical surge suppression and a UPS that will supply the area  with at least 8 hours of standby power in the event of commercial power failure; Provide standby lighting that  will last for at least half an hour if commercial power fails; | Ok | There exists a backup generator. |
| SMART signaling, line interactive UPSs are installed in all cabinets to support the active devices installed in them. | Ok | 3KVA ups |
| The main distribution frame (MDF) cabinet has 1  UPS of capacity of 1500VA for core switch installation.  All UPSs are rack mountable. | Ok | 3KVA ups |
| Telecommunication/equipment rooms is located in secure restricted areas. The rooms are fitted with access control in line with GoK information security standards. | No | No biometric access.  No CCTV surveillance.  Fire suppression system needs servicing. |

**Structured Cabling**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Finding** | **Remarks** |
| A work area has a minimum of two information outlet  ports. | Ok | One is functional and the other one is not activated. |
| There is no splicing of any cables installed.  Intermediate cross connects transition points are not allowed. | Ok |  |
| All user area patch cords and cabinet patch cords are supplied to match the total number of data outlet | Ok |  |
| All fiber optic patch panels must be rack mounted 22 u floor standing is used or a u 19” rack wall mounted  cabinet located in a suitable closet. All cabinets must have a forced cooling | Ok | Size of cabinet should be as per the need which is 22u cabinet |
| Horizontal cabling should not terminate directly  to an application specific device but rather to a  telecommunication outlet; | Ok | Only done for ICT block A  And block B  The rest of the blocks is unstructured and needs to be structured. |
| Patch cables or equipment cords should be used to  connect the device to the cabling; | Ok | Okay for ICT block A and B , the rest is not okay |
| Horizontal Cabling infrastructure is done using category 6 cable or higher 4-pair 100 Ω unshielded twisted-pair (UTP) or 4-pair 100 Ω fully shielded twisted pair | Ok | CAT6 UTP |
| Patch cords used in the horizontal Cabling, including equipment cables/cords, should not exceed 5m. | Ok | 3 meter-user cables  1 meter-patch panel cables |
| Horizontal cable between the face plate and the patch panel shall not exceed 90m. | Ok |  |
| For back bone cables interconnecting between buildings, telecommunications rooms, equipment rooms, main terminal space, and entrance facilities, the backbone cabling shall be configured in a star topology | Ok | The whole network is star as per the network topology |

**Cable Security**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Finding** | **Remarks** |
| Network cabling should be protected from unauthorized interception or damage, for example by using a conduit or by  avoiding routes through public areas; | Ok | Only in ICT block A and block B  Other areas its insecure |
| Power cables should be segregated from communications cables to prevent interference | Ok | Only in ICT block A and block B  Other blocks not compliant |
| Clearly identifiable cable and equipment markings should be used to minimize handling errors, such as accidental patching of wrong network cables; | Ok | Only in ICT block A and block B  Other blocks are not compliant with this standard. |
| Documented patch list should be used to reduce the possibility of errors; | None | To improve on that |
| For sensitive or critical systems further controls to consider include:   * Installation of armoured conduit and locked rooms or boxes at inspection and termination points; * use of alternative routings and/or transmission media   providing appropriate security;   * use of fibre optic cabling; * initiation of technical sweeps and physical inspections for   unauthorised devices being attached to the cables;   * controlled access to patch panels and cable rooms | partial | Mainly done for ICT block A and block B.  Other areas are not compliant. |
|  |  |  |
| Horizontal Cabling infrastructure is done using category 6 cable or higher 4-pair 100 Ω unshielded twisted-pair (UTP) or 4-pair 100 Ω fully shielded twisted pair | Ok |  |
| Patch cords used in the horizontal Cabling, including equipment cables/cords, should not exceed 5m. | Ok |  |
| Horizontal cable between the face plate and the patch panel shall not exceed 90m. | Ok |  |
| For back bone cables interconnecting between buildings, telecommunications rooms, equipment rooms, main terminal space, and entrance facilities, the backbone cabling shall be configured in a star topology | Ok |  |