**Draft County Audit Programs**

1 | P a g e

**GOVERNMENT OF KENYA**

**DRAFT AUDIT PROGRAMS FOR COUNTY GOVERNMENTS**

**April 2024**

**DATA PROTECTION & RECORD MANAGEMENT AUDIT PROGRAM**

**(To be customised for each Program)**

|  |  |  |
| --- | --- | --- |
| **Audit Program No.:** | **Period Under Review:** | **Department:** |
| **Prepared By:** |
| **Reviewed By:** |

1. **Sub Processes: Data Protection**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Audit Objectives** | **Risks** | **Expected Internal Controls** | **Audit Test** |
| 1. | To confirm compliant with relevant data protection laws and regulations. | Noncompliance with relevant laws and regulationsFailure to establish data protection mechanism | Approved Data protection PolicyData protection impact assessment report. | **TOD*** Establish the key requirements of laws, regulations, policies and procedures on data protection.
* If the control is not documented, enquire from process owner how it is meant to be executed.

**TOI** Obtain the Data protection Policy.* Confirm that the design documented under TOD is implemented as documented.
* Walkthrough and document the process flow/ map. Note any gaps in implementation.

**TOE*** Confirm whether the County has established Data Protection Policy.
* Confirm whether the County is registered as Data Controller and Processor. Sec 18(1) Data Protection Act, 2019
* Confirm whether a valid certificate of registration is issued. Sec 20 Data Protection Act, 2019
* Confirm whether Data protection officer is appointed by Data Controller Sec 24 Data Protection Act, 2019
* Confirm qualification of Data protection officer in line with Sec 24 (5) Data Protection Act, 2019
* Confirm whether the details of Data protection officer are communicated to the Data Commissioner and published in the website Sec 24 (6) Data Protection Act, 2019
* Ascertain whether Data protection officer has facilitated capacity building of staff on data processing Sec 24 (7c) Data Protection Act, 2019
* Ascertain whether data protection impact assessment was done prior to processing Sec 31 (1) Data Protection Act, 2019
 |
|  |  | Collection and sharing of data without consent. | Signed Consent forms.Approved Data protection Policy | **TOD*** Establish the key requirements of laws, regulations, policies and procedures on data protection.
* If the control is not documented, enquire from process owner how it is meant to be executed.

**TOI*** Obtain the Data protection Policy and consent forms.
* Confirm that the design documented under TOD is implemented as documented.
* Walkthrough and document the process flow/ map. Note any gaps in implementation.

**TOE*** Verify whether there is consent from data subject Sec 28 (2c) Data Protection Act, 2019
* Confirm whether data is collected for lawful purposes and is explicitly defined to data subject Sec 28 (3) Data Protection Act, 2019
* Confirm whether data subject consented sharing of data to third parties Sec 40 (2) Data Protection Act, 2019
 |
|  |  | Inadequate safeguards of data leading to unauthorized access, data theft, public exposure, data breach and illicit modification. | Access rights | **TOD*** Establish the key requirements of laws, regulations, policies and procedures on data protection.
* If the control is not documented, enquire from process owner how it is meant to be executed.

**TOI** Obtain the Data protection Policy and ICT Policy.* Confirm that the design documented under TOD is implemented as documented.
* Walkthrough and document the process flow/ map. Note any gaps in implementation.

**TOE*** Ascertain whether passwords are safeguarded for data that is of confidential nature and electronically stored. **A. 26 PSC HR Policy, 2016**
* Ascertain whether continuous risks management mechanism for personal data have been established and implemented line with **Sec 41 (4), Data Protection Act, 2019**
* In case of data leakage confirm whether measures were taken in line with **Sec 43, Data Protection Act, 2019**
* Ascertain whether Data that is of sensitive nature is legally collected and processed with the owner consent **Sec 44-47 Data Protection Act, 2019**
* Confirm whether electronic data is accessed in line with **PFM Reg 110 (2 & 3)**
 |
| 2.  | To ascertain whether there are proper means of personal data storage and disposal. |  | Reports of periodic review  | **TOD*** Establish the key requirements of laws, regulations, policies and procedures on data protection.
* If the control is not documented, enquire from process owner how it is meant to be executed.

**TOI** Obtain the Data protection Policy.* Confirm that the design documented under TOD is implemented as documented.
* Walkthrough and document the process flow/ map. Note any gaps in implementation.

**TOE*** Confirm from the Data Protection Policy and periodic reports whether there is periodic review on the need for storage of personal data. **Sec 34 (3) Data Protection Act, 2019**
* Confirm whether personal data is held for the stipulated time and disposed in line with **Sec. 39 (1 & 2) Data Protection Act, 2019**
 |

* 1. **RECORD MANAGEMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Audit Objectives** | **Risks** | **Expected Internal Controls** | **Audit Test** |
| 1. | To confirm compliance with laws and regulation on financial records management  | Noncompliance with the existing laws and regulations on financial records management | Approved finance and procedure manual Vote booksCash booksFinancial reportsPayment vouchers  | **TOD*** Establish the key requirements of laws, regulations, policies and procedures on establishment of county records.
* If the control is not documented, enquire from process owner how it is meant to be executed.

**TOI** Obtain the finance procedure manual.* Confirm that the design documented under TOD is implemented as documented.
* Walkthrough and document the process flow/ map. Note any gaps in implementation.

**TOE*** Ascertain whether the operationalization of the finance and procedure manual.
* Confirm whether financial records are maintained under Constitution of Kenya Article 226.
* Confirm whether the accounting officer keeps financial records as per PFM Regulation 2015, Sec51. 1(i), 74 (6) a & b, 77, 87. (2), 118,119, 133 & 134.
 |
|  |  | Inadequate storage of financial and nonfinancial records | * Records management systems
* Backup systems
* Registers
 | **TOE*** Ascertain compliance with the procedure manual on storage of records
* Ascertain that the accounting officer ensures that Storage of records in on electronic or manual PFM Regulation 2015. 102
* Confirm that for any alteration of financial records are properly recorded PFM Reg 2015, 102 (3)
* Ascertain that systems are in place for management of nonfinancial records e.g. reports on program and projects PFM Reg 2015 129(2)
* Confirm preservation of accountable documents, books and records for a certain stipulated time PFM Reg 2015,Sec 118
 |