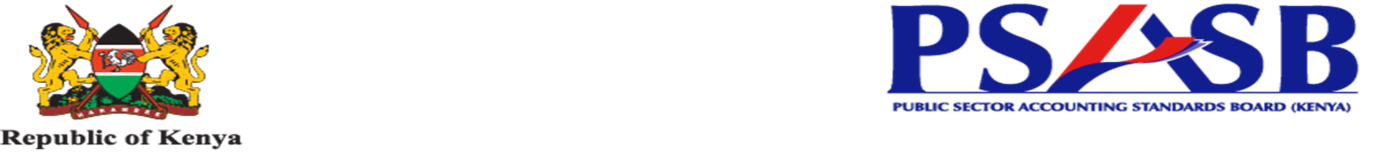
**Draft County Audit Programs**

1 | P a g e



**GOVERNMENT OF KENYA**

**DRAFT AUDIT PROGRAMS FOR COUNTY GOVERNMENTS**

**April 2024**

**AUDIT OF PROGRAM FOR GENERAL IT CONTROLS - ICT PROCESSES**

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Audit Objectives** | **Risks** | **Expected Internal Controls** | **Audit Test** |
|  | To determine whether IT systems are in compliance with applicable laws, regulations,  contracts , industry guidelines, governance criteria, policies and procedures. | Non-compliance | Approved ICT Policy | **TOD**  Establish the key requirements of laws, regulations, policies and procedures in the development of ICT Policy.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Obtain ICT Policy  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Confirm the existence of ICT Policy *Section 11.5 of ICT Governance Standard 2023*  Confirm that the ICT Policy is in compliance with the National ICT roadmap and Vision 2030.(Vision 2030 & National ICT roadmap)  Confirm whether the ICT Policy has been approved by the County Assembly *Section 30 (2)(f) of the CGA 2012*  Confirm whether the ICT Policy is aligned to applicable laws, regulations, and industry guidelines *-Applicable section of the laws, regulations and industry guidelines that is infringed.*  Confirm that the policy covers the following aspects;   1. Access Control (*section 11 of ICT security standard)* 2. Password Policy (*section 11.5.14 of ICT security standard)* 3. Child online safety policy (*section 11.9 of ICT security standard)* 4. Change Management policies and procedures (*section 11.13 of ICT security standard)* 5. Cryptographic policy (*section 12.1 of ICT security standard)* 6. Vendor Management Policy (*section 13.1.1.1 of ICT security standard)* 7. Policy on intellectual rights (*section 14. of ICT security standard)* 8. Data policy for privacy and protection of personally identifiable information (*section 14.4.1 of ICT security standard)* 9. Information Security policy (*section 11 of ICT security standard)* 10. Confidentiality policy (*section 7.3.10.2 of ICT security standard)* 11. Data Integrity policy (*section 7.3.10.4 of ICT security standard)* 12. Exit strategy policy (*section 7.3.10.6 of ICT security standard)* 13. Information transfer policy (*section 8.2 of ICT security standard)* 14. Electronic messaging policy (*section 8.3 of ICT security standard)* 15. Clear desk and clear screen policy (*section 9.1.4&5 of ICT security standard)* 16. Back up policy (*section 9.3.1.1 of ICT security standard)* 17. Incident management policy (*section 9.4.8 of ICT security standard)* 18. User end-point device security policy (*section 10 of ICT security standard)* 19. Remote working policy (*section 10.1.3 of ICT security standard)* 20. ICT training policy (*section 14.6 of ICT Governance standard)* 21. ICT enterprise security architecture policy and procedures(security architecture principle 6 of governing principles) 22. Electronic records management policy (section 7.1.2 of the electronic records management standard) 23. Bring your own device policy (section 8.4 of the end user computing standard) 24. Acceptable internet usage policy(section 8.6 of govt Ict networks) 25. Policy on governance of information assets (Annex A.10 on ICT human capital and development standard) 26. Policy on information security testing. (Annex A.10 on ICT human capital and development standard)   Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  |  | ICT Governance committees | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures in the establishment of ICT Governance committees.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Obtain one appointment letter of the committee member.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Confirm the existence of ICT Strategy Committee and IT Steering Committee S*ection 9.2 of ICT Governance Standard 2023*  Obtain the terms of reference for the committee members and confirm that the terms are aligned to the responsibilities set out in Appendix 1 *of ICT Governance Standard 2023.*  Review ICT strategy committee minutes ,reports and correspondences to confirm that it undertakes the following duties:  *Provides insight and advice to*  *the board on topics such as:*  *-The relevance of the*  *development in IT from a*  *business perspective*  *-The alignment of IT with the*  *business direction*  *-The achievement of strategic IT*  *objectives*  *-The availability of suitable*  *IT resources, skills and*  *infrastructure to meet the*  *strategic objectives*  *-Optimization of IT costs,*  *including the role of and value*  *delivery of external IT sourcing*  *-Risk, return and competitive*  *aspects of IT investments*  *-The contribution of IT to the*  *business.*  *-Exposure to IT Risks, including*  *compliance risks*  *-Direction to management*  *relative to IT strategy*  *-Drivers and catalysts for the*  *boards IT*  Review ICT steering committee minutes ,reports and correspondences to confirm that it undertakes the following duties:  *Decides the overall level of IT*  *spending and how costs will be*  *allocated*  *-Aligns and approves the*  *enterprise’s IT architecture*  *-Approves project plans and*  *budgets, setting priorities and*  *milestones*  *-Acquires and assigns*  *appropriate resources*  *-Ensures that projects*  *continuously meet business*  *requirements including a*  *reevaluation of the business*  *case*  *-Monitors projects plan for*  *delivery of expected value and*  *desired outcomes, on time and*  *within budget*  *-Monitors resource and priority*  *conflict between enterprise*  *divisions and the IT functions as*  *well as between projects.*  *-Makes recommendations*  *and requests for changes to*  *strategic plans (Priorities,*  *funding, technology approaches*  *and resources)*  *-Communicates strategic goals*  *to projects teams*  *-Is a major contributor to*  *management’s IT governance*  *responsibilities and practices*  Confirm that the entity establishes information security subcommittee and project steering committee Appendix 1 *of ICT Governance Standard 2023.*  Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  |  | Approved Architectural Centre | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures of IT systems architectural designs.  If the control is not documented, enquire from the process owner how it is meant to be executed.  **TOI**  Identify one IT system.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**   1. **Data Centre** 2. **Planning layout**   Confirm that there is adequate space between the racks/cabinets. The layout should have both hot and cold aisles with a minimum of 1.2 meter for the cold aisle and a minimum of 1.0 meters on the hot aisle.  Confirm that the building structural system is made of either steel, concrete or fabricated material.  Carry out other tests on the data centre layout and physical environment as provided in section 8.1 & 10 respectively of the Data Centre standard.   1. **Cooling system**   Confirm that there is adequate cooling equipment as well as raised floor/overhead cable tray for more flexible cooling.  Confirm that the cabinets and racks are arranged in an alternating pattern to create hot and cold aisle.  Carry out other tests on the cooling system as provided in section 8.2 of the Data Centre standard.   1. **Power system**   Confirm that there are generator(s) or UPS System(s) to support the Data Center for at least 8 hours.  Confirm that there exists Power Distribution Units (PDUs) for distribution to critical electronic equipment.  Carry out other tests on the power system as provided in section 8.3 of the Data Centre standard.   1. **Fire detection and suppression system**   Confirm that appropriate extractor fans are installed to extract any gas discharge / leakage.  Confirm that the Data center shall always have fire detection, extinguisher, and suppression systems.  Carry out other tests on the fire detection and suppression system as provided in section 8.4 of the Data Centre standard.   1. **Cabling system**   Confirm that a minimum laser-optimized 50 microns single/multimode fiber for backbone cabling and with minimum 24 cores backbone cable is used.    Confirm that a labeling scheme for all racks, power, cabinets, patch panels, patch cords and cables is maintained.  Carry out other tests on the cabling system as provided in section 9.1 of the Data Centre standard.   1. **Physical Security**   Confirm that there exist physical controls on access to the data Centre such as intruder detection system,CCTVs in strategic locations, identification and authentication systems, anti-tailgating/anti-pass-back turn style gate,single point of entry etc(section 11 of data centre standard)   1. **Monitoring systems**   Confirm that monitoring systems are installed to check the health status of all the active and computing devices.    Confirm that there is a monitoring tool to check on the data center environment i.e., temperature, humidity, and power.  Confirm that a real time monitoring system is in place to check the Physical security of the data center.   1. **Networking**   Carry out tests on the Networking system as provided in Government ICT networks standard.  7.1.15 MCDA  Confirm that the entity has established a data center. Sec 6.1.2 on infrastructure sharing, as per the National ICT Policy.  Check if the centers are a minimum of a level 2 as provided by the Sec 6.1.2 on data centers as per the National ICT Policy.  Verify if the data center site space and layout comply with the standards. Appendices A.1 of the data center standards.  Review technical configurations, charts, schematics,  network diagrams to confirm if the comply with the standards  Review documentation regarding approved remote  communication channels, mechanisms, protocols, and  standards (i.e., extranet, VPN, SSH, FTP, Wi  Review procedures for setting up, siting, and managing networked work stations and portable and mobile devices.  Assess the security of procedures for monitoring, adding, removing, and configuring all devices on the network  Review description of messaging architecture,  authentication, encryption methods, auditing/logging  Determine whether telecommunications provide a reliable and secure environment.  Consider load balancing devices, redundant systems, and alternate procedures for the continuation of telecommunication operations  Determine if EDI (Electronic Data Interchange)  is utilized. If so, evaluate security and authenticity of interchange |
|  |  | Environmental pollution | Approved electronic waste management policy | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on electronic waste disposal.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Obtain one disposed electronic device.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Check if there is an inventory of e-waste production, Sec 6.2.1(Environmental section) of the National ICT Policy  Verify if the e-waste is categorized as per provision of Sec 4.2 of the Guidelines for E waste management by NEMA 2010  Confirm the collection and storage of the e-waste is  as per the provisions of Sec 6.3 of the Guidelines for E waste management by NEMA 2010.  Confirm that the entity has a framework with appropriate legislation to support e-waste management  Confirm that the entity monitors the processes of e-waste handling regularly  Confirm that the management has established a plan with responsibilities for different target groups  (section 5.6 of the NEMA guidelines on e-waste mgt) |
|  |  |  | Annual evaluation | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on annual evaluation of IT systems.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Identify one IT system  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE(sec 11.4.2 Ict gov. Standards)**  Confirm that there exists a framework for IT infrastructure improvement  Confirm that the entity annually evaluates the capacity of IT infrastructure to understand the current environment and plan for future needs.  Confirm that the entity sets realistic targets for IT infrastructure improvement, prioritize gaps, and propose achievable solutions. |
|  |  | Loss of intellectual property | Approved contract agreement | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on contract formulation.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Select one approved contract.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Obtain a listing of all ICT related contracts and sample in according to the approved sampling criteria.  Confirm that all contracts are negotiated, drafted, vetted, and interpreted by the County Attorney for and on behalf of the County Attorney and its agencies to ensure that there is equitable distribution of risk.  Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  |  | Patent | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on patenting.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Select one county government’s own developed systems.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Obtain a listing of all county government’s own developed systems.  Confirm that the innovations are patented. *Section 22 of the Industrial Property Act 2001*  Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  | To determine confidentiality, integrity  and availability of ICT assets,  data and information. | Data breach/ Loss of data | Authentication Control | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on authentication controls.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Select one ICT system.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Confirm that associated web services use Multi-Factor Authentication *Section 10.3.9 of systems and application Standard 2023*  Confirm the existence of function for authenticating users in the system. *Annex 1 Enterprise viewpoint: fundamentals of e-government; Modules for the implementation of electronic procedures*  Where the entity provides certification services, confirm that the certificate contains ;—  (a) Information identifying the certification service provider;  (b) Information identifying the signature owner;  (c) signature-verification data which corresponds to signature- creation data;  (d) The commencement and expiry date of the certificate; (e) Information regarding the authorization of the subscriber, if a subscriber is acting on behalf of another person;  (f) Information regarding the conditions of usage of the certificate and limits on the value of transactions, where applicable;  (g) The secure electronic signature of the certification service provider that verifies the information in the certificate;  (h) Sufficient information that can be used to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate would be listed, if the certificate is suspended or revoked; and  Confirm that during the procurement process, any restrictions regarding how security and authentication is to be handled by the package is explained in the tender specifications.  Incase the entity lacks approved authentication procedures, confirm that the vendor supplies information regarding how security and authorization are handled within the product, if this is a requirement for the application.  *Annex 6: phases of systems development; Technical Requirements; Systems and application Standard 2023*  Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  |  | Input Controls | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on input controls.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Select one ICT system.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Obtain a listing of all ICT systems.  Confirm that the method for input is identified, e.g., online data entry by the functional office, interfaces with existing systems, etc.  Confirm that for each input source, the functional office owning the data source (and responsible for the accuracy of the data) is identified.  Confirm that any verification of input data is described. Confirm that frequency of data input and the approximate volume of data is identified.  Confirm that any other batch update processes (other than for interfaces to the system) is described, including: the database update logic, data editing, and error handling.  *Annex 6 – Phases of system development of the system and application Standard 2023*  Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  |  | Access Controls | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on access controls.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Select one ICT system.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Confirm that uniform application forms for registration of new users, deregistration of users and modification of user roles are in existence.  Confirm that processes of safeguarding completed application forms are in existence;  Confirm that duties are segregated  Confirm that there is use of multi-factor authentication including standardization of user primary identity linked to national identification numbers, payroll numbers and assigned responsibilities  Confirm the utilization of appropriate password length for login.  Confirm that all users of the system are authorized by the system administrator;  Confirm that where a password becomes insecure or potentially insecure, as soon as is practicable, a new secure password is implemented.  Confirm that appropriate disciplinary action is taken for any unlawful entry on the automated public financial management system using such persons password.  *PFM Regulation 110*  Confirm that where the ICT system is leased, data access procedures are defined in the lease agreement, including how the Data shall be accessed on lease expiry.  *Section* 6.3.1.16 *of systems and application Standard 2023*  Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  |  | Cryptographic controls | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on cryptographic controls.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Select one ICT system.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE** –Chapter 4 of ICTA Security Standards  Confirm if the entity has developed and implemented a policy on the use of encryption for protection of information.  Confirm that the entity has developed and implemented a policy on the use, protection, and lifetime of cryptographic keys.  Confirm that information transported by mobile or removable media devices or across communication lines is encrypted.  Confirm if encryption algorithm is of the appropriate strength and quality.  Confirm that the digital signature certificates are issued by a licensed certifying authority.  Confirm that security systems and processes are tested regularly.  Carry out other tests for operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  | Regulatory risk  Fines and penalties  Litigations | Advisories by the County Attorney | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on issuance of advisories.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Obtain one advisory report.  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE** (*Section 7 of the office of the County Attorney Act)*  Confirm that the County Attorney advises the departments on legislative and other legal matters.  Confirm that, where necessary, the County Attorney revises the county laws  Confirm that the County Attorney negotiates, drafts, vets, and interprets documents and agreements entered in relation to IT systems. |
|  |  | User integrity | Approved code of conduct | **TOD**   * Establish the key requirements of laws, regulations, policies, and procedures on Code of Conduct for Public Officers in the County * If the control is not documented, enquire from process owner how it is meant to be executed.     **TOI**   * Obtain the signed Code of Conduct for one Chief Officer * Confirm that the design documented under TOD is implemented as documented. * Walkthrough and document the process flow/ map. Note any gaps in implementation     **TOE**   * Obtain all the files of the Chief Officers who have been designated as Accounting Officers * Confirm that the County Government has developed a Specific Code of Conduct and Ethics for Public Officers in the County *Sec. 5(1) of the Public Officers Ethics Act, 2003* * Confirm that the Chief Officers have signed a Specific Code of Conduct and Ethics issued by the County Government at the time of taking the oath of office or within seven days of assuming a State office *Sec. 34 of The Public Service Code of Conduct and Ethics, 2016* * Where there has been any breach of the Code, confirm how the disciplinary proceeding has been dealt with as *per section 41 of the Leadership and integrity Act 2012* * Confirm that the system is implemented in a manner that is consistent with the security tenet of limiting access based on end-user role (e.g., staff members, System Administrators, third party partners,etc) *Security architecture Principle 2 of the General guiding principles.* * Confirm that access to secure locations is restricted to those with legitimate requirements and unethical users are immediately debarred from using the system. PR39 *of the General guiding principles.* * Carry out other tests of operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  |  | Reputation risk | Approved communication policy | **TOD**   * Establish the key requirements of laws, regulations, policies and procedures on communication in the County * If the control is not documented, enquire from process owner how it is meant to be executed.     **TOI**   * Obtain the Approved Communication 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 that communication by CEC members with Heads of Departments under their control is in writing. *Article A.9 (2)&(4) of the County HR manual*  Confirm that no public officer communicates with the media, under any circumstances, either in writing or by granting interview and making statements on matters affecting county government programs or policies without the specific authority of the relevant authority in the county government. D8 (2) *of the County HR manual*  Confirm that there is expeditious treatment of all communication received by the entity .*A.19 (1) of Public Service HR Manual*   * Carry out other tests of operating effectiveness aligned to specific county policies, procedures, service delivery standards, minutes of meetings and strategic plans. |
|  | To determine whether ICT operations are efficient and effective. | System downtime  Single point failure | Approved BCP | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on Business Continuity.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Identify one ICT system  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE** *9.3 of Govt ICT security Standard*  Confirm that the BCP plan is established, documented, implemented and maintained  Confirm that there are established processes to ensure the prevention and recovery from potential threats and that personnel and assets are protected and are able to recover quickly in the event of a disruption/disaster. *.* This includes:   1. Establishing information backup 2. Ensuring backups are stored in a remote location away from the primary site 3. The backup is regular tested for reliance   Confirm that incident response personnel with the necessary responsibility, authority and competence is appointed.  Confirm that the existing hardware and software are supported by alternative or duplicate facilities to ensure redundancy. |
|  |  | Denial of service that may result to revenue loss | Approved BCP | Refer to BCP tests conducted above |
|  | To determine whether there is seamless integration of ICT systems & technology to improve service delivery | Staff capacity constraints due to inadequate skills & competencies | Approved training plan | ***Refer to training and development WP*** |
|  |  | System incompatibility | Pre-use testing for compatibility | **TOD**  Establish the key requirements of laws, regulations, policies, and procedures on system testing.  If the control is not documented, enquire from process owner how it is meant to be executed.  **TOI**  Identify one ICT system  Confirm that the design documented under TOD is implemented as documented.  Walkthrough and note any gaps in implementation  **TOE**  Confirm that the system is tested to ensure that all portions of the system work correctly (and as specified) and work together.(*Govt ICT standards-systems and applications-system testing pg 92)*  Confirm that the open standard in relation to open source systems are compatible with the extensions *(annex 7 –of Govt ICT standards pg .105-Predatory)*  Confirm that the system is compatible with existing and future hardware and software platforms and existing procedures and operations *(General* *provisions 6.3.1.19 V.pg.19) & pg.82-compatibility-feasibility study) Standards IT GOVERNANCE* *STANDARDS*  *2023 SEC 8.4*  Confirm that the website loads quickly and is compatible with multiple browsers and devices *(6.5.10 &13)*  Confirm that new solutions must be coordinated between the different levels to achieve maximum service depth and width on the largest national scale possible and in order to ensure the compatibility of administrative level.*(Annexes pg 49)* |

Other additional controls to be tested include;

1. **Organizational controls**

* Information security and management roles and responsibilities
* Segregation of duties
* Management responsibilities
* Threat intelligence
* Inventory of information and other associated assets
* Acceptable use of information and other associated assets
* Return of assets on employee exit
* Classification of information
* Information transfer
* Vendor management policy
* Protection of records (Records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release)
* Independent review of information security
* Compliance with policies, rules, and standards for information security
* Documented operating procedures

1. **People Controls**

* Screening
* Terms and conditions of employment
* Information security awareness, education, and training
* Disciplinary process
* Responsibilities after termination or change of employment
* Confidentiality or non-disclosure agreements
* Remote working policy

1. **Physical Controls (Workstation)**

* Physical security perimeter
* Physical entry
* Securing offices, rooms, and facilities
* Physical security monitoring
* Protecting against physical and environmental threats
* Equipment siting and protection
* Security of assets off-premises
* Storage media
* Equipment maintenance
* Secure disposal or re-use of equipment

1. **Technological controls**

* Privileged access rights
* Access to source code
* Protection against malware
* Management of technical vulnerabilities
* Configuration management
* Logging /Log audit trails
* Monitoring activities
* Clock synchronization
* Use of privileged utility programs
* Installation of software on operational systems
* Network security
* Segregation of networks
* Web filtering
* Secure development life cycle
* Vendor management policy
* Change management
* Segregation of duties
* Process controls e.g. sequential, duplication checks, processing limits, exception reporting, data integrity checks, workflow authorisation,reconciliation procedures etc
* Output controls e.g information sharing,review and reconciliation,confidentiality measures etc
* Input controls e.g limit checks,validation checks, field checks, range checks, form checks,duplication checks,transactional totals,sequence checks,authorization etc

**References**

* + ICTA Standards(
  + Access to Information Act ,2016
  + ISO 27001
  + National ICT Masterplan
  + Data Protection Acts & relevant regulations
  + Guidelines on e waste management by NEMA,2010
  + Applicable Human Resource Policy and procedure Manuals
  + Contractual agreements
  + Office of the County Attorneys Act
  + Public Officers Ethics Act,2003 & attendant regulations
  + Leadership and Integrity Act & attendant regulations
  + Applicable ICT policies
  + County Government Act,2012
  + Industrial Property Act 2001
  + Copyright Act 2001
  + PFM Act & attendant regulation