|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Annexure A: Authentication Checklist** | |  |  |  |  |  |  |
|  |  |  | **[APPLICATION SYSTEM NAME]** | | | **Reference to Issue Raised** | **Focus Area conclusion** |
| **Ref.** | **FOCUS AREA** | **Examples of evidence to be obtained / verified** | **Answer [Yes / No / N/A]** | **Reference to evidence obtained** | **(Record of work done / Comments)** |
| **CONTROLS REQUIRED FOR ELECTRONIC RECORDS** | | | | | | |  |
| **SV** | **SYSTEM VALIDATION: Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern altered invalid records.** |  |  |  |  |  | **Good** |
| SV.1 | Is the system supported by validation standards and procedures? | a. Obtain the policies and procedures that support the system and ensure that it has been formally approved. B. Evaluate the policies and procedures and ensure that it address the areas indicated in SV.2 below. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SV.2 | Does the system provide for the following controls: 2.1 Audit trails 2.2 Backup and restore 2.3 Archiving 2.4 Security controls 2.5 Terminal checks 2.6 e-Signatures | a. Obtain evidence of audit trails from the system. b. Obtain evidence of backup and restore performed on the system. c. Obtain evidence of the archiving performed d. Obtain evidence of security settings being configured on the system. e. Obtain evidence of input checks that exist on the system. f. Obtain evidence of that e-signatures being used by the system (will be tested in detail later on) |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SV.3 | Proper change control processes and logs exist when changes are made on the system. | a. Formal change control process exist to approve changes made to documents on the system. b. Changes made to documents on the system is logged in an audit trail and reviewed on predetermined basis. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SV.4 | Does the system recognise invalid records? | a. The system has proper input validations to validate records. b. The database does not allow a user to manually modify a record. Users only obtain access to records through the application (user access to the database must be limited and reviewed). |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **RI** | **RECORD INSPECTION: The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by the AGSA.** |  |  |  |  |  | **Good** |
| RI.1 | Can the system generate accurate and complete copies of records in both human readable and electronic form (ASCII, PDF) for inspection, off-line review, and copying by the AGSA? | a. Confirm whether the required documents for auditing purposes can be obtained from the auditee in ASCII and PDF format.  b. Determine whether the auditee has a SOP (policy and procedure) for handing over of electronic records to the AGSA for inspection. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| RI.2 | Can the system generate copies of users with their individual user rights (e.g., file access, electronic signature)? | a. This should be possible in paper copies and electronic copies in PDF format only |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **RP** | **RECORD PROTECTION: Protection of records to enable their accurate and ready retrieval throughout the records retention period.** |  |  |  |  |  | **Good** |
| RP.1 | Are all electronic records saved to a secure location, preferable on the local area network? | a. Obtain evidence of where these files are securely stored and whom has access to this network location. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| RP.2 | Does the auditee have an SOP (policies and procedures) to cover the backups, restore and recovery for the data on this system which also indicates whom is responsible for this? | a. Obtain evidence of this SOP. b. Obtain evidence of the backups that has been performed as has been indicated in the SOP. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| RP.3 | Does the auditee have an SOPs (policy and procedure) to cover the long term archiving and retrieval of the data on the system which also indicates whom is responsible for this? | a. Obtain evidence of this SOP. b. Obtain evidence of the latest archiving that was performed as has been indicated in the SOP. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| RP.4 | How is it ensured that all the electronic records are included in the system backups? | a. Obtain evidence of how completeness of the system backups are ensured (is ts done through tool to ensure completeness and accuracy). |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| RP.5 | Can data generated in earlier software versions be retrieved from archives and viewed in its entirety? | a. Obtain evidence that the restore function allow you to import backups from earlier software versions. b. Obtain evidence that backup and restore actions are documented in the system audit trails. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| RP.6 | If records can be copied outside the software, is user access to the copy read-only?  \* If no, does the software prohibit the overwriting of the original record by the copy? | a. Obtain evidence that records should preferably not be allowed to be copied from within the software. b. Obtain evidence that records are only be allowed to be exported or saved as a different document with a different date and time stamp. The original file may not be overwritten. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| RP.7 | Are critical records stored in one location only?  \* If not, do validated automatic functions exist to maintain data integrity? | a. Obtain evidence that critical records are identified. b. Obtain evidence if data is stored in different locations or if all data is stored in the same location with the same level of protection. (If stored in the same location with the same level of protection, it will be sufficient.) |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| RP.8 | Is simultaneous write access to the same electronic record by multiple users prohibited? | a. Obtain evidence that the system prevents two or more users simultaneously saving the same electronic records. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| RP.9 | Can data be recreated after the system failed? | a. Obtain evidence that backup recovery tests have been performed to ensure that data could be recovered, or recreated from a backup. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| RP.10 | Are the records protected from hazards such as fire, heat and water by environment controls (e.g. ventilation)? | a. Through observation, determine whether the database where the data is store is protected from environmental hazards. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| RP.11 | Have retention periods for the electronic records retained in the system been specified? | a. Refer to the auditee's policy |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **SEC** | **SECURITY: Limiting system access to authorised individuals** |  |  |  |  |  | **Good** |
| SEC.1 | Are devices for storage of electronic records (e.g. PCs, file/database servers and backup and archive durable media) located in a controlled area or physically secured? | a. Through observation, determine whether the devices where the data is store is physically protected. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SEC.2 | Does the system limit system access to authorised individuals? | a. Obtain a list of users with access to the system. b. Obtain the user access policy and procedures relating to this system and ensure that is covers creation and termination of users. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SEC.3 | Does the system prevent deletion of users from the system in order to ensure the uniqueness of user IDs? The User ID should be "Deactivated" but retained. | a. Obtain evidence that user IDs are not retained on the system by being made "inactive" and not reassigned to new users. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SEC.4 | Does the system have a password-protected inactivity lock, which lock the system after a period of inactivity by user? | a. Obtain evidence that the system automatically locks after a period of inactivity that requires that the user logs on again with a password to gain access to the system again. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SEC.5 | Is user access to the operating system restricted to the system administrator or an equivalent authorised user? | a. Obtain a list of the users with access to the operating system and ensure that only the system administrator or user with the assigned right has access. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SEC.6 | If the system can be accessed remotely, are additional security measures such as "call back" or SecurID included? | a. If the system can be accessed remotely, determine if additional security measures have been implemented and obtained evidence therefore. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SEC.7 | Are attempts at unauthosed use, and to lock the account after several consecutive unsuccessful attempts to enter a password? | a. Obtain evidence that the number of login attempts has been defined on the system by the system administrator. b. Obtain evidence that after the defined number of failed login attempts the user account is locked. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SEC.8 | Does the auditee have security policy and procedures to manage the system security? | a. Obtain evidence of the security policy and procedure and ensure that it has been formally approved. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **AT** | **AUDIT TRAIL: Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for AGSA's review and copying.** | |  |  |  |  | **Good** |
| AT.1 | Are there computer-generated (automated) audit trails of all user actions? | a. Obtain evidence of these audit trails. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| AT.2 | Are audit trails entries date-stamped (DD-MM-YYY)? | a. From the evidence obtained above, evaluate whether the activities logged are date stamped. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.3 | Are audit trails time-stamped HH-MM-SS in local time? | a. From the evidence obtained above, evaluate whether the activities logged are time-stamped in local time? |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.4 | Are there controls to ensure that the system clock date and time stamps are accurate and secure from tampering (e.g. changing the system clock)? | a. On the PC, determine whether is the system clock is accurate and secure from being manually changed. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.5 | Do audit trails include operator identity, using full name or the customer-defined user ID of an individual? | a. From the evidence obtained above, evaluate whether the operator identity (user ID) is given by the unique user name? |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.6 | Is there an audit trail for system activity, including all user login and failed access attempts? | a. From the evidence obtained above, evaluate whether the failed logon attempts are also logged? |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.7 | Is an audit trail generated during creation of all data? | a. Obtain evidence that an audit trail exist of all data created. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.8 | Is an audit trail generated during modification of all data? | a. Obtain evidence that an audit trail exist of all data modification. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| AT.9 | Is an audit trail generate during "deletion" or "inactivation" of all data? | a. Obtain evidence that an audit trail exist of deletion and/or inactivation of data. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.10 | If a signed record is changed, does the system retain and display the old and new value? | a. Obtain evidence that the system retain the old and new values when a signed record is changed. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.11 | Does each audit trail entry describe the action performed? | a. From the evidence obtained above, evaluate whether the entries describe the actions performed? |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.12 | Does the audit trail contain sufficient information to allow a reviewer to trace all changes to a signed record from its current state back to the original values? | a. From the evidence obtained above, evaluate whether the entries contain sufficient information to trace all changes as indicated? |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.13 | Is the audit trail directly linked to the record, but located separately? | a. From the evidence obtained above, evaluate whether the entries can be directly linked to the record but is separately stored |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT,14 | Is the audit trail backed up, and maintained for at least as long as the retention of the underlying records? | a. Obtain evidence that the audit trail is also stored in the database and part of the backup. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.15 | Is a read-only display or report available for viewing the audit history? | a. Obtain evidence that the audit trail can be displayed or printed by using suitable filter criteria. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |
| AT.16 | Are all users, (including the system administrator) unable to modify audit trail details? | a. Obain evidence that nobody is allowed to modify audit trail information information by obtaining user access rights to the audit trail and confirming the type of access they have to the audit trail data. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| AT.17 | Are changes to user access control levels (i.e. user roles) and permissions (i.e. user rights) audit trailed? | a. From the evidence obtained above, evaluate whether the changes to users' access control levels and permissions have been logged. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **AC** | **AUTHORITY CHECK: Use of authority checks to ensure that only authorised individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.** | |  |  |  |  | **Good** |
| AC.1 | Does the software require entry of a separate user ID and password, in addition to that which is required by the operating system? | a. Through observation, determine whether the users need to enter a separate password to access the system. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| AC.2 | Does each user have an individual unique account? | a. Obtain the user access list from the system and ensure that each user on the system can be uniquely identified. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| AC.3 | Does the system have different user-defined access control levels? | a. Determine if the system make provision to assign users different user roles and user rights. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| AC.4 | If the system has different user levels, are there SOPs (policies and procedures) in place to describe how a user's access shall be defined? | a. Obtain the auditee's policies and procedures which describes these access rights. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| AC.5 | Are modifications/deletions to data always performed through a formal software change control process? (e.g. Data is not changed through SQL or other data access tools.) | a. Obtain the auditee's policies and procedures which describes these access rights. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **ARA** | **ACCOUNTABILITY & RESPONSIBILITY FOR ACTIONS: The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under heir electronic signatures, in order to deter record and signature falsifications** | |  |  |  |  | **Good** |
| ARA.1 | Have policies and/or procedures holding individuals accountable and responsible for actions initiated under their electronic signatures been established and followed? | a. Obtain and inspect the policies and procedures to ensure that these documents properly indicate the responsibilities and accountabilities relating to applying electronic signatures to documents. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **SDC** | **SYSTEM DOCUMENTATION CONTROLS: Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.** | |  |  |  |  | **Good** |
| SDC.1 | Are there adequate controls over the distribution of documentation for system operation and maintenance; and system logs? (i.e. SOPs should be issued under controlled instances and not be readily available to anyone.) | a. Determine what the process is to obtain the system operation and maintenance SOPs as well as the system logs and ensure that this process is controlled. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SDC.2 | Has a change control process been implemented for changes and modification to system documentation which is logged in an audit trailed with a time stamp? | a. Obtain the change control process and ensure that this applicable to system changes as well and that it requires changes to be logged in an audit trail and to be time stamped. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **SR** | **SIGNING REQUIREMENTS: Signed electronic records should contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature** | |  |  |  |  | **Good** |
| SR.1 | Does the electronically signed records contain information associated with the signing that clearly indicated the full printed name of the signer? | a Obtain evidence that the electronically signed documents that want to be relied upon clearly indicates the full printed name of the signer. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SR.2 | Does the electronically signed records contain information associated with the signing that clearly indicated the date and time when the signature was executed? | a Obtain evidence that the electronically signed documents that want to be relied upon clearly indicates the date and time when the signature was executed. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| SR.3 | Does the electronically signed records contain information associated with the signing that clearly indicated the meaning of the signature? | a Obtain evidence that the electronically signed documents that want to be relied upon clearly indicates the meaning of the signature. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **CONTROLS REQUIRED FOR ELECTRONIC SIGNATURES:** | | | | | |  |  |
| **LSER** | **LINKING SIGNATURES TO ELECTRONIC RECORDS: Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.** | |  |  |  |  | **Good** |
| LSER.1 | Are all electronic signatures on electronic records linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means? | ? |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| LSER.2 | Are handwritten signatures on printouts of electronic records linked to their respective electronic records? \* Minimum requirement is initials of signer, print date/time unique sample identifier, and, if appropriate, file name and location / file size. |  |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| LSER.3 | Does the system identify whether a record has been modified after signing and requires a new signature? |  |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| LSER.4 | When changes are made to previously approved electronic records, are electronic or handwritten signatures applied to updated records, and linked to other original signed records? |  |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **UOS** | **UNIQUENESS OF SIGNATURE: Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.** | |  |  |  |  | **Good** |
| UOS.1 | Are electronic signatures unique to an individual? | a. Obtain evidence that no user account can share the same electronic signature. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| UOS.2 | Does the system prohibit the use of shared/group accounts as components of electronic signatures? | a. Obtain evidence from the system that only unique user accounts can be created. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **VOI** | **VERIFICATION OF IDENTITIES: Before an organisation establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organisation shall verify the identity of the individual.** | |  |  |  |  | **Concerning** |
| VOI.1 | Electronic signatures should not be allowed to be reuse by, or reassigned to, anyone else. | a. Obtain evidence that the user account (and therefore the electronic signature) is unique for the lifetime of the database. b. Obain evidence that the user accounts are only disabled but not deleted from the database, by selecting previously terminated user, and inspecting the user accounts to ensure that the user accounts were only disabled and not deleted from the database. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| VOI.2 | Is the identity of an individual verified before an electronic signature is allocated? | a. Obtain evidence that the identity of the user is verified by means of ID/passport before an electronic signature is allocated. b. Ensure that this verification process is included in the organisation's policies and procedures relating to electronic signatures. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| VOI.3 | Has the auditee informed the AGSA via a formal letter that they intend to make use of electronic signatures, before using electronic signature for the financial year under review? | a. Even though this is not regulatory requirements, auditees should inform the AGSA timely of their intent to make use of electronic signatures due to the additional verification and assurance processes that needs to be performed before reliance can be placed on the documents for audit purposes. b. Obtain proof of this formal letter. If it does not exist, inform the audit of this requirement going forward. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **ESCC** | **ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS: Electronic signatures that are not based upon biometrics should: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing should be executed using all electronic signature components; subsequent signings should be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing should be executed using all of the following electronic signature components: (a) Be used only by their genuine owners; and (b) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.** | |  |  |  |  | **Concerning** |
| ESCC.1 | Is the signature made up of at least two components, such as an identification code and password, or an ID card and a password? | a. Obtain evidence of the two components that used to apply electronic signatures to documents within the system. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| ESCC.2 | When several signings are made during a continuous session, is the secret part of the signature executed at each signing? | a. Obtain evidence that both components must be executed at the first signing of a session. b. There after obtain evidence that the secret part of the signature is required at each signing. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| ESCC.3 | If signings are not done in a continuous session, are both components of the electronic signature executed with each signing? | a Obtain evidence that both components must be executed for each signing when there is no continuous signing of documents. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| ESCC.4 | Are signatures designed to ensure that they can only be used by their genuine owners? | a. Obtain evidence that each user is assigned a unique identification code that is linked to their specified password that must be entered together before the electronic signature can be applied. b. Also ensure that the system does not allow that the same combination of ID code and password cannot be assigned to a different user on the system. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| ESCC.5 | Have biometric electronic signature been implemented and validated including attempted use by other users? | a. Determine electronic signatures are being applied via biometric scanners. b. If yes, obtain evidence if two way authentication is also required for these signatures. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| **MOP** | **MONITORING OF IDs AND PASSWORDS: It should be ensured that identification codes and passwords issued are periodically monitored, recalled or revised. Where identification and/or password tokens are used, loss management procedures to electronically deauthorise lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification codes or password information, and to issue temporary or permanent replace using suitable, rigorous controls should exist.** | |  |  |  |  | **Intervention required** |
| MOP.1 | Are procedures in place to ensure that the validity of identification codes periodically reviewed? | a. Inspect the electronic signature policies and procedures and ensure that is requires that validity of identification codes are periodically reviewed and that it indicates specifically by whom. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| MOP.2 | Do passwords periodically expire? | a. Inspect the electronic signature policies and procedures and ensure that is requires that password expires periodically. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| MOP.3 | Are passwords obscured when entered? | a. Inspect the electronic signature policies and procedures and ensure that is requires that password are obscured when it is entered by the user and stored in the system. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| MOP.4 | Are there procedures in place for recalling identification codes and password tokens (if used) if a person leaves the organisation? | a. Inspect the electronic signature policies and procedures and ensure that when tokens are used to provide users with identification codes and passwords to apply electronic signatures to documents, that there is specific procedures to recall these tokens when a person leave the organisation. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| MOP.5 | Is there a procedure in place for electronically deactivating an identification code or password if it suspected that it has been compromised or has been lost? | a. Inspect the electronic signature policies and procedures and ensure that when tokens are used to provide users with identification codes and passwords to apply electronic signatures to documents, that there is specific procedures to deactivate these tokens when it is suspected that these tokens have been stolen or lost and that signatures that have applied to documents during that time be marked as invalid. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| MOP.6 | Is there a technical feature to detect attempts at unauthorised use of electronic signatures? | a. Obtain evidence that audit tails log unsuccessful attempts to apply signatures to documents and automatically report it to the administrator. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
| MOP.7 | Is there a procedure in place for immediate reporting any attempts at unauthosed use of identification codes and password? | a. Inspect the electronic signature policies and procedures and ensure that there is a procedure in place to allow the administrator to immediately report unsuccessful attempts of applying signatures to documents to the correct authority. |  |  | > Who: > When (Date): > Evaluation (Record of work done: Is the document formal/ draft and/or is it addressing the stated process): > Conclusion: |  |  |
|  | **OVERALL CONCLUSION** |  | | | |  |  |
|  |  |  |  |  |  |  |  |
| **List risks factors identified (If applicable)** | | |  |  |  |  |  |