Notes:

1) Cloud Services include Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Function as a Service (FaaS), Data as a Service (DaaS), Integration Platform as a Service (iPaaS), Security as a Service (SECaaS) and Disaster Recovery as a Service (DRaaS).
2) On-premises Systems include all systems that are placed and hosted on the Eskom corporate local area network (LAN) or business information network (BIN), and this does not include systems that are placed and hosted on the operational technology (OT) or process control network (PCN).
3) Service Organisation Control (SOC) attestation reports are only applicable to Cloud Services, not systems on-premises on the Eskom corporate local area network (LAN) or business information network (BIN) and operational technology (OT) network.
4) SOC 1 Type II and SOC 2 Type II is an attestation standard put forth by the Auditing Standards
5) Board of the American Institute of Certified Public Accountants (AICPA) that addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide cloud services to user entities.
6) SOC 1 Type II is a mandatory requirement for all Cloud Services that store and process financial information.
7) SOC 2 Type II is a mandatory requirement for all Cloud Services that store and process Personal Identification Information (PII) and Intellectual Property (IP) information.
8) The SOC reports must be for the Service Provider that submits the technical proposal as part of the Request For Proposal (RFP) for the Cloud Service offered and not for the Service Provider or sub-organisation (such as Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Computing Services (GCP) where the Cloud Service is hosted.

Security Control		Mandatory/ Optional/ Preferred
1.	External Third-Party Attestation Reports The Cloud Service Provider (CSP) shall: a) For all cloud services that store and process financial information and personal identifiable information (PII) including intellectual property (IP), the CSP shall have a valid Service Organisation Control (SOC) 1 and SOC 2 Type II reports, such attestation reports shall be submitted to Eskom for review. b) Up to once per period of twelve (12) months, the CSP will provide comprehensive summaries of its latest SOC 2 report at no cost upon Eskom's written request. c) if the SOC Reports indicate any deficiencies or matter requiring attention, the CSP shall use commercially reasonable efforts to address all such items without any costs to the Eskom. d) Subject to Section 1.b, if vendor's reporting cycle is not aligned with the financial year, and/or the SOC report is older than six (6) months, the CSP shall submit a bridge letter to the Eskom at no cost, and such bridging letter shall not cover a period exceeding three (3) months.	Mandatory for all cloud services that store and process PII, Intellectual Property (IP), and financial information.
2.	For all on-premises systems that store and process financial information, PII and IP, a valid Information Security Standard (ISO) 27001 certificate is required.	Mandatory for all on-premises
3.	For all Cloud Services that store and process financial information, PII and IP information, a valid Information Security Standard (ISO) 27017 and Information Security Standard (ISO) 27018 certificates are required.	Mandatory for all cloud services
4.	The Cloud Service (if hosted in the cloud) or system (if hosted on premises) shall be able to integrate with existing Eskom's identity providers (IdP's) such as Microsoft (MS) Active Directory (AD), Entra Identity (ID) and shall support Security Assertion Markup Language (SAML) 2.0, Open Authorization (OAuth) 2.0 and OAuth 2.1 to enable Multi-Factor Authentication (MFA) and Single Sign-On (SSO).	Mandatory for all cloud services and on-prem systems
5.	Privileged Access Management (PAM) the system shall be able to onboard privileged accounts onto PAM tools, such as CyberArk but not limited to onboard privileged accounts to securely manage, rotate passwords, monitor, record sessions, control, enforce access to privileged accounts, auditing and reporting capabilities.	Mandatory for all cloud services and on-prem systems
6.	The System shall employ a Role-based access control (RBAC) mechanism.	Mandatory for all cloud services and on-prem systems

Security Control		Mandatory/ Optional/ Preferred
7.	For all systems that store and process financial information, personal information (PI) and intellectual property (IP) information, data at rest using minimum Advanced Encryption Standard (AES)-256, data in use and in transit (or in motion) using minimum Transport Layer Security (TLS) 1.3 or later version shall be encrypted.	Mandatory for all cloud services and on-prem systems
8.	Data shall be secured at minimum using a secure hash algorithm (SHA)-256 for data integrity, securing transactions, and messages.	Mandatory for all cloud services and on-prem systems
9.	Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators.	Mandatory for all cloud services and on-prem systems
10.	Sensitive information such as personal identifiable information (PII) data in non-production environments shall be masked.	Mandatory for all cloud services and on-prem systems
11.	Incremental daily back-ups shall be done, encrypted, and securely kept offsite only for all critical systems.	Mandatory for all systems classified a mission critical
12.	Real-time data synchronization or data replication to a secondary or disaster recovery (DR) site, located in different regions shall be employed only for critical systems.	Mandatory for all systems classified a mission critical
13.	Disaster Recovery Plan (DRP) shall be defined, annually tested, and such DRP test results shall be shared with the Eskom Cybersecurity team only for critical systems.	Mandatory for all systems classified a mission critical
14.	A back up Restore Plan and Procedure shall be defined, annually tested, and such test results shall be shared with Eskom's Cyber Security team.	Mandatory for all cloud services and on-prem systems
15.	Patch Management Process shall be defined. The software updates and patches shall be tested in a non-production environment before being deployed into the production (PROD) environment.	Mandatory for all cloud services and on-prem systems
16.	The static application security test (SAST), dynamic application security test (DAST), vulnerability assessment and penetration test shall be conducted prior deploying the cloud system and on-prem system to production, all critical, high, and medium vulnerabilities shall be addressed prior deploying production, and the summary of the test results shall be submitted to the Eskom Cybersecurity team for review and acceptance.	Mandatory for all cloud services and on-prem systems
17.	The CSP shall comply with applicable privacy and protection of personal information Acts such as General Data Protection Regulation (GDPR) in European Union (EU) and Protection of Personal Information Act (POPIA) in South Africa (SA) where the cloud service is hosted, and the region where the data subjects are physically located and where the data is collected.	Mandatory for all cloud services that store and process PII

Security Control		Mandatory/ Optional/ Preferred
18.	The CSP shall notify Eskom immediately or within twenty-four (24) hours when any cyber security breach has occurred. Although the GDPR and the South African Cybercrimes Act 19 of 2020 states that the notification shall be sent within seventy-two (72) hours, Eskom shall be notified sooner to allow Eskom to notify the information regulator and take necessary actions to minimize the impact on Eskom.	Mandatory for all cloud systems that store and process PII
19.	The CSP shall notify Eskom within one (1) month if there are any significant changes to the business, platform and hosting service provider or any change that could have an impact the security assessment conducted and the auditor's opinion on the System and Organization Control's (SOC) audit.	Mandatory for all cloud services
20.	The database shall be placed within Eskom corporate Local Area Network (LAN)/Business Information Network (BIN) network (if hosted on premise) and partner private network (If hosted in the cloud) behind the perimeter firewall.	Mandatory for all cloud services and on-prem systems
21.	Database Security Management tools shall be employed to provide regulatory compliance, encryption, key management, granular access controls, flexible data masking, comprehensive activity monitoring, and sophisticated auditing capabilities.	Mandatory for all cloud services and on-prem systems
22.	Distributed denial of service (DDoS) protection mechanism shall be employed for all services.	Mandatory for all cloud services
23.	Web Application Firewall (WAF) for all internet facing applications and/or web-based applications shall be employed.	Mandatory for all cloud services
24.	The Service shall support the prevailing enterprise services bus (ESB), application programmable interfaces (API's) and Integration Platform as a Service (iPaaS) platforms for security, logging and monitoring for both on-prem, hybrid-cloud and multi-cloud environments.	Mandatory for all cloud services and on-prem systems
25.	The Cloud Service shall provide e-Discovery capability to identify, collect and produce electronically stored information (ESI) in response to a request for production in a lawsuit or investigation as part of the cloud services offered.	Mandatory for all cloud services
26.	The on-premises System and Cloud Service shall be able to integrate with Security Information and Event Management (SIEM) standard technologies such as Syslog, Windows event logging, Simple Network Management Protocol (SNMP) and Application Programming Interface (API) but not limited to these technologies listed.	Mandatory for both cloud services and on-premises system