AI CONTROLS MATRIX v1.0.3

Control Domain	Control Title	Control ID	Control Specification
Audit & Assurance-A&A			
Audit & Assurance	Audit and Assurance Policy and Procedures	**A&A-01**	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually or upon significant changes.
Audit & Assurance	Independent Assessments	**A&A-02**	Conduct independent audit and assurance assessments according to relevant standards at least annually.
Audit & Assurance	Risk Based Planning Assessment	**A&A-03**	Perform independent audit and assurance assessments in response to significant changes or emerging risks and according to risk-based plans and policies.

Audit & Assurance	Requirements Compliance	**A&A-04**	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.
Audit & Assurance	Audit Management Process	**A&A-05**	Define and implement an Audit Management process aligned with global auditing standards, to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.
Audit & Assurance	Remediation	**A&A-06**	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.
Application & Interface Security-AIS			

Application & Interface Security	Application and Interface Security Policy and Procedures	**AIS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security. Review and update the policies and procedures at least annually or after significant system changes.
Application & Interface Security	Application Security Baseline Requirements	**AIS-02**	Establish, document and maintain baseline requirements for securing applications."
Application & Interface Security	Application Security Metrics	**AIS-03**	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.

Application & Interface Security	Secure Application Development Lifecycle	**AIS-04**	Define and implement a secure software development lifecycle (SDLC) process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements defined by the organization.
Application & Interface Security	Application Security Testing	**AIS-05**	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while meeting organizational delivery goals. Automate when applicable and possible.
Application & Interface Security	Secure Application Deployment	**AIS-06**	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.

Application & Interface Security	Application Vulnerability Remediation	**AIS-07**	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.
Application & Interface Security	Input Validation	**AIS-08**	Validate, filter, modify or block, as necessary, input against adversarial patterns, failure patterns and unwanted behaviour according to organisational policies and applicable laws and regulations.
Application & Interface Security	Output Validation	**AIS-09**	Validate, filter, modify or block, as necessary, output against adversarial patterns, failure patterns and unwanted behaviour according to organisational policies and applicable laws and regulations.

Application & Interface Security	API Security	**AIS-10**	Define and implement processes, procedures, and technical measures to secure APIs. Review and update for any improvements at least annually or after significant system changes.
Application & Interface Security	Agents Security Boundaries	**AIS-11**	Establish security boundaries for agents.
Application & Interface Security	Source Code Managemement	**AIS-12**	Implement source code management practices, such as version control, code review & static code analysis, aligning with the SDLC process.

Application & Interface Security	AI Sandboxing	**AIS-13**	Implement sandboxing techniques to execute AI tools and plugins in isolated environments to prevent unintended interactions with critical systems or data and limit the possibility of lateral movement.
Application & Interface Security	AI Cache Protection	**AIS-14**	Implement security measures to protect caches in GenAI systems and services.
Application & Interface Security	Prompt Differentation	**AIS-15**	Implement mechanisms enabling the model to clearly distinguish user-provided input instructions from data and system instructions (e.g., system prompts).
Business Continuity Management and Operational Resilience-BCR			

Business Continuity Management and Operational Resilience	Business Continuity Management Policy and Procedures	**BCR-01**	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually, or when significant changes occur that could impact risk exposure.
Business Continuity Management and Operational Resilience	Risk Assessment and Impact Analysis	**BCR-02**	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. Review and update the risk assessment and impact analysis at least annually or upon significant changes.
Business Continuity Management and Operational Resilience	Business Continuity Strategy	**BCR-03**	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.

Business Continuity Management and Operational Resilience	Business Continuity Planning	**BCR-04**	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.
Business Continuity Management and Operational Resilience	Documentation	**BCR-05**	Develop, identify, and acquire documentation, both internally and from external parties, that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review at least annually or upon significant changes.
Business Continuity Management and Operational Resilience	Business Continuity Exercises	**BCR-06**	Follow a structured approach to evaluate the effectiveness of the business continuity and operational resilience plans at planned intervals or upon significant changes.

Business Continuity Management and Operational Resilience	Communication	**BCR-07**	Establish and maintain communication channels with all relevant stakeholders in the course of business continuity and resilience procedures.
Business Continuity Management and Operational Resilience	Backup	**BCR-08**	Periodically perform backups. Ensure the confidentiality, integrity and availability of the backup, and verify restoration from backup for resiliency.
Business Continuity Management and Operational Resilience	Disaster Response Plan	**BCR-09**	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.

Business Continuity Management and Operational Resilience	Response Plan Exercise	**BCR-10**	Exercise the disaster response plan annually or upon significant changes, including, if possible, participation of local emergency authorities.
Business Continuity Management and Operational Resilience	Equipment Redundancy	**BCR-11**	Supplement business-critical equipment with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance in accordance with applicable industry standards.
Change Control and Configuration Management-CCC			
Change Control and Configuration Management	Change Management Policy and Procedures	**CCC-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to assets owned, controlled or used by the organization. Review and update the policies and procedures at least annually, or upon significant changes.

Change Control and Configuration Management	Quality Testing	**CCC-02**	Establish, maintain and implement a defined quality change control, approval and testing process incorporating baselines, testing, and release standards.
Change Control and Configuration Management	Change Management Technology	**CCC-03**	Implement a change management procedure to manage the risks associated with applying changes to assets owned, controlled or used by the organization.
Change Control and Configuration Management	Change Authorization	**CCC-04**	Implement and enforce a procedure to authorize addition, removal, update, and management of assets, owned, controlled or used by the organization.

Change Control and Configuration Management	Change Agreements	**CCC-05**	Include provisions limiting changes directly impacting customer owned environments/tenants to explicitly authorized requests within service level agreements.
Change Control and Configuration Management	Change Management Baseline	**CCC-06**	Establish change management baselines for all relevant authorized changes on organization assets. Review and update the change management baseline at least annually or upon significant changes.
Change Control and Configuration Management	Detection of Baseline Deviation	**CCC-07**	Implement detection measures with proactive notification in case of changes deviating from the established baseline.

Change Control and Configuration Management	Exception Management	**CCC-08**	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.
Change Control and Configuration Management	Change Restoration	**CCC-09**	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.
Cryptography, Encryption & Key Management-CEK			
Cryptography, Encryption & Key Management	Encryption and Key Management Policy and Procedures	**CEK-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually or upon significant changes.

Cryptography, Encryption & Key Management	CEK Roles and Responsibilities	**CEK-02**	Define and implement cryptographic, encryption and key management roles and responsibilities.
Cryptography, Encryption & Key Management	Data Encryption	**CEK-03**	Provide data protection at-rest, in-transit and, where applicable, in-use by using cryptographic libraries certified to approved standards.
Cryptography, Encryption & Key Management	Encryption Algorithm	**CEK-04**	Utilize encryption algorithms following industry standards for protecting data, based on the data classification and associated risks.

Cryptography, Encryption & Key Management	Encryption Change Management	**CEK-05**	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.
Cryptography, Encryption & Key Management	Encryption Change Cost Benefit Analysis	**CEK-06**	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.
Cryptography, Encryption & Key Management	Encryption Risk Management	**CEK-07**	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.

Cryptography, Encryption & Key Management	Customer Key Management Capability	**CEK-08**	Providers must provide the capability for customers to manage their own data encryption keys.
Cryptography, Encryption & Key Management	Encryption and Key Management Audit	**CEK-09**	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).
Cryptography, Encryption & Key Management	Key Generation	**CEK-10**	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.

Cryptography, Encryption & Key Management	Key Purpose	**CEK-11**	Manage cryptographic secret and private keys that are provisioned for a unique purpose.
Cryptography, Encryption & Key Management	Key Rotation	**CEK-12**	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.
Cryptography, Encryption & Key Management	Key Revocation	**CEK-13**	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.

Cryptography, Encryption & Key Management	Key Destruction	**CEK-14**	Define, implement, and evaluate processes, procedures, and technical measures to securely destroy cryptographic keys when they are no longer needed, which include provisions for legal and regulatory requirements.
Cryptography, Encryption & Key Management	Key Activation	**CEK-15**	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.
Cryptography, Encryption & Key Management	Key Suspension	**CEK-16**	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.

Cryptography, Encryption & Key Management	Key Deactivation	**CEK-17**	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.
Cryptography, Encryption & Key Management	Key Archival	**CEK-18**	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.
Cryptography, Encryption & Key Management	Key Compromise	**CEK-19**	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.

Cryptography, Encryption & Key Management	Key Recovery	**CEK-20**	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.
Cryptography, Encryption & Key Management	Key Inventory Management	**CEK-21**	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.
Datacenter Security-DCS			
Datacenter Security	Off-Site Equipment Disposal Policy and Procedures	**DCS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually, or upon significant changes.

Datacenter Security	Off-Site Transfer Authorization Policy and Procedures	**DCS-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually, or upon significant changes.
Datacenter Security	Secure Area Policy and Procedures	**DCS-03**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually, or upon significant changes.
Datacenter Security	Secure Media Transportation Policy and Procedures	**DCS-04**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually, or upon significant changes.

Datacenter Security	Assets Classification	**DCS-05**	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk. Review and update the assets' classification at least annually or upon significant changes.
Datacenter Security	Assets Cataloguing and Tracking	**DCS-06**	Catalogue and track all relevant physical and logical assets located at all of the service providers sites within a secured system. Review and update the catalogue at least annually or upon significant changes.
Datacenter Security	Controlled Physical Access Points	**DCS-07**	Design and implement physical security perimeters to safeguard personnel, data, and information systems.

Datacenter Security	Equipment Identification	**DCS-08**	Use equipment identification as a method for connection authentication.
Datacenter Security	Secure Area Authorization	**DCS-09**	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.
Datacenter Security	Surveillance System	**DCS-10**	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.

Datacenter Security	Adverse Event Response Training	**DCS-11**	Train datacenter personnel to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts.
Datacenter Security	Cabling Security	**DCS-12**	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.
Datacenter Security	Environmental Systems	**DCS-13**	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.

Datacenter Security	Secure Utilities	**DCS-14**	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.
Datacenter Security	Equipment Location	**DCS-15**	Keep business-critical equipment away from locations subject to high probability for environmental risk events.
Data Security and Privacy Lifecycle Management-DSP			
Data Security and Privacy Lifecycle Management	Security and Privacy Policy and Procedures	**DSP-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection, preparation and handling of data throughout its lifecycle, and according to all applicable laws and regulations,standards, and risk level. Review and update the policies and procedures at least annually.

Data Security and Privacy Lifecycle Management	Secure Disposal	**DSP-02**	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.
Data Security and Privacy Lifecycle Management	Data Inventory	**DSP-03**	Create and maintain a data inventory, at least for any sensitive, regulated and personal data. Review and update the inventory at least annually or upon significant changes.
Data Security and Privacy Lifecycle Management	Data Classification	**DSP-04**	Classify data according to its type and sensitivity level.

Data Security and Privacy Lifecycle Management	Data Flow Documentation	**DSP-05**	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.
Data Security and Privacy Lifecycle Management	Data Ownership and Stewardship	**DSP-06**	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.
Data Security and Privacy Lifecycle Management	Data Protection by Design and Default	**DSP-07**	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.

Data Security and Privacy Lifecycle Management	Data Privacy by Design and Default	**DSP-08**	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.
Data Security and Privacy Lifecycle Management	Data Protection Impact Assessment	**DSP-09**	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.
Data Security and Privacy Lifecycle Management	Sensitive Data Transfer	**DSP-10**	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.

Data Security and Privacy Lifecycle Management	Personal Data Access, Reversal, Rectification and Deletion	**DSP-11**	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.
Data Security and Privacy Lifecycle Management	Limitation of Purpose in Personal Data Processing	**DSP-12**	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.
Data Security and Privacy Lifecycle Management	Personal Data Sub-processing	**DSP-13**	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.

Data Security and Privacy Lifecycle Management	Disclosure of Data Sub-processors	**DSP-14**	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.
Data Security and Privacy Lifecycle Management	Limitation of Production Data Use	**DSP-15**	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.
Data Security and Privacy Lifecycle Management	Data Retention and Deletion	**DSP-16**	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.

Data Security and Privacy Lifecycle Management	Sensitive Data Protection	**DSP-17**	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.
Data Security and Privacy Lifecycle Management	Disclosure Notification	**DSP-18**	The providers should implement and describe to customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations.
Data Security and Privacy Lifecycle Management	Data Location	**DSP-19**	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.

Data Security and Privacy Lifecycle Management	Data Provenance and Transparency	**DSP-20**	Define, implement and evaluate processes, procedures and technical measures to: 1) Document and trace data sources, and 2) Make the data source available according to legal and regulatory requirements
Data Security and Privacy Lifecycle Management	Data Poisoning Prevention & Detection	**DSP-21**	Define, implement and evaluate processes, procedures and technical measures to prevent data poisoning in AI models and continuously detect such.
Data Security and Privacy Lifecycle Management	Privacy Enhancing Technologies	**DSP-22**	Use Privacy Enhancing Technologies for training data, informed by risk and privacy impact analysis and business use cases.

Data Security and Privacy Lifecycle Management	Data Integrity Check	**DSP-23**	Regularly validate the consistency and conformity of training, fine-tuning or augmentation data. Implement dataset versioning to ensure traceability and enforce restrictions to prevent unauthorized changes.
Data Security and Privacy Lifecycle Management	Data Differentiation and Relevance	**DSP-24**	Ensure training-data differentiation and relevance to the intended use of the AI Model.
Governance, Risk and Compliance-GRC			
Governance, Risk and Compliance	Governance Program Policy and Procedures	**GRC-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization and related to AI systems as well. Review and update the policies and procedures at least annually.

Governance, Risk and Compliance	Risk Management Program	**GRC-02**	Establish and maintain a formal, documented, and leadership-sponsored AI Risk Management (AIRM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks.
Governance, Risk and Compliance	Organizational Policy Reviews	**GRC-03**	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.
Governance, Risk and Compliance	Policy Exception Process	**GRC-04**	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.

Governance, Risk and Compliance	Information Security Program	**GRC-05**	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the AICM.
Governance, Risk and Compliance	Governance Responsibility Model	**GRC-06**	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.
Governance, Risk and Compliance	Information System Regulatory Mapping	**GRC-07**	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. Review at least annually or when a substantial change occurs within the organization.

Governance, Risk and Compliance	Special Interest Groups	**GRC-08**	Establish and maintain contact with related special interest groups and other relevant entities in line with business context.
Governance, Risk and Compliance	Acceptable Use of the AI Service	**GRC-09**	Define, document and enforce policies and procedures on the acceptable use of AI services offered by the organization. Ensure effectiveness by continuous risk assessments, reviews and human oversight.
Governance, Risk and Compliance	AI Impact Assessment	**GRC-10**	Establish, document, and communicate to all relevant stakeholders an AI Impact Assessment process and its criteria to regularly evaluate the ethical, societal, operational, legal, and security impacts of the AI system throughout its lifecycle.

Governance, Risk and Compliance	Bias and Fairness Assessment	**GRC-11**	Regularly evaluate AI systems, models, datasets & algorithms for bias and fairness to ensure compliance with ethical standards.
Governance, Risk and Compliance	Ethics Committee	**GRC-12**	Establish an ethics committee to review AI applications, ensuring alignment with ethical standards and organizational values.
Governance, Risk and Compliance	Explainability Requirement	**GRC-13**	Establish, document, and communicate the degree of explainability needed for the AI Services.
Governance, Risk and Compliance	Explainability Evaluation	**GRC-14**	Evaluate, document, and communicate the degree of explainability of the AI Services, including possible limitations and exceptions.

Governance, Risk and Compliance	Human supervision	**GRC-15**	Establish, execute, and assess processes, procedures, and technical measures to ensure human oversight and control of the AI system in compliance with regulatory requirements and organizational risk management.
Human Resources-HRS			
Human Resources	Background Screening Policy and Procedures	**HRS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.
Human Resources	Acceptable Use of Technology Policy and Procedures	**HRS-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.

Human Resources	Clean Desk Policy and Procedures	**HRS-03**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.
Human Resources	Remote and Home Working Policy and Procedures	**HRS-04**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.
Human Resources	Asset returns	**HRS-05**	Establish and document procedures for the return of organization-owned assets by terminated employees.

Human Resources	Employment Termination	**HRS-06**	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.
Human Resources	Employment Agreement Process	**HRS-07**	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.
Human Resources	Employment Agreement Content	**HRS-08**	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.

Human Resources	Personnel Roles and Responsibilities	**HRS-09**	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.
Human Resources	Non-Disclosure Agreements	**HRS-10**	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.
Human Resources	Security Awareness Training	**HRS-11**	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.

Human Resources	Personal and Sensitive Data Awareness and Training	**HRS-12**	Provide employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.
Human Resources	Compliance User Responsibility	**HRS-13**	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.
Human Resources	AI Competency Training	**HRS-14**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures defining the AI training program for all relevant personnel of the organization based on their roles and provide regular training updates.

Human Resources	AI Acceptable Use	**HRS-15**	Establish, document, and communicate to all personnel the policies and procedures on the acceptable use of AI technologies within the organization.
Identity & Access Management-IAM			
Identity & Access Management	Identity and Access Management Policy and Procedures	**IAM-01**	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually, or upon significant changes.
Identity & Access Management	Strong Password Policy and Procedures	**IAM-02**	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.

Identity & Access Management	Identity Inventory	**IAM-03**	Manage, store, and regularly review the inventory of identities, and monitor their level of access.
Identity & Access Management	Separation of Duties	**IAM-04**	Employ the separation of duties principle when implementing information system access.
Identity & Access Management	Least Privilege	**IAM-05**	Employ the least privilege principle when implementing information system access.

Identity & Access Management	User Access Provisioning	**IAM-06**	Define and implement an identity access provisioning process which authorizes, records, and communicates access changes to data and assets.
Identity & Access Management	User Access Changes and Revocation	**IAM-07**	De-provision or modify identity access in a timely manner.
Identity & Access Management	User Access Review	**IAM-08**	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurated with organizational risk tolerance and at least annually, or upon significant changes.

Identity & Access Management	Segregation of Privileged Access Roles	**IAM-09**	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.
Identity & Access Management	Management of Privileged Access Roles	**IAM-10**	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.
Identity & Access Management	Customers' Approval for Agreed Privileged Access Roles	**IAM-11**	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.

Identity & Access Management	Safeguard Logs Integrity	**IAM-12**	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.
Identity & Access Management	Uniquely Identifiable Users	**IAM-13**	Define, implement and evaluate processes, procedures and technical measures, that ensure identities' activities are identifiable through uniquely associated IDs.
Identity & Access Management	Strong Authentication	**IAM-14**	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.

Identity & Access Management	Passwords and Secrets Management	**IAM-15**	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords and other secrets.
Identity & Access Management	Authorization Mechanisms	**IAM-16**	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.
Identity & Access Management	Knowledge Access Control - Need to Know	**IAM-17**	Define policy and procedure for "need to know" access to knowledge, information and data within the organization and in the context of the AI system to be applied when regulating access to resources.

Identity & Access Management	Output Modification and Special Authorization	**IAM-18**	When allowing model output modification of AI generated output, establish a role for this access and allow changes only by authorized identities.
Identity & Access Management	Agent Access Restriction	**IAM-19**	Restrict agents' access to the tools and plugins necessary for the activity or use case at hand, ensuring adherence to the principles of need-to-know and least privilege.
Interoperability & Portability-IPY			
Interoperability & Portability	Interoperability and Portability Policy and Procedures	**IPY-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually or upon significant changes.

Interoperability & Portability	Application Interface Availability	**IPY-02**	Provide application interface(s) to AICs so that they programmatically retrieve their data to enable interoperability and portability.
Interoperability & Portability	Secure Interoperability and Portability Management	**IPY-03**	Implement cryptographically secure and standardized network protocols for the management, import and export of data, according to industry standards.
Interoperability & Portability	Data Portability Contractual Obligations	**IPY-04**	Agreements must include provisions specifying AICs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the AICs d. Data deletion policy
Infrastructure Security-I&S			

Infrastructure Security	Infrastructure and Virtualization Security Policy and Procedures	**I&S-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually, or upon significant changes.
Infrastructure Security	Capacity and Resource Planning	**I&S-02**	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.
Infrastructure Security	Network Security	**I&S-03**	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.

Infrastructure Security	OS Hardening and Base Controls	**I&S-04**	Harden host and guest OS, hypervisor or infrastructure control plane, according to their respective best practices, and supported by technical controls, as part of a security baseline.
Infrastructure Security	Production and Non-Production Environments	**I&S-05**	Separate production and non-production environments.
Infrastructure Security	Segmentation and Segregation	**I&S-06**	Design, develop, deploy and configure applications and infrastructures such that tenant access is appropriately segmented and segregated, monitored and restricted.

Infrastructure Security	Migration to Hosted Environments	**I&S-07**	Use secure and encrypted communication channels when migrating servers, services, applications, or data to hosted environments. Such channels must include only up-to-date and approved protocols.
Infrastructure Security	Network Architecture Documentation	**I&S-08**	Identify and document high-risk environments.
Infrastructure Security	Network Defense	**I&S-09**	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.
Logging and Monitoring-LOG			

Logging and Monitoring	Logging and Monitoring Policy and Procedures	**LOG-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually, or upon significant changes.
Logging and Monitoring	Audit Logs Protection	**LOG-02**	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.
Logging and Monitoring	Security Monitoring and Alerting	**LOG-03**	Identify and monitor security-related events within applications, the underlying infrastructure, supply chain, and consider logging other events based on risk evaluation. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.

Logging and Monitoring	Audit Logs Access and Accountability	**LOG-04**	Restrict access to audit logs and maintain records of access to logs.
Logging and Monitoring	Audit Logs Monitoring and Response	**LOG-05**	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.
Logging and Monitoring	Clock Synchronization	**LOG-06**	Use a reliable time source across all relevant information processing systems.

Logging and Monitoring	Logging Scope	**LOG-07**	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.
Logging and Monitoring	Log Records	**LOG-08**	Generate audit records containing relevant security information.
Logging and Monitoring	Log Protection	**LOG-09**	Protect audit records from unauthorized access, modification, and deletion.

Logging and Monitoring	Encryption Monitoring and Reporting	**LOG-10**	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.
Logging and Monitoring	Transaction/Activity Logging	**LOG-11**	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.
Logging and Monitoring	Access Control Logs	**LOG-12**	Monitor and log physical access using an auditable access control system.

Logging and Monitoring	Failures and Anomalies Reporting	**LOG-13**	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.
Logging and Monitoring	Input Monitoring	**LOG-14**	Log and monitor all input events (content and metadata) to enable auditing and reporting on the usage of AI models.
Logging and Monitoring	Output Monitoring	**LOG-15**	Log and monitor all output events (content and metadata) to enable auditing and reporting on usage of AI models.
Model Security-MDS			

Model Security	Training Pipeline Security	**MDS-01**	Define, implement, and evaluate policies, procedures, and technical measures that ensure the security of the Training Pipeline. Regularly review and update policies, procedures and technical measures to address new security threats and best practices.
Model Security	Model Artifact Scanning	**MDS-02**	Define, implement, and evaluate policies, procedures, and technical measures for the scanning of model artifacts for vulnerabilities and attacks, at each step of the service lifecycle and at each hand over point. Regularly review and update policies, procedures and technical measures to address model artifact scanning.
Model Security	Model Documentation	**MDS-03**	Define, implement, enforce, approve, document, communicate, maintain and evaluate processes and procedures for model documentation. Regularly review and update the model documentation.

Model Security	Model Documentation Requirements	**MDS-04**	Establish and implement baseline requirements for Model documentation.
Model Security	Model Documentation Validation	**MDS-05**	Define, implement, and evaluate processes, procedures, and technical measures for the validation of the Model documentation aligned with the current model.
Model Security	Adversarial Attack Analysis	**MDS-06**	Define, implement, and evaluate processes and technical measures to assess adversarial threats specific to each AI model.

Model Security	Robustness against Adversarial Attack / Model Hardening	**MDS-07**	Define, implement, and evaluate processes, procedures, and technical measures for Model Hardening to mitigate relevant adversarial attacks as identified in the Threat Analysis and Adversarial Threat Analysis.
Model Security	Model Integrity Checks	**MDS-08**	Regularly calculate and compare checksums using cryptographic hashes of model checkpoints to detect unauthorized modifications. Apply at least annually based on the level of risk, or after any change of hands.
Model Security	Model Signing/Ownership Verification	**MDS-09**	Sign models cryptographically and verify signatures to ensure model provenance and ownership, any time the model changes hands or is loaded from storage.
Model Security	Model Continuous Monitoring	**MDS-10**	Define, implement, and evaluate processes, procedures, and technical measures for continuous monitoring of model performance metrics over time to identify sudden shifts or unexpected changes in predictions that could degrade model performance.
Model Security	Model Failure	**MDS-11**	Perform a risk-based evaluation of the model and model serving infrastructure for model failure. Define and implement measures to mitigate model and model serving infrastructure failures, and regularly evaluate throughout the AI system's lifecycle.

Model Security	Open Model Risk Assessment	**MDS-12**	Establish a process to evaluate risk associated with open models. Periodically review these risk factors, and implement a process to monitor and mitigate any determined vulnerabilities.
Model Security	Secure Model Format	**MDS-13**	Adopt secure model formats and processes for AI model serialization where applicable.
Security Incident Management, E-Discovery, & Cloud Forensics-SEF			
Security Incident Management, E-Discovery, & Cloud Forensics	Security Incident Management Policy and Procedures	**SEF-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Forensics. Review and update the policies and procedures at least annually or upon significant changes.
Security Incident Management, E-Discovery, & Cloud Forensics	Service Management Policy and Procedures	**SEF-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually, or upon significant changes.

Security Incident Management, E-Discovery, & Cloud Forensics	Incident Response Plans	**SEF-03**	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: a communication strategy for notifying relevant internal departments, impacted AICs, and other business critical relationships (such as supply-chain) that may be impacted.
Security Incident Management, E-Discovery, & Cloud Forensics	Incident Response Testing	**SEF-04**	Follow a structured approach to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes.
Security Incident Management, E-Discovery, & Cloud Forensics	Incident Response Metrics	**SEF-05**	Establish, monitor and report information security incident metrics.

Security Incident Management, E-Discovery, & Cloud Forensics	Event Triage Processes	**SEF-06**	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.
Security Incident Management, E-Discovery, & Cloud Forensics	Security Breach Notification	**SEF-07**	Define and implement, processes, procedures and technical measures for security breach notifications. Report material security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.
Security Incident Management, E-Discovery, & Cloud Forensics	Points of Contact Maintenance	**SEF-08**	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. Review and update the points of contact at least annually.

Security Incident Management, E-Discovery, & Cloud Forensics	Incident Response	**SEF-09**	Define incident categories and severity levels for AI systems, and determine response procedures for each, including automated response where applicable.
Supply Chain Management, Transparency, and Accountability-STA			
Supply Chain Management, Transparency, and Accountability	Supply Chain Risk Management Policies and Procedures	**STA-01**	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for supply chain risk management. Review and update the policies and procedures at least annually or upon significant changes.
Supply Chain Management, Transparency, and Accountability	SSRM Policy and Procedures	**STA-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually, or upon significant changes.

Supply Chain Management, Transparency, and Accountability	SSRM Supply Chain	**STA-03**	Apply, document, implement and manage the SSRM throughout the supply chain.
Supply Chain Management, Transparency, and Accountability	SSRM Guidance	**STA-04**	Provide SSRM Guidance to the Customer detailing information about the SSRM applicability throughout the supply chain.
Supply Chain Management, Transparency, and Accountability	SSRM Control Ownership	**STA-05**	Delineate the shared ownership and applicability of all CSA AICM controls according to the SSRM.

Supply Chain Management, Transparency, and Accountability	SSRM Documentation Review	**STA-06**	Review and validate SSRM documentation.
Supply Chain Management, Transparency, and Accountability	SSRM Control Implementation	**STA-07**	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.
Supply Chain Management, Transparency, and Accountability	Supply Chain Inventory	**STA-08**	Develop and maintain an inventory of all supply chain relationships.

Supply Chain Management, Transparency, and Accountability	Supply Chain Risk Management	**STA-09**	Periodically review risk factors associated with supply chain relationships.
Supply Chain Management, Transparency, and Accountability	Primary Service and Contractual Agreement	**STA-10**	Service agreements must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy
Supply Chain Management, Transparency, and Accountability	Supply Chain Agreement Review	**STA-11**	Review supply chain agreements at least annually, or upon significant changes.

Supply Chain Management, Transparency, and Accountability	Supply Chain Compliance Assessment	**STA-12**	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.
Supply Chain Management, Transparency, and Accountability	Supply Chain Service Agreement Compliance	**STA-13**	Implement policies requiring all service providers throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.
Supply Chain Management, Transparency, and Accountability	Supply Chain Governance Review	**STA-14**	Periodically review the organization's supply chain partners' IT governance policies and procedures.

Supply Chain Management, Transparency, and Accountability	Supply Chain Data Security Assessment	**STA-15**	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.
Supply Chain Management, Transparency, and Accountability	Service Bill of Material (BOM)	**STA-16**	Define, implement, and enforce a process for establishing a Bill of Material for the service supply chain. Review and update the Bill of Material at least annually or upon significant changes.
Threat & Vulnerability Management-TVM			
Threat & Vulnerability Management	Threat and Vulnerability Management Policy and Procedures	**TVM-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities and threats, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually or upon significant changes.

Threat & Vulnerability Management	Malware and Malicious Instructions Protection Policy and Procedures	**TVM-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware and malicious instructions. Review and update the policies and procedures at least annually or upon significant changes.
Threat & Vulnerability Management	Vulnerability Identification	**TVM-03**	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.
Threat & Vulnerability Management	Detection Updates	**TVM-04**	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.

Threat & Vulnerability Management	External Library Vulnerabilities	**TVM-05**	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.
Threat & Vulnerability Management	Penetration Testing	**TVM-06**	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.
Threat & Vulnerability Management	Vulnerability Remediation Schedule	**TVM-07**	Define, implement and evaluate processes, procedures and technical measures based on identified risks to support scheduled and emergency responses to vulnerability identification.

Threat & Vulnerability Management	Vulnerability Prioritization	**TVM-08**	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.
Threat & Vulnerability Management	Vulnerability Management Reporting	**TVM-09**	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.
Threat & Vulnerability Management	Vulnerability Management Metrics	**TVM-10**	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.

Threat & Vulnerability Management	Guardrails	**TVM-11**	Define and implement processes, procedures and technical measures to apply guardrails to the AI system. Continuously evaluate guardrails for changes in regulatory requirements and risk scenarios.
Threat & Vulnerability Management	Threat Analysis and Modelling	**TVM-12**	Define implement and evaluate threat analysis process and procedures to identify, assess and review the threat landscape for Cloud and AI systems. Build threat models according to industry best practices to inform the risk mitigation strategy.
Threat & Vulnerability Management	Threat Response	**TVM-13**	Use a risk-based method for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures.
Universal Endpoint Management-UEM			

Universal Endpoint Management	Endpoint Devices Policy and Procedures	**UEM-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually or upon significant system changes.
Universal Endpoint Management	Application and Service Approval	**UEM-02**	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.
Universal Endpoint Management	Compatibility	**UEM-03**	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.

Universal Endpoint Management	Endpoint Inventory	**UEM-04**	Maintain an inventory of all endpoints used to store and process company data.
Universal Endpoint Management	Endpoint Management	**UEM-05**	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.
Universal Endpoint Management	Automatic Lock Screen	**UEM-06**	Configure all relevant interactive-use endpoints to require an automatic lock screen.

Universal Endpoint Management	Operating Systems	**UEM-07**	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.
Universal Endpoint Management	Storage Encryption	**UEM-08**	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.
Universal Endpoint Management	Anti-Malware Detection and Prevention	**UEM-09**	Configure managed endpoints with anti-malware detection and prevention technology and services.

Universal Endpoint Management	Software Firewall	**UEM-10**	Configure managed endpoints with properly configured software firewalls.
Universal Endpoint Management	Data Loss Prevention	**UEM-11**	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.
Universal Endpoint Management	Remote Locate	**UEM-12**	Enable remote geo-location capabilities for all managed mobile endpoints, according to all applicable laws and regulations.

Universal Endpoint Management	Remote Wipe	**UEM-13**	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.
Universal Endpoint Management	Third-Party Endpoint Security Posture	**UEM-14**	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.