GOVERNANCE

GOVERNANCE

EQUITABLE GROWTH, FINANCE & INSTITUTIONS INSIGHT

Data Classification Matrix and Cloud Assessment Framework

Cloud Assessment Framework and Evaluation Methodology

World Bank Advisory Services and Analytics

Supported by the GovTech Global Partnership - www.worldbank.org/govtech

WORLD BANK GROUP

GovTech
Putting people first

1818 H Street NW,
Washington DC 20433
Telephone: 202-473-1000;
Internet: www.worldbank.org

>>>

Contents

Tables

>>>

Acknowledgments

This note has been developed under the World Bank GovTech Global Partnership by a team led by Khuram Farooq (Senior Governance Specialist). The World Bank team was composed of Hunt La Cascia (Senior Public Sector Specialist); Knut Leipold (Lead Procurement Specialist); and Bertram Boie (Senior Digital Development Specialist); Robert Shields (Consultant); and Constantine Pagedas (Consultant). Overall guidance for the report was provided by Tracey Marie Lane (Practice Manager, Governance GP); Edward Olowo-Okere (Senior Advisor, EFI VP); Arturo Herrera Gutierrez (Global Director, Governance GP); and Donna Andrews (Acting Practice Manager, Governance GP).

The note benefited from the expertise of the following World Bank experts: Natalija Gelvanovska-Garcia (Senior Digital Development Specialist), Dolele Sylla (Senior Governance Specialist) and Ishtiak Siddique (Senior Procurement Specialist).

The note also benefited from the expertise of the following individuals: Matt Jodlowski (Australia, Policy Lead, Digital Strategy, Digital Transformation Agency); Bushra Al Blooshi (UAE, Research and Innovation Head, Dubai Electronic Security Center, Digital Dubai); Ben Vandersteen (United Kingdom, Technical Architect, Government Digital Service); Ayanda Nkundla (South Africa, Senior Manager, ICT Compliance, Department of Public Service and Administration); Alufheli Swalivha (South Africa, Director, Public Service ICT Stakeholder Management, Department of Public Service and Administration); Zaid Aboobaker (South Africa, Chief Director, E-Government, Department of Public Service and Administration); and various officials from Japan's Information-technology Promotion Agency.

The following members of a Cloud Computing Working Group initiated by the World Bank GovTech initiative contributed their expertise: Cheow Hoe Chan (Singapore, Government Chief Digital Technology Officer, GovTech Singapore); Richard Tay (Singapore, Head for the Whole-of-Government Operations, GovTech Singapore); Karen Kee (Singapore, Deputy Director, GovTech Singapore); Ben Vandersteen (United Kingdom, Technical Architect, Government Digital Service); Liz Lutgendorff (United Kingdom, International Lead Insight and Analysis Advisor, Government Digital Service); Abhishek Singh (India, President and CEO, National eGov Dept, Ministry of Electronics and IT); Bramhanand Jha (India, Sr. Consultant, Program Management, Ministry of Electronics and IT); Vinay Thakur (India, COO, National eGovernance Division, Ministry of Electronics and IT); Rachel Ran (Israel, Head of Cloud Strategy, National Digital Agency); Keren Katsir Stiebel (Israel, CMO, Director of Marketing, Communications and Foreign

Affairs, Government ICT Authority); Toshiyuki Zamma (Japan, Head of International Strategy, Digital Agency); Kensuke Yabata (Japan, Director, Digital Agency); Sungjoo Son (South Korea, Director, Ministry of the Interior and Safety); Erica Dubach (Switzerland, Head of Division on Transformation and Interoperability, Swiss Federal Chancellery); Philippe Bruegger (Switzerland, Project Manager, SECO); Natalie Bertsch (Switzerland, Project Manager, SECO); Bushra Al Blooshi (UAE, Research and Innovation Head - Dubai Electronic Security Center, Digital Dubai); Ahmed AlSalman (UAE, Senior Manager Cloud Services, The Telecommunications and Digital Government Regulatory Authority); Omar Alriyami (UAE, Director, Data Analysis and Engineering, Statistics Centre, Abu Dhabi); Aziz Alkayyoomi (UAE, Acting Director of Information Technology, Statistics Centre, Abu Dhabi); and Maximiliano Maneiro (Uruguay, Emerging Technologies Manager, Electronic Government and Information and Knowledge Society Agency).

Richard Crabbe provided editorial services, and Maria Lopez designed the final publication.

This report was made possible by the World Bank's GovTech Initiative and the GovTech Global Partnership trust fund, building on support of financial and in-kind partners that include the Ministry of Finance of Austria, the State Secretariat for Economic Affairs (SECO) of Switzerland, the Ministry of Economy and Finance (MOEF) of the Republic of Korea, the Ministry of Economic Development of the Russian Federation, the Ministry of Interior and Safety (MOIS) of the Republic of Korea, the Government of Japan and the Federal Ministry for Economic Cooperation and Development (BMZ) of Germany.

>>>

Introduction

This *Data Classification Matrix and Cloud Assessment Framework* ("the Framework") supports the policy goals articulated in the World Bank's *Institutional and Procurement Practice Note for Cloud Computing Services in the Public Sector* ("the Practice Note"). The Framework is intended to support World Bank client countries, practitioners, and multilateral and bilateral development partners ("readers") to manage the risks of acquiring public cloud solutions. These suggestions are based on good practices identified in the Practice Note.

The Framework first offers a data classification scheme for government data and personally identifiable information (PII)[1] of citizens that governments and their contractors handle based upon the confidentiality, integrity, and availability security objectives. The Framework then suggests cloud security requirements corresponding to each proposed data classification level. These proposed security requirements are based upon international standards and "good practices" identified in the Practice Note. The Framework also offers a Checklist for procuring agencies seeking to procure cloud services.

Data and Information System Categorizations

1.1 Security Objectives

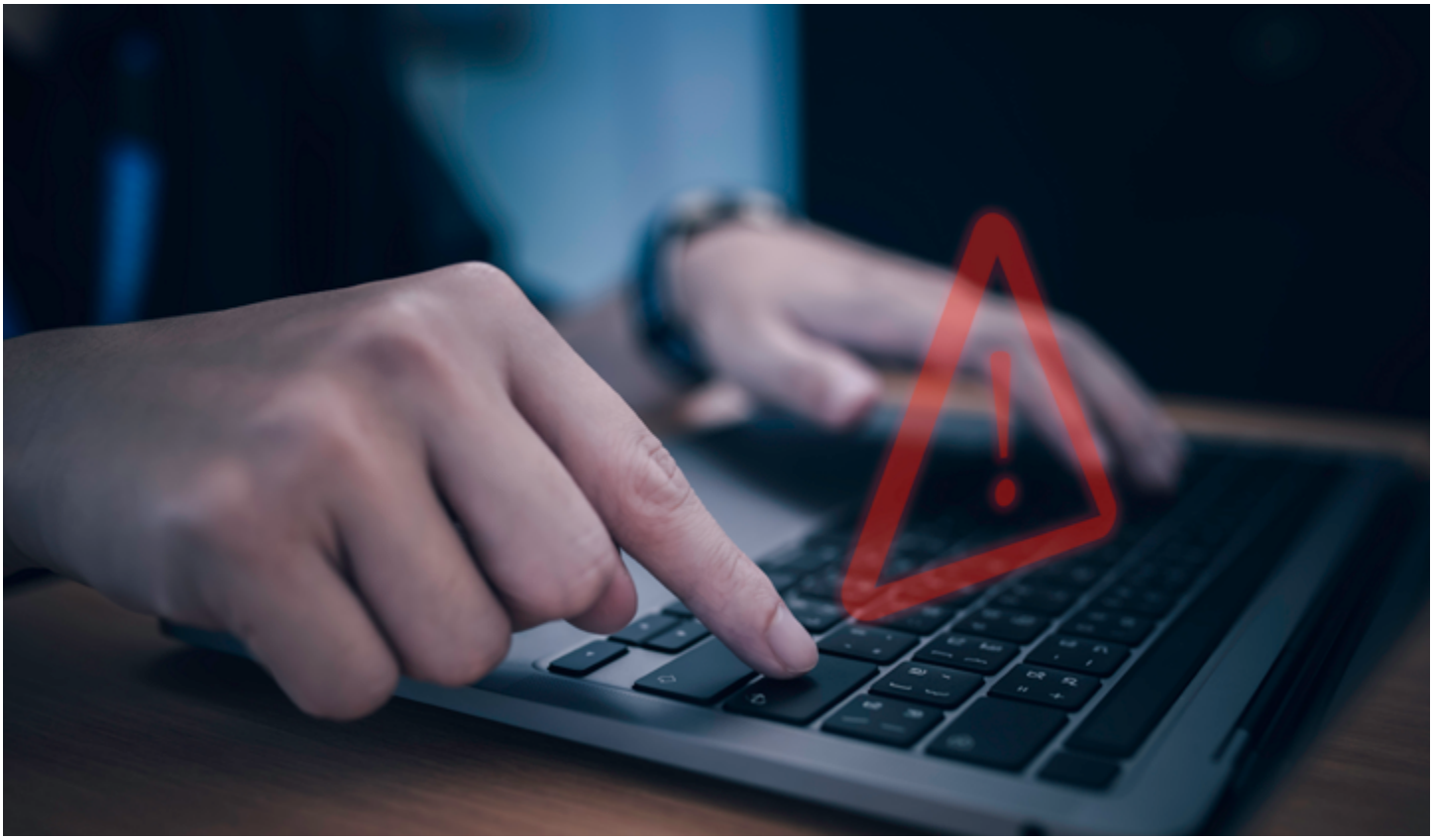
The determination of data classification levels is based on three security objectives commonly cited across various international and national-level security requirements, such as ISO/IEC 27001.

- **Confidentiality** means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy (PII) and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

- **Integrity** involves guarding against improper information modification or destruction and includes ensuring information's non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- **Availability** means ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.[2]

The combined "Confidentiality, Integrity, Availability" (CIA) framework is the basis for this data classification matrix.



1.2 Potential Impacts

International and national organizations also typically consider three levels of potential impact on organizations or individuals should there be a breach of security – a loss of CIA. These potential impact levels which inform the overall data classification scheme are described below.

- **Low Impact:** The loss of CIA could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals.
    - For example, the loss of CIA could cause a minor degradation in mission capability, and result in minor damage to organizational assets, minor financial loss, or minor harm to individuals.[3]
- **Moderate Impact:** The loss of CIA could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals.
    - For example, the loss of CIA could cause a significant degradation in mission capability, and result in significant damage to organizational assets, significant financial loss, or significant harm to individuals that does not involve loss of life or serious life-threatening injuries.[4]
- **High Impact:** The loss of CIA could be expected to have a ***severe*** or ***catastrophic*** adverse effect on organizational operations, organizational assets, or individuals.
    - For example, the loss of CIA could cause a severe degradation in mission capability, resulting in major damage to organizational assets, major financial loss; or severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.[5]

2

>>>

Public Data

Public Data is data produced by government or private entities that may be openly disclosed to individuals and governmental or non-governmental organizations for use, reuse, and sharing with third parties. There is no or very limited CIA impact of the loss of Public Data on organizational operations, organizational assets, or individuals. Generally, public sector entities seeking cloud services that process, store, or otherwise handle Public Data could procure cloud services from any government contractor. Moreover, in general, Public Data do not need to have any geographic boundary restrictions.

3

>>>

Four Levels of Data Classification – Public, Official, Secret, and Top Secret

Table 1 below offers a four-tiered data classification matrix. This matrix is meant to be customizable to each country's existing data classification scheme. Data owners within public sector entities should be responsible for conducting a review of their data to determine the classification levels of their data and information systems.

> > >

TABLE 1 - Suggested Data Classification Levels

	Public	Official	Secret	Top Secret
Impact on CIA	**Low Impact:**	**Moderate Impact:**	**High Impact:**	**High Impact:**
	The loss of confidentiality, integrity, or availability could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality, integrity, or availability could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality, integrity, or availability for **Secret** Data could be expected to have a ***severe*** or ***catastrophic*** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality, integrity, or availability for **Top Secret** Data could be expected to have an ***exceptionally grave*** adverse effect on organizational operations, organizational assets, or individuals.

Source: Cyber Security Principles | Cyber.gov.au.

It is suggested that public sector entities employ a "high watermark" policy for data classification: the overall impact level of data or information should equal the highest impact level among the three security objectives (Confidentiality, Integrity, Availability). For example, a system with data classified as Low-Impact Confidentiality, Moderate-Impact Integrity, and Low-Impact Availability would be considered a Moderate-Impact system overall and would therefore be considered at the "Official" data classification level.

The UK has adopted a principles-based and sensitivity/risk-based approach on data classification, with a focus on confidentiality, availability, and integrity. By avoiding specificity and focusing on outcomes, the UK classification system allows for adaptation for each particular category or classification of government data and uses of such data, and further for the opportunity to supplement as appropriate by government department specific contractual requirements.[6]

4

>>>

Suggested Cloud Security Requirements for Public, Official, Secret, and Top Secret Data

4.1 Certifications

Each country should determine a cloud security requirements regime that fits its risk profile and e-government capabilities. This report offers two options for consideration:

- **Option 1: Simplified Approach.** Under this system, a country would require CSPs to demonstrate that they possess certain international certifications in order to handle nonpublic data. This approach is suggested for countries with less mature e-government capabilities.

- **Option 2: Tiered Approach.** Here, a country would establish a tiered certification system that enacts certain security control requirements for each data classification level. This approach may be preferrable for countries with advanced e-government capabilities.

OPTION 1: Simplified Approach

A country could leverage existing international cybersecurity standards, such as ISO/IEC and Cloud Security Alliance (CSA) security controls. Both ISO/IEC and CSA certifications are highly respected, widely used global cybersecurity standards that many CSPs already possess. Moreover, it is much simpler and easier for countries to verify a CSP's compliance with these international certifications instead of developing and using a new set of security controls. As such, Option 1 may be more compatible for governments without existing capabilities to conduct thorough security assessments of cloud services.

Under this suggested framework, procuring agencies processing or storing nonpublic data must procure cloud services that possess the following international certifications:

- ISO/IEC 27001 with the ISO/IEC 27017 extension, ***AND***
- CSA Level 2 STAR (using CSA Cloud Control Matrix 4.0.5).[7]

A country can create a process whereby a CSP's compliance with the ISO and CSA certifications undergo a light-touch verification by a certification body (also called a third-party assessor (3PA)) accredited under the ISO/IEC 17021-1:2015 certification. A typical light-touch on-site verification process should take no more than two days to complete.

- Entities conducting a verification of a CSP's certification under this scheme should adopt the concept of "inheritance," whereby every layer of the cloud stack must be certified. For example, if a SaaS is built upon a certified PaaS or IaaS, an assessor must only assess the SaaS.

Procuring agencies processing or storing Public Data should not be required to procure cloud services that possess an ISO or CSA certification. However, ISO or CSA certification is recommended. Alternatively, alignment with such security standards is encouraged.

Exemption for Certain CSPs for Official Data: ISO and CSA certifications may be cost-prohibitive for some local CSPs identified as small and medium-sized enterprises (SMEs).[8] As such, countries should consider providing a less cost-prohibitive path for local SMEs[9] seeking to handle nonpublic data.

- For local SMEs that do not obtain the ISO or CSA certifications, procuring agencies may consider the security of the cloud services offerings of these businesses for systems that handle Official Data on a case-by-case basis.
- During the case-by-case considerations, the local SME must be able to self-attest adherence to a reputable security standard, such as the CSA Level 1: Self-Assessment. In turn, a procuring agency (or another government office) should conduct an on-site verification of the self-attestation.
- That said, local SMEs with SaaS offerings could benefit from the concept of inheritance, whereby it should only be assess by the software layer of the cloud stack if it is built upon a certified PaaS or IaaS.

OPTION 2: Tiered Approach

A country could use a tiered approach to pre-approve CSPs for government procurement. For example, a country could create certification requirements based upon the security controls within the US government's FedRAMP program – taken from the NIST Special Publication 800-53 (Revision 5) catalogue of security controls.[10] The current number of controls for each FedRAMP baseline[11] are provided below.:

- FedRAMP Low Baseline: 150 controls.
- FedRAMP Moderate Baseline: 304 controls.
- FedRAMP High Baseline: 392 controls.

A country can create a process whereby a 3PA certifies a cloud service's compliance with the Low, Moderate, or High Baselines based upon FedRAMP controls. Unlike Option 1, this process requires high technical experience with the government. Indeed, this process would typically take several weeks or months to complete. As such, Option 2 may be more compatible for governments that have existing capabilities to conduct thorough security assessments of cloud services.

4.2 Data Residency

Procuring agencies should take a risk-based approach to data residency. As the data classification level increases from Public to Top Secret, so should the consideration of requiring CSPs to process, store, and transmit data within a country's geographic boundaries. This Framework proposes the following data residency policy.

- **Public Data:** Data residency should not be required for Public Data.
- **Official Data:** Each country should make a risk-informed decision at the policy level (such as the Cabinet Office) on

whether it should enact a data residency requirement for Official Data.

- There are numerous legal and security considerations when determining whether government data should be retained within the country's geographic boundaries. Key considerations include whether other countries have appropriate data protection laws and whether there are existing data transfer agreements in place with other countries.

- A country may instead choose to provide policy-level *guidance* to procuring agencies, which would be ultimately responsible for determining data residency requirements for their Official Data. In such cases, the policy-level guidance would outline the considerations for procuring agencies when making a risk-based decision on data residency requirements of their cloud contracts. Each procuring agency's decision should depend largely upon *where* (in which country) the data would be handled and whether that country has consistent data protection laws and has an existing data transfer agreement, meaning sufficient legal protections for the data.

- **Secret and Top Secret Data:** CSPs should be required to ensure data remains within the country's geographic boundaries for Secret Data and Top Secret Data.

4.3 Cloud Deployment Models

It is advised that the public cloud should be the preference for procuring agencies handling Public Data and Official Data. In cases concerning Secret Data or Top Secret Data, procuring agencies should instead seek private cloud or community cloud offerings (such as a government cloud). Procuring agencies may also prefer on-premises information systems instead of private or government cloud solutions.

4.4 Security Clearances

Countries should strongly consider establishing a policy that any commercial entity offering computing services handling Secret Data or Top Secret Data should be required to obtain security clearances for its employees in alignment with national policies.

Table 2 below outlines a suggested cloud security requirements corresponding to each data classification level. This Table is intended to be customizable to each country's context.

> > >

TABLE 2 - Suggested Cloud Security Requirements – OPTION 1 (Simplified Approach)

Cloud Security Requirements	Public	Official	Secret/Top Secret
Certifications	No Requirement (ISO or CSA Certification alignment is encouraged)	ISO or CSA Certification Required (with exemptions for small and local CSPs)	ISO or CSA Certification Required
Data Residency	Not Required	Determined at the Policy Level	Required
Cloud Deployment Type	Any cloud deployment (public cloud preferred)	Any cloud deployment (public cloud preferred)	Private or community clouds (i.e., government clouds ("GCloud")) *only*. All data processing, storage, and transit to occur on-premise.
Security Clearances for Vendors	Not Required	Not Required	Required

> > >

TABLE 3 - Suggested Cloud Security Requirements – OPTION 2 (Tiered Approach)

Cloud Security Requirements	Public	Official	Secret/Top Secret
Certifications	FedRAMP Low Baseline	FedRAMP Moderate Baseline	FedRAMP High Baseline
Data Residency	Not Required	Determined at the Policy Level	Required
Cloud Deployment Type	Any cloud deployment (public cloud preferred)	Any cloud deployment (public cloud preferred)	Private or community clouds (i.e., government clouds ("GCloud")) *only*. All data processing, storage, and transit to occur on-premise.
Security Clearances for Vendors	Not Required	Not Required	Required

The above considerations are meant to be broadly applicable to countries, which can customize their approach to secure cloud procurement based upon their specific context.

Suggested Checklists for Procuring Agencies

Each procuring agency is ultimately responsible for the risk management of its data and information systems. As such, each procuring agency must work with the CSP, any 3PAs, and other entities such as a central cybersecurity body to ensure cybersecurity and data privacy risks related to its data are properly managed.

Procuring agencies may refer to the Checklist below, based upon the South African Department of Public Service and Administration's 2022 *Public Service Cloud Computing Determination and Directive.* This Checklist offers key considerations for a procuring agency during the pre-procurement, cloud consumption, and cloud termination phases of a cloud service procurement lifecycle. Countries may customize the Checklist to their specific contexts.

> > >

TABLE 4 - Suggested Considerations for Procuring Agencies Seeking Cloud Services

Action	Detail
Pre-Procurement	
Data Classification	The procuring agency must classify their information systems and data. Table 1 offers a suggested Data Classification Matrix to consider.
Data Residency	Data residency requirements should be followed. Tables 2 and 3 offers a suggested data residency policy based upon data classification levels.
Risk and Readiness Assessment	The procuring agency should consider facilitating an internal Risk Assessment and Cloud Readiness Assessment before procuring cloud services to ensure the agency has the technical capacity to integrate the cloud service into its environment.
Business Case	The procuring agency should consider facilitating preparation of a Business Case for a cloud service that may include the following elements: • Scope of cloud service required. • Budget and total cost of ownership calculation. • Human resource skills required to support the cloud services environment. • Infrastructure required to enable the cloud service. • Intended benefit of the cloud service. • Outcome of the Risk and Readiness Assessments.
Cloud Security Requirements	The procuring agency must identify any cloud security requirements of the cloud service contract based upon the data classification levels of the relevant information system(s) (see Section 4.1 above).
Compliance with Laws, Regulations, and Agency Guidance	The procuring agency must ensure that security of the data aligns with any relevant national laws and regulations, and existing department information security policies.
Contract	The procuring agency must conclude a valid contract with a CSP before using a cloud service. See **Box 4** of the *Institutional and Procurement Practice Note for Cloud Computing Services in the Public Sector* for additional guidance.
Contract Length	The procuring agency should consider short-term contracts (two years or less), with portability options to avoid vendor lock-in.
Cloud Service Consumption	
Data backups	The procuring agency should work with the CSP to ensure a mechanism to back up data on the cloud.
Data protection and ownership	The procuring agency should ensure that the CSP has no ownership rights on the stored data regardless of the format or storage medium and that proper protection mechanism is being applied.

Table 4 continued

Action	Detail
Cloud Service Consumption	
Service continuity	The procuring agency should ensure that proper cloud security controls are implemented by the CSP, addressing agency's requirements for periodic testing of the continuity and disaster recovery plans, and communicating the results to agency.
Continuous Monitoring	The procuring agency is responsible for working with CSPs to maintain a secure public cloud environment. Activities may include security incident notifications and security control change notifications.
Cloud Service Termination	
Protecting Data and Applications	The procuring agency should ensure that all data and/or applications are transferred to a new CSP, returned to the agency, and/or permanently deleted at the conclusion of the contract. See **Box 3** for data migration considerations.

>>>

Certification Verification Outline

This section lists the security controls for the ISO/IEC 27001 with the ISO/IEC 27017 extension and the CSA Level 2 STAR (using CSA Cloud Control Matrix 4.0.5).

6.1 ISO/IEC Controls

6.1.1 ISO/IEC 27001:2013

> > >
TABLE 5 - ISO/IEC 27001:2013 Controls Table

Section	Information Security Control
A.5	**Information security policies**
A.5.1	**Management direction for information security**
A5.1.1	Policies for information security
A5.1.2	Review of the policies for information security
A.6	**Organization of information security**
A.6.1	Internal organization
A.6.1.1	Information security roles and responsibilities
A.6.1.2	Segregation of duties
A.6.1.3	Contact with authorities
A.6.1.4	Contact with special interest groups
A.6.1.5	Information security in project management
A.6.2	**Mobile devices and teleworking**
A.6.2.1	Mobile device policy
A.6.2.2	Teleworking
A.7	**Human resource security**
A.7.1	**Prior to employment**
A.7.1.1	Screening
A.7.1.2	Terms and conditions of employment
A.7.2	**During employment**
A.7.2.1	Management responsibilities
A.7.2.2	Information security awareness, education and training

Table 5 continued

Section	Information Security Control
A.7.2.3	Disciplinary process
A.7.3	**Termination and change of employment**
A.7.3.1	Termination or change of employment responsibilities
A.8	**Asset management**
A.8.1	**Responsibility for assets**
A.8.1.1	Inventory of assets
A.8.1.2	Ownership of assets
A.8.1.3	Acceptable use of assets
A.8.1.4	Return of assets
A.8.2	**Information classification**
A.8.2.1	Classification of information
A.8.2.2	Labelling of information
A.8.2.3	Handling of assets
A.8.3	**Media handling**
A.8.3.1	Management of removable media
A.8.3.2	Disposal of media
A.8.3.3	Physical media transfer
A.9	**Access control**
A.9.1	**Business requirements of access control**
A.9.1.1	Access control policy
A.9.1.2	Access to networks and network services
A.9.2	**User access management**
A.9.2.1	User registration and de-registration
A.9.2.2	User access provisioning
A.9.2.3	Management of privileged access rights

Table 5 continued

Section	Information Security Control
A.9.2.4	Management of secret authentication information of users
A.9.2.5	Review of user access rights
A.9.2.6	Removal or adjustment of access rights
A.9.3	**User responsibilities**
A.9.3.1	Use of secret authentication information
A.9.4	**System and application access control**
A.9.4.1	Information access restriction
A.9.4.2	Secure log-on procedures
A.9.4.3	Password management system
A.9.4.4	Use of privileged utility programs
A.9.4.5	Access control to program source code
A.10	**Cryptography**
A.10.1	**Cryptographic controls**
A.10.1.1	Policy on the use of cryptographic controls
A.10.1.2	Key management
A.11	**Physical and environmental security**
A.11.1	**Secure areas**
A.11.1.1	Physical security perimeter
A.11.1.2	Physical entry controls
A.11.1.3	Securing offices, rooms and facilities
A.11.1.4	Protecting against external and environmental threats
A.11.1.5	Working in secure areas
A.11.1.6	Delivery and loading areas
A.11.2	**Equipment**
A.11.2.1	Equipment siting and protection

Table 5 continued

Section	Information Security Control
A.11.2.2	Supporting utilities
A.11.2.3	Cabling security
A.11.2.4	Equipment maintenance
A.11.2.5	Removal of assets
A.11.2.6	Security of equipment and assets off-premises
A.11.2.7	Secure disposal or reuse of equipment
A.11.2.8	Unattended user equipment
A.11.2.9	Clear desk and clear screen policy
A.12	**Operations security**
A.12.1	**Operational procedures and responsibilities**
A.12.1.1	Documented operating procedures
A.12.1.2	Change management
A.12.1.3	Capacity management
A.12.1.4	Separation of development, testing and operational environments
A.12.2	**Protection from malware**
A.12.2.1	Controls against malware
A.12.3	**Backup**
A.12.3.1	Information backup
A.12.4	**Logging and monitoring**
A.12.4.1	Event logging
A.12.4.2	Protection of log information
A.12.4.3	Administrator and operator logs
A.12.4.4	Clock synchronization
A.12.5	**Control of operational software**
A.12.5.1	Installation of software on operational systems

Table 5 continued

Section	Information Security Control
A.12.6	**Technical vulnerability management**
A.12.6.1	Management of technical vulnerabilities
A.12.6.2	Restrictions on software installation
A.12.7	**Information systems audit considerations**
A.12.7.1	Information systems audit controls
A.13	**Communications security**
A.13.1	**Network security management**
A.13.1.1	Network controls
A.13.1.2	Security of network services
A.13.1.3	Segregation in network
A.13.2	**Information transfer**
A.13.2.1	Information transfer policies and procedures
A.13.2.2	Agreements on information transfer
A.13.2.3	Electronic messaging
A.13.2.4	Confidentiality or nondisclosure agreements
A.14	**System acquisition, development and maintenance**
A.14.1	**Security requirements of information systems**
A.14.1.1	Information security requirements analysis and specification
A.14.1.2	Securing application services on public networks
A.14.1.3	Protecting application services transactions
A.14.2	**Security in development and support processes**
A.14.2.1	Secure development policy
A.14.2.2	System change control and procedures
A.14.2.3	Technical review of applications after operating platform changes
A.14.2.4	Restrictions on changes to software packages

Table 5 continued

Section	Information Security Control
A.14.2.5	Secure system engineering principles
A.14.2.6	Secure development environment
A.14.2.7	Outsourced development
A.14.2.8	System security testing
A.14.2.9	System acceptance testing
A.14.3	**Test data**
A.14.3.1	Protection of test data
A.15	**Supplier relationships**
A.15.1	**Information security in supplier relationships**
A.15.1.1	Information security policy for supplier relationships
A.15.1.2	Addressing security within supplier agreements
A.15.1.3	Information and communication technology supply chain
A.15.2	**Supplier service delivery management**
A.15.2.1	Monitoring and review of supplier services
A.15.2.2	Managing changes to supplier services
A.16	**Information security incident management**
A.16.1	Management of information security incidents and improvements
A.16.1.1	Responsibilities and procedures
A.16.1.2	Reporting information security events
A.16.1.3	Reporting information security weaknesses
A.16.1.4	Assessment of and decision on information security events
A.16.1.5	Response to information security incidents
A.16.1.6	Learning from information security incidents
A.16.1.7	Collection of evidence

Table 5 continued

Section	Information Security Control
A.17	**Information security aspects of business continuity management**
A.17.1	**Information security continuity**
A.17.1.1	Planning information security continuity
A.17.1.2	Implementing information security continuity
A.17.1.3	Verify, review and evaluate information security continuity
A.17.2	**Redundancies**
A.17.2.1	Availability of information processing facilities
A.18	**Compliance**
A.18.1	**Compliance with legal and contractual requirements**
A.18.1.1	Identification of applicable legislation and contractual requirements
A.18.1.2	Intellectual property rights
A.18.1.3	Protection of records
A.18.1.4	Privacy and protection of personally identifiable information
A.18.1.5	Regulation of cryptographic controls
A.18.2	**Information security reviews**
A.18.2.1	Independent review of information security
A.18.2.2	Compliance with security policies and standards
A.18.2.3	Technical compliance review

6.1.2 ISO/IEC 27017:2015 Extension

> > >
TABLE 6 - ISO/IEC 27017:2015 Extension Controls Table

Section	Information Security Control
CLD.6.3	**Relationship between cloud service customer and cloud service provider**
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment
CLD.8.1	**Responsibility for assets**
CLD.8.1.5	Removal of cloud service customer assets
CLD.9.5	**Access control of cloud service customer data in shared virtual environment**
CLD.9.5.1	Segregation in virtual computing environments
CLD.9.5.2	Virtual machine hardening
CLD.12.1	**Operational procedures and responsibilities**
CLD.12.1.5	Administrator's operational security
CLD.12.4	**Logging and monitoring**
CLD.12.4.5	Monitoring of Cloud Services
CLD.13.1	**Network security management**
CLD.13.1.4	Alignment of security management for virtual and physical networks

6.2 CSA Level 2 STAR Controls

> > >
TABLE 7 - CCM v4.0.5 Controls Table

Control ID	Information Security Control
Audit & Assurance	
A&A-01	Audit and Assurance Policy and Procedures
A&A-02	Independent Assessments
A&A-03	Risk Based Planning Assessment
A&A-04	Requirements Compliance

Table 7 continued

Control ID	Information Security Control
Audit & Assurance	
A&A-05	Audit Management Process
A&A-06	Remediation
Application & Interface Security	
AIS-01	Application and Interface Security Policy and Procedures
AIS-02	Application Security Baseline Requirements
AIS-03	Application Security Metrics
AIS-04	Secure Application Design and Development
AIS-05	Automated Application Security Testing
AIS-06	Automated Secure Application Deployment
AIS-07	Application Vulnerability Remediation
Business Continuity Management and Operational Resilience	
BCR-01	Business Continuity Management Policy and Procedures
BCR-02	Risk Assessment and Impact Analysis
BCR-03	Business Continuity Strategy
BCR-04	Business Continuity Planning
BCR-05	Documentation
BCR-06	Business Continuity Exercises
BCR-07	Communication
BCR-08	Backup
BCR-09	Disaster Response Plan
BCR-10	Response Plan Exercise
BCR-11	Equipment Redundancy

Table 7 continued

Control ID	Information Security Control
Change Control and Configuration Management	
CCC-01	Change Management Policy and Procedures
CCC-02	Quality Testing
CCC-03	Change Management Technology
CCC-04	Unauthorized Change Protection
CCC-05	Change Agreements
CCC-06	Change Management Baseline
CCC-07	Detection of Baseline Deviation
CCC-08	Exception Management
CCC-09	Change Restoration
Cryptography, Encryption & Key Management	
CEK-01	Encryption and Key Management Policy and Procedures
CEK-02	CEK Roles and Responsibilities
CEK-03	Data Encryption
CEK-04	Encryption Algorithm
CEK-05	Encryption Change Management
CEK-06	Encryption Change Cost Benefit Analysis
CEK-07	Encryption Risk Management
CEK-08	CSC Key Management Capability
CEK-09	Encryption and Key Management Audit
CEK-10	Key Generation
CEK-11	Key Purpose
CEK-12	Key Rotation
CEK-13	Key Revocation
CEK-14	Key Destruction

Table 7 continued

Control ID	Information Security Control
Cryptography, Encryption & Key Management	
CEK-15	Key Activation
CEK-16	Key Suspension
CEK-17	Key Deactivation
CEK-18	Key Archival
CEK-19	Key Compromise
CEK-20	Key Recovery
CEK-21	Key Inventory Management
Datacenter Security	
DCS-01	Off-Site Equipment Disposal Policy and Procedures
DCS-02	Off-Site Transfer Authorization Policy and Procedures
DCS-03	Secure Area Policy and Procedures
DCS-04	Secure Media Transportation Policy and Procedures
DCS-05	Assets Classification
DCS-06	Assets Cataloguing and Tracking
DCS-07	Controlled Access Points
DCS-08	Equipment Identification
DCS-09	Secure Area Authorization
DCS-10	Surveillance System
DCS-11	Unauthorized Access Response Training
DCS-12	Cabling Security
DCS-13	Environmental Systems
DCS-14	Secure Utilities
DCS-15	Equipment Location

Table 7 continued

Control ID	Information Security Control
Data Security and Privacy Lifecycle Management	
DSP-01	Security and Privacy Policy and Procedures
DSP-02	Secure Disposal
DSP-03	Data Inventory
DSP-04	Data Classification
DSP-05	Data Flow Documentation
DSP-06	Data Ownership and Stewardship
DSP-07	Data Protection by Design and Default
DSP-08	Data Privacy by Design and Default
DSP-09	Data Protection Impact Assessment
DSP-10	Sensitive Data Transfer
DSP-11	Personal Data Access, Reversal, Rectification and Deletion
DSP-12	Limitation of Purpose in Personal Data Processing
DSP-13	Personal Data Sub-processing
DSP-14	Disclosure of Data Sub-processors
DSP-15	Limitation of Production Data Use
DSP-16	Data Retention and Deletion
DSP-17	Sensitive Data Protection
DSP-18	Disclosure Notification
DSP-19	Data Location
Governance, Risk and Compliance	
GRC-01	Governance Program Policy and Procedures
GRC-02	Risk Management Program
GRC-03	Organizational Policy Reviews
GRC-04	Policy Exception Process

Table 7 continued

Control ID	Information Security Control
Governance, Risk and Compliance	
GRC-05	Information Security Program
GRC-06	Governance Responsibility Model
GRC-07	Information System Regulatory Mapping
GRC-08	Special Interest Groups
Human Resources	
HRS-01	Background Screening Policy and Procedures
HRS-02	Acceptable Use of Technology Policy and Procedures
HRS-03	Clean Desk Policy and Procedures
HRS-04	Remote and Home Working Policy and Procedures
HRS-05	Asset returns
HRS-06	Employment Termination
HRS-07	Employment Agreement Process
HRS-08	Employment Agreement Content
HRS-09	Personnel Roles and Responsibilities
HRS-10	Non-Disclosure Agreements
HRS-11	Security Awareness Training
HRS-12	Personal and Sensitive Data Awareness and Training
HRS-13	Compliance User Responsibility
Identity & Access Management	
IAM-01	Identity and Access Management Policy and Procedures
IAM-02	Strong Password Policy and Procedures
IAM-03	Identity Inventory
IAM-04	Separation of Duties
IAM-05	Least Privilege

Table 7 continued

Control ID	Information Security Control
Identity & Access Management	
IAM-06	User Access Provisioning
IAM-07	User Access Changes and Revocation
IAM-08	User Access Review
IAM-09	Segregation of Privileged Access Roles
IAM-10	Management of Privileged Access Roles
IAM-11	CSCs Approval for Agreed Privileged Access Roles
IAM-12	Safeguard Logs Integrity
IAM-13	Uniquely Identifiable Users
IAM-14	Strong Authentication
IAM-15	Passwords Management
IAM-16	Authorization Mechanisms
Interoperability & Portability	
IPY-01	Interoperability and Portability Policy and Procedures
IPY-02	Application Interface Availability
IPY-03	Secure Interoperability and Portability Management
IPY-04	Data Portability Contractual Obligations
Infrastructure & Virtualization Security	
IVS-01	Infrastructure and Virtualization Security Policy and Procedures
IVS-02	Capacity and Resource Planning
IVS-03	Network Security
IVS-04	OS Hardening and Base Controls
IVS-05	Production and Non-Production Environments
IVS-06	Segmentation and Segregation
IVS-07	Migration to Cloud Environments

Table 7 continued

Control ID	Information Security Control
Infrastructure & Virtualization Security	
IVS-08	Network Architecture Documentation
IVS-09	Network Defense
Logging and Monitoring	
LOG-01	Logging and Monitoring Policy and Procedures
LOG-02	Audit Logs Protection
LOG-03	Security Monitoring and Alerting
LOG-04	Audit Logs Access and Accountability
LOG-05	Audit Logs Monitoring and Response
LOG-06	Clock Synchronization
LOG-07	Logging Scope
LOG-08	Log Records
LOG-09	Log Protection
LOG-10	Encryption Monitoring and Reporting
LOG-11	Transaction/Activity Logging
LOG-12	Access Control Logs
LOG-13	Failures and Anomalies Reporting
Security Incident Management, E-Discovery, & Cloud Forensics	
SEF-01	Security Incident Management Policy and Procedures
SEF-02	Service Management Policy and Procedures
SEF-03	Incident Response Plans
SEF-04	Incident Response Testing
SEF-05	Incident Response Metrics
SEF-06	Event Triage Processes
SEF-07	Security Breach Notification

Table 7 continued

Control ID	Information Security Control
Security Incident Management, E-Discovery, & Cloud Forensics	
SEF-08	Points of Contact Maintenance
Supply Chain Management, Transparency, and Accountability	
STA-01	SSRM Policy and Procedures
STA-02	SSRM Supply Chain
STA-03	SSRM Guidance
STA-04	SSRM Control Ownership
STA-05	SSRM Documentation Review
STA-06	SSRM Control Implementation
STA-07	Supply Chain Inventory
STA-08	Supply Chain Risk Management
STA-09	Primary Service and Contractual Agreement
STA-10	Supply Chain Agreement Review
STA-11	Internal Compliance Testing
STA-12	Supply Chain Service Agreement Compliance
STA-13	Supply Chain Governance Review
STA-14	Supply Chain Data Security Assessment
Threat & Vulnerability Management	
TVM-01	Threat and Vulnerability Management Policy and Procedures
TVM-02	Malware Protection Policy and Procedures
TVM-03	Vulnerability Remediation Schedule
TVM-04	Detection Updates
TVM-05	External Library Vulnerabilities
TVM-06	Penetration Testing
TVM-07	Vulnerability Identification

Table 7 continued

Control ID	Information Security Control
Threat & Vulnerability Management	
TVM-08	Vulnerability Prioritization
TVM-09	Vulnerability Management Reporting
TVM-10	Vulnerability Management Metrics
Universal Endpoint Management	
UEM-01	Endpoint Devices Policy and Procedures
UEM-02	Application and Service Approval
UEM-03	Compatibility
UEM-04	Endpoint Inventory
UEM-05	Endpoint Management
UEM-06	Automatic Lock Screen
UEM-07	Operating Systems
UEM-08	Storage Encryption
UEM-09	Anti-Malware Detection and Prevention
UEM-10	Software Firewall
UEM-11	Data Loss Prevention
UEM-12	Remote Locate
UEM-13	Remote Wipe
UEM-14	Third-Party Endpoint Security Posture

>>>

Notes

1. PII is defined as is any piece of information that confirms an individual's identity. A person's PII can include their Address; National Insurance Number or Social Security Number; Driver's license; Financial information, including bank accounts; and Medical records. See: https://www.isms.online/iso-27002/control-5-34-privacy-and-protection-of-pii/.

2. "Federal Information Processing Standards Publication 199 (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems," US National institute of Standards and Technology, 2004. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.

3. Federal Information Processing Standards Publication 199 (FIPS 199).

4. FIPS 199.

5. FIPS 199.

6. See pages 36-38 in the Data Ecosystem Report for a detailed description of the UK classification model.

7. It is suggested to require both certifications as each contains some cloud security controls that do not exist in the other. A mapping of these controls can be found at: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

8. Typical ISO 27001 certification costs (itgovernanceusa.com); STAR Registry Submissions | CSA (cloudsecurityalliance.org).

9. The threshold for what constitutes an SME should be customizable to each country's context.

10. FedRAMP_Security_Controls_Baseline_Rev_5_Public_Comment_2021_12_20.xlsx (live.com).

11. FedRAMP's Revision 5 baseline security controls are in draft form as of September 13, 2022.

>>>

Annex. References

A list of document references from the **U.S. National Institute of Standards and Technology** (NIST), the **International Standards Organization** (ISO) / **International Electrotechnical Commission** (IEC), and the **Cloud Security Alliance** (CSA) are provided below.

Authority/Body	Document
NIST	SP 800-145 - The NIST Definition of Cloud Computing
NIST	SP 500-322 - Evaluation of Cloud Computing Services Based on NIST SP 800-145
ISO/IEC	17788 - Cloud Computing Overview and Vocabulary
ISO/IEC	27001 - Information Security Management
ISO/IEC	27002 - Information Security, Cybersecurity, and Privacy Protection — Information Security Controls
ISO/IEC	27017 - Code of Practice for Information Security Controls Based On ISO/IEC 27002 For Cloud Services
ISO/IEC	27018 - Code of Practice for Protection of Personally Identifiable Information (PII) In Public Clouds Acting as PII Processors
ISO/IEC	19086 – Cloud Computing Service Level Agreements (SLA) Framework
ISO/IEC	19941 – Cloud Computing Interoperability and Portability
CSA	CSA CCM - Cloud Controls Matrix

Supported by the GovTech Global Partnership - www.worldbank.org/govtech