حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

CSP Security Standard

TABLE OF CONTENTS

Introduction

The Cloud Service Provider (CSP) Security Standard produced by Dubai Electronic Security Center (DESC) sets out requirements and guidance for CSPs and those organizations using any cloud services. Compliance with this standard is mandatory for all CSPs wishing to offer cloud services for Dubai government and semi government entities.

Correlation with other Standards

The standard is based on the following nationally and internationally recognized standards:

- ISO/IEC 27001:2013
- ISO/IEC 27002: 2013
- ISO/IEC 27017:2015
- CSA Cloud Controls Matrix 3.0.1
- ISR:2017

This standard does not repeat any of the requirements and /or controls from the above standards it is based on, and instead only refined and new requirements and controls are cited. This approach is chosen simplify the certification process, as existing certifications against ISO/IEC 27001 (with or without ISO/IEC 27017) and CSA Level 2 Star can be used.

This standard is a sector-specific ISO/IEC 27001 application and uses the control structure of ISO/IEC 27002; it is also makes use of the concepts in ISO/IEC 27009.

ISO/IEC 27017 is only cited if there are sector-specific additions to ISO/IEC 27002

CSA Cloud Controls Matrix 3.0.1 is only cited if there is a control directly corresponding to ISO/IEC 27002. Each CSA Cloud Controls Matrix 3.0.1 is only cited once to support easy implementation.

The CSA Control Matrix 3.0.1 controls that do not correspond to any of the controls in ISO/IEC 27002 are contained in Section 19 of this standard.

In this standard, ISR:2017 is used to ensure compliance within the legal jurisdiction and geographical boundaries of the United Arab Emirates, only the three controls related to this requirement are part of this standard. In addition, it is important for CSPs to be able to provide their services under any circumstances; this requirement yields the need for a disaster recovery site, as also stated in ISR.

Cloud service specific controls are denoted by the prefix CLD in front of the control number.

Please note that this standard deviates from the CSA Cloud Controls Matrix 3.0.1 in the assignment of controls being recommended for the CSP customers. In this standard all relevant controls from ISO/IEC 27002 and ISO/IEC 27017 are considered to be recommended for CSP customers.

Similar approaches using existing control sets and international standards have been taken by:

> **CS Mark Japan**
> Security standard for CSPs in Japan, based on ISO/IEC 27002 and ISO/IEC 27017. The CS Mark provides a common standard that addresses the CSP customers' security concerns and objective criteria for the customer (governments and organizations) can use to select a CSP.

> **The Multi-Tier Cloud Security (MTCS) Singapore Standard**
> The Singapore Standard is the world's first cloud security standard providing risk management practices and security specifications for multi-tiered cloud computing, which was developed under the Information Technology Standards Committee (ITSC) for Cloud Service Providers (CSP). The MTCS is designed for CSPs to strengthen and show the cloud security controls they have in place as well as to help cloud users, auditors and certifiers understand the necessary cloud security requirements.

> **FedRAMP Security Assessment Framework in the United States**
> A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP standardizes how Federal Information Security Management Act (FISMA) applies to cloud computing services and is based on NIST special publication 800-37/800-53. CSPs interested in having the US Government as a consumer must meet the FedRAMP security requirements and implement FedRAMP baseline security controls, which is verified by following the FedRAMP Security Assessment Framework.

1 SCOPE

This CSP Security Standard contains mandatory requirements and controls for information security of Cloud Service Providers (CSPs) offering their service to government and semi government entities in Dubai. This standard also provides guidance for customers of these CSPs.

Any requirements from ISO/IEC 27001 that apply unchanged will not be included in this standard; only additional or refined requirements will be included. The titles of the controls from ISO/IEC 27002, ISO/IEC 27017, CSA Cloud Controls Matrix 3.0.1 and ISR:2017 are cited to ensure that a complete statement of applicability can be produced.

This standard is applicable to all CSPs offering cloud services in Dubai, and can also be used by any customers of these services. Government and semi government organizations in Dubai shall ensure that any CSP they are using comply with this standard.

2 NORMATIVE REFERENCES

Recommendation ITU-T Y.3500 | ISO/IEC 17788, Information technology – Cloud computing – Overview and vocabulary

Recommendation ITU-T Y.3502 | ISO/IEC 17789, Information technology – Cloud computing – Reference architecture

ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

CSA Cloud Controls Matrix 3.0.1

Information Security Regulations: 2017

3 CLOUD COMPUTING

Cloud Computing is a form of information and communication technology sourcing and delivery model that enables convenient, on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released.

3.1 Cloud Computing Service Models

IaaS

Infrastructure as a Service is where the CSP provides processing, storage, networks and other fundamental computing resources to the customer. The underlying cloud infrastructure is managed and delivered by the provider but the customer has control over the deployed systems and applications.

PaaS

Platform as a Service allows the consumer to deploy their own (consumer-created or acquired) applications onto the cloud infrastructure. The programming languages, frameworks, libraries, services and tools used to create the applications are provided by the CSP. Similar to IaaS, the underlying cloud infrastructure is managed and delivered by the providers but the consumer has control over the deployed applications.

SaaS

Software as a Service provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a client interface or a program interface. The CSP manages the cloud infrastructure and platform, including applications, network, servers, operating systems and storage where the consumer is only using the service.

3.2 Cloud Computing Risks

Cloud computing is accompanied by various risks and, as an emerging technology, these risks continue to develop and evolve, thereby necessitating the development of appropriate security standards. Every aspect of cloud computing brings risks that, if not properly addressed, can cause significant damage to an organization. These might include:

- Unauthorized access to data
- System unavailability
- System vulnerabilities
- Account hijacking
- Data loss
- Denial of service

- Vulnerabilities introduced by shared technology

4 CLOUD SECURITY REQUIREMENTS

ISO/IEC 27001:2013 requirement 6.1.3 c) is refined as follows:

Compare the controls determined in 6.1.3 b) above with those in Clauses 5 – 19 of this standard to verify that no necessary controls have been omitted.

ISO/IEC 27001:2013 requirement 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

- the necessary controls (see ISO/IEC 27001:2013, 6.1.3 b) and c)),
- justification for their inclusion,
- whether the necessary controls are implemented or not, and
- justification for excluding any of the controls in Clauses 5 – 18 of this standard.

All other requirements from ISO/IEC 27001:2013 apply unchanged. In addition, the controls GRM-02, GRM-04, GRM-05, GRM-08, GRM-10, GRM-11 and IAM-07 from CSA Cloud Controls Matrix 3.0.1 shall be applied. Furthermore, the following controls from ISR:2017 apply to ensure compliance with the legal jurisdiction and geographical boundaries of the United Arab Emirates: ISR:2017 2.1.2, ISR:2017 7.4.2.4 and ISR:2017 13.2.1.1.1. To ensure continuity of services under any circumstances, a disaster recovery site shall be in place, as stated in ISR Main Control – 7.3 Disaster Recovery.

All CSPs offering services in Dubai shall comply with these requirements. It is recommended that customers of CSPs are also complying with ISO/IEC 27001 and/or ISR. Controls that apply only to CSPs are explicitly stated.

All controls in Clauses 5–19 apply to the Cloud Service Delivery Models SaaS, PaaS and IaaS, unless otherwise stated.

5 INFORMATION SECURITY POLICIES

5.1 Management direction for information security

The objective specified in ISO/IEC 27002, 5.1 applies.

5.1.1 POLICIES FOR INFORMATION SECURITY

The control, implementation guidance and other information provided in ISO/IEC 27002, 5.1.1 and ISO/IEC 27017, 5.1.1 apply. In addition, the control GRM-06 from CSA Cloud Controls Matrix 3.0.1 applies.

5.1.2 REVIEW OF THE POLICIES FOR INFORMATION SECURITY

The control, implementation guidance and other information provided in ISO/IEC 27002, 5.1.2 apply. In addition, the control GRM-09 from CSA Cloud Controls Matrix 3.0.1 applies.

6 ORGANIZATION OF INFORMATION SECURITY

6.1 Internal organization

The objective specified in ISO/IEC 27002, 6.1 applies.

6.1.1 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 6.1.1 and ISO/IEC 27017, 6.1.1 apply. In addition, the control HRS-07 from CSA Cloud Controls Matrix 3.0.1 applies.

6.1.2 SEGREGATION OF DUTIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 6.1.2 apply. In addition, the control IAM-05 from CSA Cloud Controls Matrix 3.0.1 applies.

6.1.3 CONTACT WITH AUTHORITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 6.1.3 and ISO/IEC 27017, 6.1.3 apply. In addition, the control SEF-01 from CSA Cloud Controls Matrix 3.0.1 applies.

6.1.4 CONTACT WITH SPECIAL INTEREST GROUPS

The control, implementation guidance and other information provided in ISO/IEC 27002, 6.1.4 apply.

6.1.5 INFORMATION SECURITY IN PROJECT MANAGEMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 6.1.5 apply.

6.2 Mobile devices and teleworking

The objective specified in ISO/IEC 27002, 6.2 applies.

6.2.1 MOBILE DEVICES POLICY

The control, implementation guidance and other information provided in ISO/IEC 27002, 6.2.1 apply. In addition, the controls HRS-05 and MOS-01 from CSA Cloud Controls Matrix 3.0.1 apply.

6.2.2 TELEWORKING

The control, implementation guidance and other information provided in ISO/IEC 27002, 6.2.2 apply.

6.3 CLD Relationship between cloud service customer and cloud service provider

The objective specified in ISO/IEC 27017, Annex A, CLD 6.3 applies.

6.3.1 **CLD** SHARED ROLES AND RESPONSIBILITIES WITHIN A CLOUD COMPUTING ENVIRONMENT

The control, implementation guidance and other information provided in ISO/IEC 27017, Annex A, CLD 6.3.1 apply.

7 HUMAN RESOURCES SECURITY

7.1 Prior to employment

The objective specified in ISO/IEC 27002, 7.1 applies.

7.1.1 SCREENING

The control, implementation guidance and other information provided in ISO/IEC 27002, 7.1.1 apply. In addition, the control HRS-02 from CSA Cloud Controls Matrix 3.0.1 applies.

7.1.2 7.1.2 TERMS AND CONDITIONS OF EMPLOYMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 7.1.2 apply. In addition, the control HRS-03 from CSA Cloud Controls Matrix 3.0.1 applies.

7.2 During employment

The objective specified in ISO/IEC 27002, 7.2 applies.

7.2.1 MANAGEMENT RESPONSIBILITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 7.2.1 apply. In addition, the control GRM-03 from CSA Cloud Controls Matrix 3.0.1 applies.

7.2.2 INFORMATION SECURITY AWARENESS, EDUCATION, AND TRAINING

The control, implementation guidance and other information provided in ISO/IEC 27002, 7.2.2 and ISO/IEC 27017, 7.2.2 apply. In addition, the controls HRS-9 and HRS-10 from CSA Cloud Controls Matrix 3.0.1 apply.

7.2.3 DISCIPLINARY PROCESS

The control, implementation guidance and other information provided in ISO/IEC 27002, 7.2.3 apply. In addition, the control GRM-07 from CSA Cloud Controls Matrix 3.0.1 applies.

7.3 Termination of employment

The objective specified in ISO/IEC 27002, 7.3 applies.

7.3.1 TERMINATION OR CHANGE OF EMPLOYMENT RESPONSIBILITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 7.3.1 apply. In addition, the control HRS-04 from CSA Cloud Controls Matrix 3.0.1 apply.

8 ASSET MANAGEMENT

8.1 Responsibility for assets

The objective specified in ISO/IEC 27002, 8.1 applies.

8.1.1 INVENTORY OF ASSETS

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.1.1 and ISO/IEC 27017, 8.1.1 apply. In addition, the control DSI-02 from CSA Cloud Controls Matrix 3.0.1 applies.

8.1.2 OWNERSHIP OF ASSETS

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.1.2 and ISO/IEC 27017, 8.1.2 apply. In addition, the control DSI-06 from CSA Cloud Controls Matrix 3.0.1 applies.

8.1.3 ACCEPTABLE USE OF ASSETS

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.1.3 apply. In addition, the control HRS-08 from CSA Cloud Controls Matrix 3.0.1 applies.

8.1.4 RETURN OF ASSETS

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.1.4 apply.

8.1.5 **CLD** REMOVAL OF CLOUD SERVICE CUSTOMER ASSETS

The control, implementation guidance and other information provided in ISO/IEC 27017, Annex A, CLD 8.1.5 apply.

8.2 Information classification

The objective specified in ISO/IEC 27002, 8.2 applies.

8.2.1 CLASSIFICATION OF INFORMATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.2.1 apply. In addition, the control DSI-01 from CSA Cloud Controls Matrix 3.0.1 applies.

8.2.2 LABELLING OF INFORMATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.2.2 and ISO/IEC 27017, 8.2.2 apply. In addition, the control DSI-04 from CSA Cloud Controls Matrix 3.0.1 applies.

8.2.3 HANDLING OF ASSETS

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.2.3 apply.

8.3 Media Handling

The objective specified in ISO/IEC 27002, 8.3 applies.

8.3.1 MANAGEMENT OF REMOVABLE MEDIA

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.3.1 apply. In addition, the control DSI-04 from CSA Cloud Controls Matrix 3.0.1 applies.

8.3.2 DISPOSAL OF MEDIA

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.3.2 apply. In addition, the control DSI-07 from CSA Cloud Controls Matrix 3.0.1 applies.

8.3.3 PHYSICAL MEDIA TRANSFER

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.3.3 apply.

9 ACCESS CONTROL

9.1 Business requirements of access control

The objective specified in ISO/IEC 27002, 9.1 applies.

9.1.1 ACCESS CONTROL POLICY

The control, implementation guidance and other information provided in ISO/IEC 27002, 8.3.3 apply. In addition, the control IAM-02 from CSA Cloud Controls Matrix 3.0.1 applies.

9.1.2 ACCESS TO NETWORKS AND NETWORK SERVICES

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.1.2 and ISO/IEC 27017, 9.1.2 apply. In addition, the controls IAM-09, DCS-03 and IVS-13 from CSA Cloud Controls Matrix 3.0.1 apply.

9.1.3 **CLD** CUSTOMER ACCESS

Control AIS-02 from CSA Cloud Controls Matrix 3.0.1 applies.

9.2 User access management

The objective specified in ISO/IEC 27002, 9.2 applies.

9.2.1 USER REGISTRATION AND DE-REGISTRATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.2.1 and ISO/IEC 27017, 9.2.1 apply. In addition, the control IAM-09 and IAM-11 from CSA Cloud Controls Matrix 3.0.1 apply.

9.2.2 USER ACCESS PROVISIONING

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.2.2 and ISO/IEC 27017, 9.2.2 apply. In addition, the control IAM-12 from CSA Cloud Controls Matrix 3.0.1 applies.

9.2.3 MANAGEMENT OF PRIVILEGED ACCESS RIGHTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.2.3 and ISO/IEC 27017, 9.2.3 apply.

9.2.4 MANAGEMENT OF SECRET AUTHENTICATION INFORMATION OF USERS

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.2.4 and ISO/IEC 27017, 9.2.4 apply. In addition, the control IAM-04 from CSA Cloud Controls Matrix 3.0.1 applies.

9.2.5 REVIEW OF USER ACCESS RIGHTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.2.5 apply. In addition, the control IAM-10 from CSA Cloud Controls Matrix 3.0.1 applies.

9.2.6 REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.2.6 apply.

9.3 User responsibilities

The objective specified in ISO/IEC 27002, 9.3 applies.

9.3.1 USE OF SECRET AUTHENTICATION INFORMATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.3.1 apply. In addition, the control IAM-08 from CSA Cloud Controls Matrix 3.0.1 applies.

9.4 System and application access control

The objective specified in ISO/IEC 27002, 9.4 applies.

9.4.1 INFORMATION ACCESS RESTRICTION

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.4.1 and ISO/IEC 27017, 9.4.1 apply. In addition, the control IVS-09 from CSA Cloud Controls Matrix 3.0.1 applies.

9.4.2 SECURE LOG-ON PROCEDURES

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.4.2 apply.

9.4.3 PASSWORD MANAGEMENT SYSTEM

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.4.3 apply. In addition, the control MOS-16 from CSA Cloud Controls Matrix 3.0.1 applies.

9.4.4 USE OF PRIVILEGED UTILITY PROGRAMS

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.4.4 and ISO/IEC 27017, 9.4.4 apply. In addition, the control IAM-13 from CSA Cloud Controls Matrix 3.0.1 applies.

9.4.5 ACCESS CONTROL TO PROGRAM SOURCE CODE

The control, implementation guidance and other information provided in ISO/IEC 27002, 9.4.5 apply. In addition, the control IAM-06 from CSA Cloud Controls Matrix 3.0.1 applies.

9.4.6 **CLD** ACCESS TO DIAGNOSTIC AND CONFIGURATION PORTS

Control IAM-03 from CSA Cloud Controls Matrix 3.0.1 applies.

9.5 CLD Access control of cloud service customer data in shared virtual environment

The objective specified in ISO/IEC 27017, Annex A, CLD 9.5 applies.

9.5.1 **CLD** SEGREGATION IN VIRTUAL COMPUTING ENVIRONMENTS

The control, implementation guidance and other information provided in ISO/IEC 27017, Annex A, CLD 9.5.1 apply. This control is applicable to CSPs only.

9.5.2 **CLD** VIRTUAL MACHINE HARDENING

The control, implementation guidance and other information provided in ISO/IEC 27017, Annex A, CLD 9.5.2 apply. In addition, the controls IVS-02and IVS-07 from CSA Cloud Controls Matrix 3.0.1 apply.

This control is applicable to CSPs only, and also only applies for IaaS.

9.5.3 **CLD** SECURE MIGRATION

Control IVS-10 from CSA Cloud Controls Matrix 3.0.1 applies.
This control is applicable to CSPs only.

9.5.4 **CLD** ACCESS TO HYPERVISOR MANAGEMENT FUNCTIONS

Control IVS-11 from CSA Cloud Controls Matrix 3.0.1 applies.
This control is applicable to CSPs only.

10 CRYPTOGRAPHY

10.1 Cryptographic controls

The objective specified in ISO/IEC 27002, 10.1 applies.

10.1.1 POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

The control, implementation guidance and other information provided in ISO/IEC 27002, 10.1.1 and ISO/IEC 27017, 10.1.1 apply. In addition, the controls EKM-03 and EKM-04 from CSA Cloud Controls Matrix 3.0.1 apply.

10.1.2 POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

The control, implementation guidance and other information provided in ISO/IEC 27002, 10.1.2 and ISO/IEC 27017, 10.1.2 apply. In addition, the controls EKM-01 and EKM-02 from CSA Cloud Controls Matrix 3.0.1 apply.

11 PHYSICAL AND ENVIRONMENTAL SECURITY

11.1 Secure Areas

The objective specified in ISO/IEC 27002, 11.1 applies.

11.1.1 PHYSICAL SECURITY PERIMETER

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.1.1 apply. In addition, the control DCS-02 from CSA Cloud Controls Matrix 3.0.1 applies.

11.1.2 PHYSICAL ENTRY CONTROLS

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.1.2 apply. In addition, the control DCS-02 from CSA Cloud Controls Matrix 3.0.1 applies.

11.1.3 SECURING OFFICES, ROOMS, AND FACILITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.1.3 apply. In addition, the control DCS-06 from CSA Cloud Controls Matrix 3.0.1 applies.

11.1.4 PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.1.4 apply. In addition, the controls BCR-05 and BCR-08 from CSA Cloud Controls Matrix 3.0.1 apply.

11.1.5 WORKING IN SECURE AREAS

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.1.5 apply. In addition, the controls DCS-07 and DCS-09 from CSA Cloud Controls Matrix 3.0.1 apply.

11.1.6 PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.1.6 apply. In addition, the control DCS-08 from CSA Cloud Controls Matrix 3.0.1 applies.

11.2 Equipment

The objective specified in ISO/IEC 27002, 11.2 applies.

11.2.1 EQUIPMENT SITING AND PROTECTION

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.1 apply. In addition, the control BCR-06 from CSA Cloud Controls Matrix 3.0.1 applies.

11.2.2 SUPPORTING UTILITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.2 apply. In addition, the control BCR-03 from CSA Cloud Controls Matrix 3.0.1 applies.

11.2.3 CABLING SECURITY

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.3 apply.

11.2.4 EQUIPMENT MAINTENANCE

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.4 apply. In addition, the control BCR-07 from CSA Cloud Controls Matrix 3.0.1 applies.

11.2.5 REMOVAL OF ASSETS

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.5 apply.

11.2.6 SECURITY OF EQUIPMENT AND ASSETS OFF-PREMISES

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.6 apply. In addition, the control DCS-04 from CSA Cloud Controls Matrix 3.0.1 applies.

11.2.7 SECURE DISPOSAL OR REUSE OF EQUIPMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.7 and ISO/IEC 27017, 11.2.7 apply. In addition, the control DCS-05 from CSA Cloud Controls Matrix 3.0.1 applies.

11.2.8 UNATTENDED USER EQUIPMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.8 apply. In addition, the control HRS-11 from CSA Cloud Controls Matrix 3.0.1 applies.

11.2.9 CLEAR DESK AND CLEAR SCREEN POLICY

The control, implementation guidance and other information provided in ISO/IEC 27002, 11.2.9 apply. In addition, the control HRS-11 from CSA Cloud Controls Matrix 3.0.1 applies.

12 OPERATIONS SECURITY

12.1 Operational procedures and responsibilities

The objective specified in ISO/IEC 27002, 12.1 applies.

12.1.1 DOCUMENTED OPERATING PROCEDURES

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.1.1 apply. In addition, the control BCR-04 from CSA Cloud Controls Matrix 3.0.1 applies.

12.1.2 CHANGE MANAGEMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.1.2 and ISO/IEC 27017, 12.1.2 apply.

12.1.3 CAPACITY MANAGEMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.1.3 and ISO/IEC 27017, 12.1.3 apply. In addition, the control IVS-04 from CSA Cloud Controls Matrix 3.0.1 applies.

12.1.4 SEPARATION OF DEVELOPMENT, TESTING, AND OPERATIONAL ENVIRONMENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.1.4 apply. In addition, the control IVS-08 from CSA Cloud Controls Matrix 3.0.1 applies.

12.1.5 **CLD** ADMINISTRATOR'S OPERATIONAL SECURITY

The control, implementation guidance and other information provided in ISO/IEC 27017, Annex A, CLD 12.1.5 apply.

12.2 Protection from Malware

The objective specified in ISO/IEC 27002, 12.2 applies.

12.2.1 CONTROLS AGAINST MALWARE

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.2.1 apply. In addition, the controls TVM-01 and TVM-03 from CSA Cloud Controls Matrix 3.0.1 apply.

12.3 Back-up

The objective specified in ISO/IEC 27002, 12.3 applies.

12.3.1 INFORMATION BACK-UP

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.3.1 and ISO/IEC 27017, 12.3.1 apply. In addition, the control BCR-11 from CSA Cloud Controls Matrix 3.0.1 applies.

12.4 Logging and monitoring

The objective specified in ISO/IEC 27002, 12.4 applies.

12.4.1 EVENT LOGGING

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.4.1 and ISO/IEC 27017, 12.4.1 apply.

12.4.2 PROTECTION OF LOG INFORMATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.4.2 apply. In addition, the control IVS-01 from CSA Cloud Controls Matrix 3.0.1 applies.

12.4.3 ADMINISTRATOR AND OPERATOR LOGS

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.4.3 and ISO/IEC 27017, 12.4.3 apply.

12.4.4 CLOCK SYNCHRONIZATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.4.4 and ISO/IEC 27017, 12.4.4 apply. In addition, the control IVS-03 from CSA Cloud Controls Matrix 3.0.1 applies.

12.4.5 **CLD** MONITORING OF CLOUD SERVICES

The control, implementation guidance and other information provided in ISO/IEC 27017, Annex A, CLD 12.4.5 apply.

This control is applicable to CSPs only.

12.5 Control of operational software

The objective specified in ISO/IEC 27002, 12.5 applies.

12.5.1 INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.5.1 apply. In addition, the control CCC-04 from CSA Cloud Controls Matrix 3.0.1 applies.

12.6 Technical vulnerability management

The objective specified in ISO/IEC 27002, 12.6 applies.

12.6.1 MANAGEMENT OF TECHNICAL VULNERABILITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.6.1 and ISO/IEC 27017, 12.6.1 apply. In addition, the control TVM-02 and IVS-05 from CSA Cloud Controls Matrix 3.0.1 apply.

12.6.2 RESTRICTIONS ON SOFTWARE INSTALLATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.6.2 apply.

12.7 Information systems audit considerations

The objective specified in ISO/IEC 27002, 12.7 applies.

12.7.1 INFORMATION SYSTEMS AUDIT CONTROLS

The control, implementation guidance and other information provided in ISO/IEC 27002, 12.7.1 apply. In addition, the control IAM-01 from CSA Cloud Controls Matrix 3.0.1 applies.

13 COMMUNICATIONS SECURITY

13.1 Network security management

The objective specified in ISO/IEC 27002, 13.1 applies.

13.1.1 NETWORK CONTROLS

The control, implementation guidance and other information provided in ISO/IEC 27002, 13.1.1 apply. In addition, the control IVS-12 from CSA Cloud Controls Matrix 3.0.1 applies.

13.1.2 SECURITY OF NETWORK SERVICES

The control, implementation guidance and other information provided in ISO/IEC 27002, 13.1.2 apply. In addition, the control IVS-06 from CSA Cloud Controls Matrix 3.0.1 applies.

13.1.3 SEGREGATION IN NETWORKS

The control, implementation guidance and other information provided in ISO/IEC 27002, 13.1.3 and ISO/IEC 27017, 13.1.3 apply.

13.1.4 CLD ALIGNMENT OF SECURITY MANAGEMENT FOR VIRTUAL AND PHYSICAL NETWORKS

The control, implementation guidance and other information provided in ISO/IEC 27017, Annex A, CLD 13.1.4 apply.

13.2 Information transfer

The objective specified in ISO/IEC 27002, 13.2 applies.

13.2.1 INFORMATION TRANSFER POLICIES AND PROCEDURES

The control, implementation guidance and other information provided in ISO/IEC 27002, 13.2.1 apply. In addition, the control IPY-03 from CSA Cloud Controls Matrix 3.0.1 applies.

13.2.2 AGREEMENTS ON INFORMATION TRANSFER

The control, implementation guidance and other information provided in ISO/IEC 27002, 13.2.2 apply.

13.2.3 ELECTRONIC MESSAGING

The control, implementation guidance and other information provided in ISO/IEC 27002, 13.2.3 apply.

13.2.4 CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 13.2.4 apply. In addition, the control HRS-06 from CSA Cloud Controls Matrix 3.0.1 applies.

14 SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE

14.1 Security requirements of information systems

The objective specified in ISO/IEC 27002, 14.1 applies.

14.1.1 INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.1.1 and ISO/IEC 27017, 14.1.1 apply. In addition, the control GRM-01 from CSA Cloud Controls Matrix 3.0.1 applies.

14.1.2 SECURING APPLICATIONS SERVICES ON PUBLIC NETWORKS

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.1.2 apply.

14.1.3 PROTECTING APPLICATION SERVICES TRANSACTIONS

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.1.3 apply. In addition, the control DSI-03 from CSA Cloud Controls Matrix 3.0.1 applies.

14.2 Security in development and support processes

The objective specified in ISO/IEC 27002, 14.2 applies.

14.2.1 SECURE DEVELOPMENT POLICY

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.1 and ISO/IEC 27017, 14.2.1 apply. In addition, the control AIS-01 from CSA Cloud Controls Matrix 3.0.1 applies.

14.2.2 SYSTEM CHANGE CONTROL PROCEDURES

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.2 apply. In addition, the controls CCC-03, CCC-05 and MOS-15 from CSA Cloud Controls Matrix 3.0.1 apply.

14.2.3 TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING PLATFORM CHANGES

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.3 apply.

14.2.4 RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.4 apply.

14.2.5 SECURE SYSTEM ENGINEERING PRINCIPLES

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.5 apply.

14.2.6 SECURE DEVELOPMENT ENVIRONMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.6 apply. In addition, the control CCC-01 from CSA Cloud Controls Matrix 3.0.1 applies.

14.2.7 OUTSOURCED DEVELOPMENT

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.7

14.2.8 SYSTEM SECURITY TESTING

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.8 apply.

14.2.9 SYSTEM ACCEPTANCE TESTING

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.2.9 and ISO/IEC 27017, 14.2.9 apply.

14.2.10 **CLD** INTEGRITY CONTROLS

Control AIS-03 from CSA Cloud Controls Matrix 3.0.1 applies.

14.2.11 **CLD** DATA SECURITY

Control AIS-04 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

14.3 Test data

The objective specified in ISO/IEC 27002, 14.3 applies.

14.3.1 PROTECTION OF TEST DATA

The control, implementation guidance and other information provided in ISO/IEC 27002, 14.3.1 apply. In addition, the control DSI-05 from CSA Cloud Controls Matrix 3.0.1 applies.

15 SUPPLIER RELATIONSHIPS

15.1 Information security in supplier relationships

The objective specified in ISO/IEC 27002, 15.1 applies.

15.1.1 INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS

The control, implementation guidance and other information provided in ISO/IEC 27002, 15.1.1 and ISO/IEC 27017, 15.1.1 apply. In addition, the control STA-07 from CSA Cloud Controls Matrix 3.0.1 applies.

15.1.2 ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 15.1.2 and ISO/IEC 27017, 15.1.2 apply. In addition, the control STA-05 from CSA Cloud Controls Matrix 3.0.1 applies.

15.1.3 INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN

The control, implementation guidance and other information provided in ISO/IEC 27002, 15.1.3 and ISO/IEC 27017, 15.1.3 apply. In addition, the controls STA-01, STA-06 and STA-08 from CSA Cloud Controls Matrix 3.0.1 apply.

This control is applicable to CSPs and the controls from ISO/IEC 27002 and ISO/IEC 27017 are recommended for CSP customers.

15.2 Supplier service delivery management

The objective specified in ISO/IEC 27002, 15.2 applies.

15.2.1 MONITORING AND REVIEW OF SUPPLIER SERVICES

The control, implementation guidance and other information provided in ISO/IEC 27002, 15.2.1 apply. In addition, the control STA-09 from CSA Cloud Controls Matrix 3.0.1 applies.

15.2.2 MANAGING CHANGES TO SUPPLIER SERVICES

The control, implementation guidance and other information provided in ISO/IEC 27002, 15.2.2 apply.

16 INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 Management of information security incidents and improvements

The objective specified in ISO/IEC 27002, 16.1 applies.

16.1.1 RESPONSIBILITIES AND PROCEDURES

The control, implementation guidance and other information provided in ISO/IEC 27002, 16.1.1 and ISO/IEC 27017, 16.1.1 apply. In addition, the control SEF-02 from CSA Cloud Controls Matrix 3.0.1 applies.

16.1.2 REPORTING INFORMATION SECURITY EVENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 16.1.2 and ISO/IEC 27017, 16.1.2 apply. In addition, the control SEF-03 from CSA Cloud Controls Matrix 3.0.1 applies.

16.1.3 REPORTING INFORMATION SECURITY WEAKNESSES

The control, implementation guidance and other information provided in ISO/IEC 27002, 16.1.3 apply.

16.1.4 ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 16.1.4 apply.

16.1.5 RESPONSE TO INFORMATION SECURITY INCIDENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 16.1.5 apply.

16.1.6 LEARNING FROM INFORMATION SECURITY INCIDENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 16.1.6 apply. In addition, the control SEF-05 from CSA Cloud Controls Matrix 3.0.1 applies.

16.1.7 COLLECTION OF EVIDENCE

The control, implementation guidance and other information provided in ISO/IEC 27002, 16.1.7 and ISO/IEC 27017, 16.1.7 apply. In addition, the control SEF-04 from CSA Cloud Controls Matrix 3.0.1 applies.

17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

17.1 Information security continuity

The objective specified in ISO/IEC 27002, 17.1 applies.

17.1.1 PLANNING INFORMATION SECURITY CONTINUITY

The control, implementation guidance and other information provided in ISO/IEC 27002, 17.1.1 apply. In addition, the control BCR-09 from CSA Cloud Controls Matrix 3.0.1 applies.

17.1.2 IMPLEMENTING INFORMATION SECURITY CONTINUITY

The control, implementation guidance and other information provided in ISO/IEC 27002, 17.1.2 apply. In addition, the control BCR-01 from CSA Cloud Controls Matrix 3.0.1 applies.

17.1.3 VERIFY, REVIEW, AND EVALUATE INFORMATION SECURITY CONTINUITY

The control, implementation guidance and other information provided in ISO/IEC 27002, 17.1.3 apply. In addition, the control BCR-02 from CSA Cloud Controls Matrix 3.0.1 applies.

17.2 Redundancies

The objective specified in ISO/IEC 27002, 17.2 applies.

17.2.1 AVAILABILITY OF INFORMATION PROCESSING FACILITIES

The control, implementation guidance and other information provided in ISO/IEC 27002, 17.2.1 apply.

18 COMPLIANCE

18.1 Compliance with legal and contractual requirements

The objective specified in ISO/IEC 27002, 18.1 applies.

18.1.1 IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL REQUIREMENTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.1.1 and ISO/IEC 27017, 18.1.1 apply. In addition, the control AAC-03 from CSA Cloud Controls Matrix 3.0.1 applies.

18.1.2 INTELLECTUAL PROPERTY RIGHTS

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.1.2 and ISO/IEC 27017, 18.1.2 apply.

18.1.3 PROTECTION OF RECORDS

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.1.3 and ISO/IEC 27017, 18.1.3 apply.

18.1.4 PRIVACY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.1.4 and ISO/IEC 27017, 18.1.4 apply.

18.1.5 REGULATION OF CRYPTOGRAPHIC CONTROLS

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.1.5 and ISO/IEC 27017, 18.1.5 apply.

18.2 Information security reviews

The objective specified in ISO/IEC 27002, 18.2 applies.

18.2.1 INDEPENDENT REVIEW OF INFORMATION SECURITY

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.2.1 and ISO/IEC 27017, 18.2.1 apply. In addition, the controls AAC-01 and AAC-02 from CSA Cloud Controls Matrix 3.0.1 apply.

18.2.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.2.2 apply. In addition, the control STA-04 from CSA Cloud Controls Matrix 3.0.1 applies.

18.2.3 TECHNICAL COMPLIANCE REVIEW

The control, implementation guidance and other information provided in ISO/IEC 27002, 18.2.3 apply.

19 CLD ADDITIONAL CONTROLS FROM CSA

19.1 CLD IT Service management

19.1.1 CLD IT GOVERNANCE AND SERVICE MANAGEMENT

Control BCR-10 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.2 CLD Controls for the provider

19.2.1 CLD SUPPORT FOR INTEROPERABILITY

Control IPY-01 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.2.2 CLD DATA PROVISION FOR CUSTOMERS

Control IPY-02 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.2.3 **CLD** SECURE NETWORK PROTOCOLS

Control IPY-04 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.2.4 **CLD** STANDARD VIRTUALIZATION PLATFORMS AND FORMATS

Control IPY-05 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.2.5 **CLD** AVAILABILITY OF SECURITY INCIDENT INFORMATION

Control STA-02 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.2.6 **CLD** SECURE CONFIGURATION

Control STA-03 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.2.7 **CLD** INTEGRITY OF VIRTUAL MACHINE IMAGE

Control IVS-02 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3 **CLD** Controls for the provider’s mobile devices and BYOD

19.3.1 **CLD** MOBILE DEVICES FOR PROVIDER DATA

Control MOS-02 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.2 **CLD** POLICY FOR APPLICATION INSTALLATION

Controls MOS-03 and MOS-04 from CSA Cloud Controls Matrix 3.0.1 apply.

This control is applicable to CSPs only.

19.3.3 **CLD** POLICY FOR THE PROVIDER’S MOBILE DEVICES

Control MOS-05 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.4 **CLD** CLOUD SERVICES FOR THE PROVIDER'S MOBILE DEVICES

Control MOS-06 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.5 **CLD** APPLICATION VALIDATION PROCESS

Control MOS-07 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.6 **CLD** BYOD POLICY

Controls MOS-08, MOS-13, MOS-17, and MOS-20 from CSA Cloud Controls Matrix 3.0.1 apply.

This control is applicable to CSPs only.

19.3.7 **CLD** INVENTORY OF MOBILE DEVICES

Control MOS-09 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.8 **CLD** MOBILE DEVICES MANAGEMENT SOLUTION

Control MOS-10 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.9 **CLD** ENCRYPTION FOR MOBILE DEVICES

Control MOS-11 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.10 **CLD** COMPLIANCE WITH SECURITY CONTROLS

Control MOS-12 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.11 **CLD** BYOD CONFIGURATION

Control MOS-14 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.12 **CLD** REMOTE WIPING OF BYOD DEVICES

Control MOS-18 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

19.3.13 **CLD** UPDATE OF MOBILE DEVICES

Control MOS-19 from CSA Cloud Controls Matrix 3.0.1 applies.

This control is applicable to CSPs only.

20 ORGANIZATIONS AND WORKS CONSULTED IN BRIEF

An extensive research was conducted on existing information security standards, regulations and frameworks in relation to cloud security during the course of drafting this standard. Pertinent information security documents were identified and consulted from the following organizations among others:

- ISO/IEC – International Standardization Organization / International Electrotechnical Commission
- CSA – Cloud Security Alliance
- ITU – International Telecommunication Union
- CSP certification solutions from different countries, such as Japan, Singapore and US
- Further various versions of several standards, regulations and frameworks related to cloud security were considered, including but not limited to:
- ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- Information Security Regulations: 2017
- CSA Cloud Controls Matrix 3.0.1
- Recommendation ITU-T Y.3500 | ISO/IEC 17788, Information technology – Cloud computing – Overview and vocabulary
- Recommendation ITU-T Y.3502 | ISO/IEC 17789, Information technology – Cloud computing – Reference architecture
- CS Mark Japan
- The Multi-Tier Cloud Security (MTCS) Singapore Standard
- FedRAMP Security Assessment Framework in the United States

ANNEX A

DEFINITIONS AND ABBREVIATIONS

A.1 Terms and Definitions

ACCESS CONTROL

Access control is a mechanism to enable authorized people to access entity resources (physical and logical) while preventing unauthorized people from doing the same.

ASSETS

Assets are economic resources. It is anything tangible or intangible that is capable of being owned or controlled to produce value and that is held to have positive economic value.

AUTHENTICATION

Authentication is the act of verifying a claim of identity. It is usually one or more of the following: something you know (password), something you have (identification card) or something you are (finger print).

AUTHORIZATION

Authorization is a mechanism that verifies that the authenticated subject can carry out the intended action.

AVAILABILITY

Part of the Information Security Triad; availability means that information should be available when it is needed.

BUSINESS CONTINUITY PLANNING (BCP)

Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an entity will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.

BRING YOUR OWN DEVICE (BYOD)

Bring your own device, (also called as bring your own technology (BYOT), bring your own phone (BYOP), and bring your own Personal Computer (BYOPC)—refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

CHANGE MANAGEMENT

Change management is a formal process for directing and controlling alterations to the information processing environment.

Note: Its objectives are to reduce the risks posed by changes to the information processing, environment and improve the stability and reliability of the processing environment as changes are made. The change management process ensures that a change is: Requested, Approved, Planned, Tested, Scheduled, Communicated, Implemented, Documented and Reviewed after the change.

CLASSIFICATION

Classification means assigning categories to assets on pre-set criteria. In Information security classification is used to categorize information assets in terms of sensitivity to protect it from unauthorized access, use, disclosure, disruption, modification or destruction.

CLOUD SECURITY

Refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Consists of all measures, practices and guidelines that must be implemented to enable a secure cloud architecture and to protect a cloud computing environment (SaaS, PaaS, IaaS etc.).

CLOUD SERVICE PROVIDER

An entity that provides cloud based platforms, infrastructure, application, and security or storage services for another entity/organization, usually for a fee.

COMPLIANCE

Compliance is the act of adhering to, and demonstrating adherence to, a standard or regulation (international or internal).

CONFIDENTIALITY

Part of the Information Security Triad; confidentiality means the nondisclosure of certain information assets except to an authorized person as per the classification level of that asset.

CONFIGURATION MANAGEMENT

Configuration management is an IT service management process that tracks all the individual configuration items (IT Assets) in an IT system with maybe be as simple as a single server or an entire IT department.

CRITICAL INFORMATION INFRASTRUCTURE (CII)

Assets, including organizations, which provide essential services that underpin the UAE’s society

Note: The Nation possesses numerous key resources, whose exploitation or destruction by any attacks could cause catastrophic effects, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction through attacks could have a debilitating effect on security and economic well-being.

CRYPTOGRAPHY

Cryptography is the concept consisting of two parts. The process of transforming usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption.

DUBAI GOVERNMENT ENTITIES/ENTITY

Any organization legally established by Dubai Government with well-defined roles and responsibilities, including but not limited to, authorities, departments, councils, committees, etc.

EVENT

Event is any observable occurrence in a system or network.

Note: Depending on their potential impact, some events need to be escalated for response.

EVIDENCE

Evidence is everything that is used to determine or demonstrate the truth of an intrusion or breach to an information system.

GOVERNANCE

Information Security governance is a subset of enterprise governance that provides strategic direction, ensures objectives are achieved, manages risk appropriately, uses entity resources responsibly, and monitors the success or failure of the enterprise security program / management system.

IDENTITY

Identity is a set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish the entity from any other entities.

IDENTITY AND ACCESS MANAGEMENT (IAM)

The the creation and management of identities for entities that may be granted logical or physical access to the organization's assets.

Note: Access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives, needs to be controlled.

INCIDENT

An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

INFORMATION

Depicts any government related information, which can exist in many forms, such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

INFORMATION SECURITY

The act of protecting information that may exist in any form, whether spoken, written, processed or transmitted electronically, etc. from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities.

INFORMATION SYSTEMS

Any computerized system used for managing and processing any government related information within a single entity or crossing multiple entities.

INFORMATION PROCESSING

Information processing entails any activity on the information including, but not limited to, creation, modification, deletion, storage, transmission, replication, encryption, decryption, etc.

INTEGRITY

Part of the Information Security Triad; integrity means that data cannot be modified without authorization, intentionally or unintentionally.

INVENTORY

Inventory is a list of goods and material owned by an entity – inventory recording could be in the form of an asset register.

LOGGING

Automated recordkeeping (by elements of an IT or OT) of system, network, or user activity.

Note: Logging may also refer to keeping a manual record (e.g., a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace.

MALICIOUS CODE

A code to infiltrate a computer system without the owner’s informed consent to make it unavailable, steal information or use it to attack other computers.

Note: This includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crime ware, rootkits, and other malicious or unwanted software.

MONITORING

Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.

MULTIFACTOR AUTHENTICATION

Concept of using two or more factors to achieve authentication.

Note: Factors include (i) something you know (e.g., password/PIN), (ii) something you have (e.g., cryptographic identification device, token), (iii) something you are (e.g., biometric), or (iv) somewhere you are (e.g., GPS token).

NETWORK ARCHITECTURE

Framework that describes the structure and behavior of communications among IT and/or OT assets and prescribes rules for interaction and interconnection.

PHYSICAL ACCESS CONTROL

Controls that monitor and control the environment of the work place and computing facilities.

Note: They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

RISK

Quantifiable likelihood of potential harm that may arise from a future event.

RISK ASSESSMENT

Step in the risk management process to determine the qualitative or quantitative value of risk in relation to a recognized threat.

Note: Quantitative risk assessment requires calculations of two components of risk; R, the magnitude of the potential loss L, and the probability p; that the loss will occur.

VULNERABILITY ASSESSMENT

Systematic examination of an IT or product to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation.

A.2 Abbreviations

BYOD: Bring Your Own Device

CSA: Cloud Security Alliance

CSP: Cloud Service Provider

CLD: Cloud service specific control

DESC: Dubai Electronic Security Center

FedRAMP: The Federal Risk and Authorization Management Program

IaaS: Infrastructure as a Service

ISO: International Organization of Standardization

ISR: Information Security Regulation

MTCS: Multi-Tier Cloud Security

NIST: National Institute of Standards and Technology

PaaS: Platform as a Service

SaaS: Software as a Service

DUBAI ELECTRONIC SECURITY CENTER

مركز دبي للأمن الإلكتروني