1 ATTACHMENT 3 - CUBE3 ASSESSMENT OF DATA CENTRE STANDARDS AND CERTIFICATIONS

There are a number of international standards applicable to the operation of cloud and computing services.

1.1 ISO 27001

ISO 27001 is the most common used security management certification outside of the United States. It consists of 133 controls and is applicable to the apparatus of the whole Information Security Management System.

In the Statement of Applicability (SOA), certified organizations can determine which controls are applicable to them.

ISO 27001 developed in 2013 and since revised has 14 major clauses:

A.5: Information security policies (2 controls)

A.6: Organization of information security (7 controls)

A.7: Human resource security - 6 controls that are applied before, during, or after employment

A.8: Asset management (10 controls)

A.9: Access control (14 controls)

A.10: Cryptography (2 controls)

A.11: Physical and environmental security (15 controls)

A.12: Operations security (14 controls)

A.13: Communications security (7 controls)

A.14: System acquisition, development and maintenance (13 controls)

A.15: Supplier relationships (5 controls)

A.16: Information security incident management (7 controls)

A.17: Information security aspects of business continuity management (4 controls)

A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

1.2 ISO/IEC 27002

ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organizations that adopt ISO/IEC 27002 must assess their own information risks, clarify their control objectives and apply suitable controls using the standard for guidance.

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS, but since ISO/IEC 27002 is merely a code of practice/guideline rather than a certification standard, organizations are free to select and implement other controls, or indeed adopt alternative complete suites of information security controls as they see fit. ISO/IEC 27001 incorporates a summary (little more than the section titles in fact) of controls from ISO/IEC 27002.

In practice, most organizations that adopt ISO/IEC 27001 also adopt ISO/IEC 27002.

1.3 ISO/IEC 27002

There is a new ISO standard for the cloud; ISO 27017. This is a code of practice for information security controls based on ISO/IEC 27002 for cloud services.

Used with the ISO/IEC 27001 series of standards, ISO/IEC 27017 provides enhanced controls for cloud service providers and cloud service customers. Unlike many other technology-related standards ISO/IEC 27017 clarifies both party's roles and responsibilities to help make cloud services as safe and secure as the rest of the data included in a certified information management system.

The standard provides cloud-based guidance on 37 of the controls in ISO/IEC 27002 but also features seven new cloud controls that address the following:

- Who is responsible for what between the cloud service provider and the cloud customer
- The removal/return of assets when a contract is terminated
- Protection and separation of the customer's virtual environment
- Virtual machine configuration
- Administrative operations and procedures associated with the cloud environment
- Cloud customer monitoring of activity within the cloud
- Virtual and cloud network environment alignment

1.4 CLOUD CONTROLS

ISO 27001 relates to data security. Other factors to think about when using cloud services include management of outsourcing. A layer of infrastructure purchased from a third party, requires that additional elements need to be covered such as preventing lock-in risks, or guaranteeing that information about the fulfilment of the service level agreement will be provided, for example. Another factor inherent in a public cloud is multitenancy. This relates to uncertainties when sharing an infrastructure with multiple customers.To manage outsourcing and multitenancy risks, CloudControls have been developed by KPMG and other companies. CloudControls consists of 44 controls which can be audited independently or as an appendix to ISO 27001. The overview below covers the different categories with examples.

Control Group	Control Sub Group	Short Control	Control
Multi-Tenancy	Multi-Tenancy	Isolation failure risk	Isolation failure risk in virtualization technology and storage is frequently reviewed and is managed to a minimum.
Outsourcing	Management Information and Control	Portability of services	Short term contracts are possible, customer virtual assets are exportable and transportable in an industry-accepted format. Sufficient access to the environment or data will be granted in order to implement migration.
Outsourcing	Legal Process	Data location and applicable jurisdictions	Customer can determine jurisdiction where data is stored. It should be communicated which governments and jurisdictions can lay claim to a customers' data.
Outsourcing	Privacy and Access to Data	Privacy policy	A privacy policy is developed, formally communicated and audited. Robust NDA clauses are added to the terms describing the confidentiality of all customer data.
Outsourcing	Infrastructure design	Informatie over resiliency management	Disaster recovery plans and availability enhancing measures should be shared with customers when relevant.
Outsourcing	Security Process	Customer vulnerability assessment	Cloud provider should provide the possibility for vulnerability assessment by customers.
Outsourcing	Operational Process	Information on degraded services	Outage reporting: If service was interrupted or degraded a detailed report will be provided on the reason and mitigation measures if relevant.
Outsourcing	Interfacing with the Service	Customer payment data	Sensitive customer data is encrypted. Measures are implemented to prevent storage and visibility of sensitive financial information.

1.5 PCI DSS

Payment Card Industry Data Security Standard (PCI DSS), which is required to handle secure card transactions.

1.6 SOC 1

The first of three new Service Organization Controls reports developed by the AICPA, this report measures the controls of a data center as relevant to financial reporting. It is essentially the same as a SSAE 16 audit.

1.7 SOC 2

This report and audit is completely different from the previous. SOC 2 measures controls specifically related to IT and data center service providers. The five controls are security, availability, processing integrity (ensuring system accuracy, completion and authorization), confidentiality and privacy. There are two types:

> Type 1 – A data center's system and suitability of its design of controls, as reported by the company.
>
> Type 2 – Includes everything in Type 1, with the addition of verification of an auditor's opinion on the operating effectiveness of the controls.

1.8 SOC 3

This report includes the auditor's opinion of SOC 2 components with an additional seal of approval to be used on websites and other documents. The report is less detailed and technical than a SOC 2 report.

1.9 EU-U.S. PRIVACY SHIELD

Privacy Shield replaces Safe Harbor as the new law maintaining the privacy and integrity of personal data. Different from HIPAA, PCI and SOX compliance requirements, Privacy Shield was developed by the U.S. Department of Commerce along with the European Commission on Data Protection.

1.10 UPTIME INSTITUTE

Conformance with the above standards will result in amongst other things high uptime as measured by the Uptime Institute. This has certified over 1000 leading data centre facilities worldwide for design, construction, management, and operations against the Tier Standards:

Tier I: Basic Capacity A Tier I data center provides dedicated site infrastructure to support information technology beyond an office setting. Tier I infrastructure includes a dedicated space for IT systems; an uninterruptible power supply (UPS) to filter power spikes, sags, and momentary outages; dedicated cooling equipment that won't get shut down at the end of normal office hours; and an engine generator to protect IT functions from extended power outages.

Tier II: Redundant Capacity Components Tier II facilities include redundant critical power and cooling components to provide select maintenance opportunities and an increased margin of safety against IT process disruptions that would result from site infrastructure equipment failures. The redundant components include power and cooling equipment such as UPS modules, chillers or pumps, and engine generators.

Tier III: Concurrently Maintainable A Tier III data center requires no shutdowns for equipment replacement and maintenance. A redundant delivery path for power and cooling is added to the redundant critical components of Tier II so that each and every component needed to support the IT processing environment can be shut down and maintained without impact on the IT operation.

Tier IV: Fault Tolerance Tier IV site infrastructure builds on Tier III, adding the concept of Fault Tolerance to the site infrastructure topology. Fault Tolerance means that when individual equipment failures or distribution path interruptions occur, the effects of the events are stopped short of the IT operations.