CSA Headed Paper

To:	ISO/IEC JTC 1/SC 27

Sobhi Mahmoud - SC 27 Committee Manager

Anna Badimo - SC 27/WG 4 Convenor Support

Liaison Statement to SC 27

Dear Sobhi,

The Cloud Security Alliance (CSA) wishes to thank ISO/IEC JTC 1/SC 27 for our on-going Category A liaison relationship and the opportunity to participate in the development of information security, cybersecurity and privacy protection standards.

CSA is particularly interested in the ongoing work of SC 27 in cybersecurity of cloud computing including information security and data protect management system standards as well as IoT and emerging technologies (e.g. AI and big data) standards.

CSA continues to follow and contribute to the development of standards in these areas across all of SC 27 working groups.

CSA would like to bring to SC 27's attention some recent highlights in the output of CSA's working groups,:

Publication in early 2021 of the 4th version of the CSA's Cloud Control Matrix, CCM v4. The Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing aligned to the CSA best practices.

Version 4 introduces changes in the structure of the framework with a new domain dedicated to log and monitoring (LOG) and a significant increase in requirements. Additional features are:

- ensured coverage of requirements deriving from new cloud technologies,
- new controls and security responsibility matrix,
- improved auditability of the controls and enhanced interoperability and compatibility.

The accompanying questionnaire, Consensus Assessments Initiative Questionnaire (CAIQ), provides a set of “yes or no” questions as well a new category that notes the security shared responsibility model (SSRM) based on the security controls in the CCM for Cloud Service Providers (CSPs) and can be used to perform a self- assessment of how well a CSP implements CSA's best practice.

Further CSA would like to inform SC 27 that the ISO/IEC 27000 series has been used in the further development of CSA STAR Certification Programme Level 3 for continuous auditing and monitoring of compliance by a cloud service provider. The development on STAR Level 3 has achieved a successful pilot and will now be moving to launch phase plans that will leverage the metrics catalogue.

CSA STAR Continuous:

- Requires STAR Level 2 to go to STAR Level 3
- Requires ISO/IEC 27001 as the ISMS framework

The “Level” concept represents a certification of a higher process. Higher strength of assurance at a higher level.

The above documents as well as all the other CSA research publications are available to download for free from the organization’s website.

We are also in process; in collaborating with CSA partners, of developing a “SMART” program which is essentalling machine readable standards. This will effectively allow organizations to evaluate compliance with a standard.

SMART enrichment is the process to transform static requirements into useable application (data that can be used).

1. Verify that the process/model reflects reality.
2. Verify that the process/model is implemented correctly. It shall satisfy all stated requirements.
3. Verifies that data (evidence) is correctly and accurately collected by the process
4. Verifies that the management system is effective.

CSA is looking forward to our continued collaboration and contributions to SC 27

DiMaria, John - **Main contact for CSA**

jdimaria@cloudsecurityalliance.org