ISO/IEC 27018 (ISO 27018): A Modern Approach to Cloud Security & Privacy

November 2014

Cloud computing in all its various forms is now the ideal model for a wide range of sectors (including government entities) in view of what it offers in terms of improved data security features, reduced operating costs, reliability, infrastructure, high levels of responsiveness to user needs in addition to its flexible financial model. Regardless of where the data is held (i.e. whether on site, within the jurisdiction, or elsewhere in the world), data security and privacy remains the biggest challenges in earning public confidence in cloud computing. For these reasons, many countries have taken steps to introduce rules and legislation to help secure the private data of their citizens. The International Organization for Standardization (ISO) has issued ISO 27018, the first-ever standard for cloud data protection. The key features of ISO 27018 are presented below.

The new standard, ISO 27018, will strengthen data privacy by adding key protections for sensitive customer information stored in the cloud. Published in July 2014 by the International Organization for Standardization, ISO 2708 sets forth guidelines for cloud service providers concerning Personally Identifiable Information ("PII"). The standard was developed in consultation with contributors from 14 countries and 5 international organizations.

Modernizing Security & Privacy in the Cloud

Before ISO 27018, there wasn't a robust, internationally-recognized benchmark for protecting cloud stored PII. The well-established ISO/IEC 27001:2005 standard provides a flexible system for identifying overall information security risks and choosing controls to address them. As an addendum to ISO 27001, ISO 27018 provides specificity to cloud service providers for assessment of risks and implementation of state-of-the-art controls for protection of PII stored in the cloud.

Key Elements of ISO 27018 and the Benefit to Customers

Cloud service providers adopting the new standard must operate under a stronger, industry-wide framework of key principles:

• **Consent**: As part of ISO 27018, cloud providers must not use the data they receive for purposes of their own advertising and marketing unless expressly instructed to do so by the customer. Moreover, it must be possible for a customer to use the service without submitting to such use of its personal data for advertising or marketing.

• **Transparency**: Cloud providers must inform customers where their data resides and make clear commitments about how that data is handled.

• **Accountability**: The standard asserts that any breach of information security should trigger a review by the service provider to determine if there was any loss, disclosure, or alteration of PII.

• **Communication**: In case of a breach, cloud providers should notify customers and regulators, and keep clear records about the incident and the response to it.

• **Independent Audit**: A successful third-party audit (from one of the big fours) of a cloud service's compliance with 27018 documents the service's conformance with the standard, and can then be relied

upon by the customer to support their own regulatory obligations.

• **Control**: Customers have explicit control of how their information is used.

Streamlined Standard

ISO 27018 standard creates a more streamlined system for adhering to regulations set by data protection authorities around the world. Since the standard incorporates the input of multiple regional regulators, embracing the standard will help demonstrate adherence to the requirements of any individual Data Protection Authority's requirements. The ISO 27018 standard brings a degree of uniformity to the industry, and adds needed protections to improve PII security and compliance in an increasingly cloud-based information environment.

Summary

ISO 27018 specifies guidelines based on other international standards (such as EU standards) for cloud data protection. This should enhance overall confidence in cloud computing adoption worldwide. ISO 27018 manages to address the numerous challenges of data protection in the cloud while achieving the intricate balance between a user's fundamental rights and the requirements to deliver services in a cloud computing model based on transparency (i.e. location of the data, methods of deletion as well as data sovereignty).

ISO 27018 is already generating positive feedback as some cloud service providers have already commenced the requisite steps for adopting these new standards and are expected to get certified very soon. We anticipate an increasing number of cloud service providers to follow in their footsteps.