

ISO/IEC JTC 1/SC 27
IT Security techniques
Secretariat: DIN (Germany)

Document type: Other document (Defined)

Title: WG4N0347 Report SP CloudSecTechStds

Status: As per resolution 19 (contained in SC 27 N13271) of the 15th SC 27/WG 4 plenary meeting, held 2013-10-21 to 2013-10-25, Incheon, Korea, this report on the study period is circulated within WG 4 for information.

It will be circulated in SC 27 as SC 27 N13281.

Secretariat's note:
This document is also concurrently being circulated as WG 4 document N0347 for test purposes ONLY as part of the WG 4 Livelink trial and is accessible at:
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

Date of document: 2013-11-29

Source: 15th ISO/IEC JTC 1/SC 27/WG 4 meeting

Expected action: INFO

No. of pages: 1+14

Email of secretary: krystyna.passia@din.de

Committee URL: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

ISO/IEC JTC 1/SC 27/WG 4
Security controls and services
Convenorship: SABS (South Africa)

Document type: Other document (Defined)

Title: Report SP Sec Cloud Tech Stds - Report on the 3rd study period in the area of Cloud security technology standards

Status: As per resolution 19 (contained in SC 27 N13271) of the 15th SC 27/WG 4 plenary meeting, held 2013-10-21 to 2013-10-25, Incheon, Korea, this report on the study period is circulated within WG 4 for information.

It will be circulated in SC 27 as SC 27 N13281.

Date of document: 2013-11-06

Source: 15th ISO/IEC JTC 1/SC 27/WG 4 meeting

Expected action: INFO

No. of pages: 1 + 13

Email of secretary:

Committee URL: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

Meeting Report: WG 4 Study Period on Cloud Security Technology Standards

In attendance: (see attached list for attendee names)

National Bodies: Japan, United States, Korea, Canada, Ireland, United Kingdom, Ireland

Liaison: CSA

Contributions Received: US, Japan (from previous meeting)

Japan Contribution Discussion:

- Koji Nakao presented a summary of the proposal
- Focus of the project would be on the assessment of the controls
- US has concerns about building a document on a standard that is not completely stable or complete yet. UK agreed with the underlying concern
- JP proposed that we extend the SP on this topic to allow potential example text as well as allow 27017 to stabilize.
- CA and KR also would like to see some examples to better understand what is being proposed.
- Consensus was to extend the SP for further input.

US Contribution Discussion:

- Said Tabet presented the US contribution on Cloud Adapted Risk Management Framework
- There seemed to be general consensus that this may prove to be an interesting topic of further study.
- MY verified that this would be complimentary to ISO/IEC 31000 and ISO/IEC 27005. Also suggested that Business continuity needs to be included
- It was noted that this could be a good companion to ITU x.1600
- It was noted that investigation with the revision of 27005 should be explored
- Consensus was that this should be included in the extended SP.

Recommendation

- Extend the SP for another 6 months
- Include the NWI (Assessment of the controls) for further study
- Include the Cloud Adapted Risk Management Framework for further study

ATTACHMENT ONE

Attendance

Koji Nakao	KDDI/Japan	ko-nakao@kddi.com
Maslina Daud	Malaysia	maslina@cybersecurity.my
Sal Francomacaro	ANSI/United States	salfra@nist.gov
Sanghoom Jeon	KAT/Korea	randyjeon@gmail.com
Kelly Friedman	SCC/Canada	kfriedman@davis.ca
John Hickey	NSAI/Ireland	john.hickey@alcatel-lucent.com
Ian Bryant	BSI/United Kingdom	ian.bryant@uk-tsi.org
Jongyoul Park	ETRI/Korea	jongyoul@etri.re.kr
Tadashi Nagamiya	JASA/Japan	nagamiya@jasa.jp
Haruo Murakami	Hitachi/Japan	haruo.murakami.te@hitachi.com
Colman Ho	Canada	colman.ho@ic.gc.ca
Said Tabet	United States	said.tabet@emc.com
Laura Lindsay	United States	laurali@microsoft.com
Eric Hibbard	Cloud Security Alliance	eric.hibbard@hds.com

ISO/IEC JTC 1/SC 27/WG 4
Cloud adapted Risk
Management Framework
(CRMF)
Study Period Topic Proposal

ISO Risk Management Standards

- ISO/IEC 31000:2009 – Risk management
 - Related Standards:
 - ISO Guide 73:2009, *Risk management - Vocabulary* complements ISO 31000 by providing a collection of terms and definitions relating to the management of risk
 - ISO/IEC 31010:2009, *Risk management – Risk assessment techniques* focuses on risk assessment
- ISO/IEC 27005:2011

Information technology -- Security techniques -- Information security risk management

Cloud Computing and Risk management

- Cloud computing roles have differing degrees of control over the computing and data processes
 - Implementation of security requirements becomes a shared responsibility among the cloud computing roles.
- Cloud computing roles involved in orchestrating cloud computing ecosystems and providing technical services are responsible for ensuring they address the cloud service customers' areas of concern

Traditional Risk Management Frameworks

- Traditional Risk Management framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.
- The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, policies, standards, or regulations.
- While the RMF is flexible and easily adaptable in most cases, it assumes a traditional IT environment, and requires some customization to address the unique characteristics of cloud-based services.

The CRMF Proposal

- An approach for a Cloud-adapted Risk Management Framework (CRMF) for a Cloud Computing Ecosystem
- CRMF defines a risk-assessment methodology for the analysis of the data collected and aggregated during the process of orchestrating a Cloud Computing Ecosystem.

Why CRMF?

- CRMF can be used to help organizations:
 - Identify security risks that are inherent with the cloud computing environments
 - Apply these risks in the selection of relevant security controls.

Cloud-specific security controls derived from a cloud based risk analysis will protect pre-migration data and identify post-migration security needs.

Applying CRMF

- Applying the CRMF on behalf of a cloud service customer and providing continuous monitoring is a responsibility shared among all cloud Actors.
- Cloud service providers should implement well-structured, cost-effective automation processes for continuous monitoring of security controls to
 - ensure their effectiveness and
 - provide near real-time measurements of security parameters in support of a risk-based decision process for organizational information systems operating in a cloud computing Ecosystem.

Proposed CRMF

We propose that CRMF be aligned with ISO27005 and ISO31000. The following is an example of steps that will need to be defined as part of the SP:

Categorize	Categorize migration to cloud computing environment
Identify	Identify security requirements fro migrated services
Select	Select architecture supporting the identified requirements
Assess	Assess cloud service providers and other roles
Authorize	Enable the cloud service providers through agreements
Monitor	Monitor the cloud service providers and other roles

Managing the Risk Inherent in Cloud Services

- Cloud service customers are responsible for information security risks incurred by the use of information system services offered by external suppliers, including cloud service providers.
- Cloud service customers:
 - can require cloud service providers to implement all steps in the CRMF process
 - should also require cloud service providers to present appropriate evidence that demonstrates their compliance with the CRMF.

Motivation for the proposed SP Topic

- Study the application of 27005 to Cloud and identify gaps.
- Propose a Risk Management Framework adapted to Cloud Computing (CRMF) as a potential new work item
- The CRMF will help identify security controls that address the specific characteristics of cloud computing environments
- The CRMF can be used to address the security risks associated with cloud computing systems by incorporating it into the terms and conditions of the contracts with external cloud service providers

Thank You!