Cloud
Standards
Customer
Council

Cloud Security Standards:
What to Expect & What to Negotiate

October, 2013

Contents

Acknowledgements

The major contributors to this whitepaper are: Chris Dotson (IBM), Mike Edwards (IBM), Ryan Kean (The Kroger Co.), Shamun Mahmud (DLT Solutions), John Meegan (IBM), Barry Pardee (Tailwind Associates), and Annie Sokol (NIST).

Executive Overview

The current landscape for information security standards specifically targeted for cloud computing environments is best characterized as immature but emerging. This space is still very much in its infancy stage but there are several standards initiatives that have recently been started that plan to deliver formal specifications in the 2014/2015 timeframe. In the interim, there is a number of *general* IT security standards that are applicable to cloud computing environments that customers should be aware of and insist that their cloud service providers support. When finalized, the cloud specific security standards will provide more detailed guidance and recommendations for both cloud service customers and cloud service providers.

This paper focuses primarily on information security requirements for public cloud deployment since this model introduces the most challenging information security concerns for cloud service customers. As cloud service customers assess the security standards support of their cloud service providers, it is important to understand and distinguish the different *types* of security standards that exist:

- *Advisory standards.* These standards are meant to be interpreted and applied to all types and sizes of organization according to the particular information security risks they face. In practice, this flexibility gives users a lot of latitude to adopt the information security controls that make sense to them, but makes it unsuitable for the relatively straightforward compliance testing implicit in most formal certification schemes.

- *Security frameworks*. Often referred to as best practices, these types of standards are suitable for certification. Security frameworks define specific policies, controls, checklists, and procedures along with processes for examining support that can be used by auditors to assess and measure a service provider's conformance.

- *Standards specifications*. These types of security standards specifically define APIs and communication protocols that must be implemented to claim support for the standard. In many cases, such standards allow for extensibility, permitting implementers to include functions that go beyond those defined in the standard. In general, formal certifications are not provided for these types of standards although compliance and interoperability test suites may be available.

Certification is an important aspect for cloud service customers to assess. Certification is often carried out by independent third-party auditors, although in some circumstances, self-certification by the provider is possible. For certification, it is typical that auditors examine the documented policies, procedures and designs of the provider and then subsequently examine the day-to-day operations of the provider to check that these follow the documentation.

Certification provides assurance to cloud service customers that their critical security requirements are being met. Therefore, it is recommended that cloud service customers identify the well-established security certifications that are important to their organizations and insist their cloud service providers demonstrate their conformance. Even though security certifications specific to cloud computing are still emerging, general security certifications that exist today are applicable to cloud computing and should be strongly considered.

Cloud Security Standards Guidance

As customers transition their applications and data to use cloud computing, it is critically important that the level of security provided in the cloud environment is equal to or better than the security provided by their traditional IT environment. Failure to ensure appropriate security protection could ultimately result in higher costs and potential loss of business thus eliminating any of the potential benefits of cloud computing. This paper focuses primarily on information security requirements for public cloud deployment since this model introduces the most challenging information security concerns for cloud service customers.

The CSCC "Security for Cloud Computing: 10 Steps to Ensure Success" white paper [1] prescribes a series of ten steps that cloud service customers should take to evaluate and manage the security of their cloud environment with the goal of mitigating risk and delivering an appropriate level of support. The following steps are discussed in detail:

1. Ensure effective governance, risk and compliance processes exist
2. Audit operational and business processes
3. Manage people, roles and identities
4. Ensure proper protection of data and information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks and connections are secure
8. Evaluate security controls on physical infrastructure and facilities
9. Manage security terms in the cloud SLA
10. Understand the security requirements of the exit process

This white paper uses the same list of ten steps as a straightforward way to complement and extend the original whitepaper. For each step, the corresponding subsection highlights the security standards and certifications that are currently available in the market as well as the cloud specific security standards that are currently being developed. Recommendations on which standards and certifications should be required of prospective cloud service providers are highlighted for each step.

Step 1: Ensure effective governance, risk and compliance processes exist

Standards to support the general governance of IT have existed for a number of years and they are in common use around the world. These governance standards are not specific to cloud computing, but they are sufficiently general so that they can be applied to the governance of cloud computing. Governance standards include:

- **ISO 38500 – IT Governance**[1]
  The ISO 38500 standard provides a framework for the governance of IT within an organization, offering guiding principles for the senior management of the organization for the effective, efficient and acceptable use of IT. It is not specific to cloud computing, but it can be used by both cloud service providers and cloud service customers.

- **COBIT**[2]
  COBIT was created by the ISACA organization and provides a framework for IT governance and IT management. It is positioned as a high level framework that sits between business goals and processes and the IT goals and processes. COBIT can be used in conjunction with more detailed standards such as ISO 20000 and ISO 27000.

- **ITIL**[3]
  ITIL (Information Technology Infrastructure Library) is a set of practices for IT service management, which can be applied to the management of cloud services. Information security management is covered, but it is typical to address this area using the ISO 27002 standard (see below).

- **ISO 20000**[4]
  The ISO 20000 series of standards is an international standard for IT service management – this series is well established and is recognized internationally. It is not specific to cloud computing and cloud services, but a new standard is being developed which addresses the application of ISO 20000 to cloud computing – this new standard is called ISO 20000-7. In addition, the ISO 20000-11 specification is under development, which describes the relationship of ISO 20000 to other frameworks and in particular, its relationship to ITIL.

- **SSAE 16**[5]
  SSAE 16 is an audit standard which applies to service organizations, which can be applied to

[1] Refer to http://www.38500.org/ for details.

[2] Refer to http://www.isaca.org/COBIT/Pages/default.aspx for details.

[3] Refer to http://www.itil-officialsite.com/ for details.

[4] Refer to http://en.wikipedia.org/wiki/ISO/IEC_20000 for details.

[5] Refer to http://ssae16.com/ for details.

cloud service providers. It is an updated and expanded version of the older SAS 70 standard. These standards focus on controls in place at the service provider organization and they are more oriented towards accountancy and financial activities.

In addition to the general standards and frameworks listed above, there are others which operate at country or regional levels or which apply to specific industries or to specific types of data. If your business operates in the relevant countries or in the relevant industry sector, these may apply. Some examples are listed below, but there are others and it is necessary to understand which may apply to your use of cloud services:

- **HIPAA**[6]
  A standard that relates to the handling of health related information, principally in the USA.

- **PCI-DSS**[7]
  A standard relating to the security of payment card data.

- **FedRAMP**[8]
  A U.S. government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- **FISMA**[9]
  A U.S. federal law which places information security requirements on federal agencies.

If IT governance by the cloud service provider is a significant concern for a cloud service customer, then cloud service customers are advised to establish if a cloud service provider complies with one or more of these governance and management standards. Of the standards listed here, one of COBIT, SSAE 16 or ITIL would be the most common to look for, depending on the type of workload(s) that the customer is considering placing into the cloud environment.

There are also some standards that deal specifically with governance and management of information security, including the identification of risks and the implementation of security controls to address these risks. The ***ISO/IEC 27000-series***[10] of standards is probably the most widely recognized and used set of standards relating to the security of ICT systems. The core standards are 27001 and 27002, with 27001 containing the requirements relating to an information security management system and 27002

[6] Refer to http://www.hhs.gov/ocr/privacy/ for details.

[7] Refer to https://www.pcisecuritystandards.org/security_standards/ for details.

[8] Refer to http://www.fedramp.gov for details.

[9] Refer to http://csrc.nist.gov/groups/SMA/fisma/index.htmlfor details.

[10] Refer to http://www.27000.org/ for details.

describing a series of controls that address specific aspects of the information security management system.

ISO 27001 is an advisory standard that is meant to be interpreted and applied to all types and sizes of organization according to the particular information security risks they face. In practice, this flexibility gives users a lot of latitude to adopt the detailed information security controls that make sense to them, but can make compliance testing more complex than some other formal certification schemes.

ISO 27002 is a collection of security controls (often referred to as best practices) that are often used as a security standard. Assuming that the design and/or operation of a cloud service provider's information security management systems are *consistent* with the standard (e.g., there are no notable gaps) it can be asserted that their environment is *compliant* with the standard.

The 27001 and 27002 standards apply generally to the operation of ICT systems. There are two new standards under development which describe the application of 27002 to cloud computing – these are ISO 27017 and ISO 27018. ISO 27017 deals with the application of the ISO 27002 specification to the use of cloud services and to the provision of cloud services. ISO 27018 deals with the application of 27002 to the handling of Personally Identifiable Information (PII) in cloud computing (sometimes described as dealing with privacy in cloud computing).

Currently, cloud service customers are advised to look for cloud service providers that conform to the ISO 27002 standard for information systems security. This is not specific to cloud computing, but its principles can still be usefully applied to the provision of cloud services. A cloud service provider can assert on its own behalf as to its compliance with a standard, but having an independent/qualified third party certify compliance is a notably stronger form of attestation. A number of cloud service providers already claim conformance to ISO 27002, many of them through third party certifications.

Once ISO 27017 and ISO 27018 are completed (currently expected in 2014), customers are advised to check if their cloud service provider conforms to these standards, since they are specific to cloud computing for information security and for the handling of PII, respectively.

Step 2: Audit operational & business processes

Cloud service customers must first check that the cloud service provider is open to third party audit – there should be appropriate terms relating to this in the service contract and/or service level agreement relating to cloud services. The auditors must be able to audit current controls and also access audit trails in the form of historic log data for the systems used to provide cloud services.

It is typical for audits to operate using the requirements of one of the common certification schemes or standards. For security controls, the ISO 27000 series is widely accepted (see step 1), and its maturity means that there are a range of certifications based on it – as an example, there is the Cybertrust certification, which is favored by some cloud service providers.

For cloud services which have a significant impact on the financial statements of service customers, the cloud service should meet the long-established SSAE 16 attestation standard.

In addition to external auditing, there are a number of on-going efforts focused on providing standard mechanisms for cloud service customers to self-manage and self-audit their applications and data running in the cloud. One such initiative is the DMTF Cloud Auditing Data Federation (CADF)[11] standard that supports the submission and retrieval of normative audit event data from cloud service providers in the form of customized reports and logs that can be dynamically generated for cloud service customers using their criteria. At this time, implementations of CADF are scare but support for this standard is planned for a future release of OpenStack.[12]

Step 3: Manage people, roles and identities

The essence of managing people, roles and identities is ensuring appropriate, controlled access to customer data and applications in the cloud computing environment. There are three groups of people to be concerned about – employees of the provider (including any subcontractors), people performing roles for the customer including service users and service administrators, and finally – everyone else!

For employees of the provider, it is typical to require the cloud service provider to have in place appropriate security controls to ensure that provider employees only have controlled and appropriate access to customer services and associated software and data. Information security management standards such as ISO 27002 describe the necessary controls for provider employees, so it is advisable for a cloud service customer to require that the provider is certified to one of these standards to provide assurance in this area.

Cloud service customers are also advised to treat sensitive data in such a way as to limit the risk exposure if a provider employee does gain inappropriate access – using the data protection measures described in step 4.

For people performing roles for the customer, in particular users and administrators of cloud services, it is necessary to have suitable Identity & Access Management (IAM) in place to ensure that a person must identify and authenticate themselves when using the cloud service and that they are granted access rights which are appropriate to their role. The cloud service customer should demand fine grained access control and a separation of roles between cloud service users and cloud service administrators. Given the additional powers that are typical for an administrator, it is also advisable to consider more stringent authentication techniques to be used for administrators as compared with cloud service users.

IAM security standards have been established before the emergence of cloud computing. For example, Kerberos was developed in the 1980s as an authentication protocol and is used in some cloud security IAM implementations today. Cloud computing customers should look for IAM capabilities that support:

- *Federated IDs.* The use of IDs that are held directly by the customer or by a trusted third party provider, so that the customer is not obliged to establish and administer an additional set of user identities in order to use each cloud service.

[11] Refer to http://www.dmtf.org/standards/cadf for more information.

[12] Refer to http://www.openstack.org/foundation/ for information on OpenStack.

- *Single sign-on*: Closely allied to federated IDs is the concept of users having a single ID and a single sign-on when using a set of different services, possibly spanning the customer's systems and multiple providers' cloud services

- *Privileged Identity Management*: The IDs of cloud service administrators are privileged in their capabilities and need special control. Common identity access management frameworks do not manage or control privileged identities and so specialized privileged identity management is needed. This key capability can be used as an information security and governance tool to help customers in meeting compliance requirements and to prevent data breaches through the use of privileged accounts.

A number of standards and technologies are available which provide federated IDs and single sign-on, including:

- **LDAP**[13]
  LDAP stands for Lightweight Directory Access Protocol and is an IETF standard widely used to provide access to directory servers, which includes authentication and authorization services.

- **SAML 2.0**[14]
  SAML stands for Security Authorization Markup Language and is an OASIS standard used for the exchange of authentication and authorization data between security domains.

- **OAuth 2.0**[15]
  OAuth 2.0 is an IETF standard for authorization. It provides authorization flows for web applications, desktop applications, mobile phones, and intelligent devices, which can be used for cloud services.

- **WS-Federation**[16]
  WS-Federation is an OASIS standard for identity federation in relation to web services. It is part of the wider WS-Security standard and in particular utilizes the WS-Trust standard for the exchange of various tokens.

- **OpenID Connect**[17]
  OpenID Connect is a specification that provides an API-friendly layer on top of the OAuth 2.0 protocol.

[13] Refer to http://tools.ietf.org/html/rfc4510 for details.

[14] Refer to https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security for details.

[15] Refer to http://oauth.net/2/ for details.

[16] Refer to http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html for details.

[17] Refer to http://openid.net/connect/ for details.

- **SCIM**[18]
  SCIM stands for System for Cross-domain Identity Management and is an IETF standard for managing user identities across domains – and specifically aimed at the needs of cloud services.

- **Active Directory Federated Services (ADFS2)**[19]
  A Microsoft proprietary specification supporting single sign-on.

For access control and security policy decisions and enforcement there is:

- **XACML**[20]
  XACML stands for *eXtensible Access Control Markup Language* and defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate authorization requests according to the rules defined in policies.

In addition, certificates are an important aspect of IAM and the cloud service customer should be aware of the support that the cloud service provider has for certificates, including PKCS[21], X.509[22] and OpenPGP[23].

Access control determines what type of authorizations to cloud accessible resources should be provided by the cloud service provider for authenticated users. Customers should require fine-grained access control both for stored data and for applications, to enable the customer to enforce their security policies. This includes being able to create and manage authorization policies for different groups of users, assigning them to different permission groups with the ability to distinguish access to different types of resources (e.g. compute, storage, network, etc.).

Determining which of the IAM standards to use will depend partly on the customer's own systems and partly on the nature of the cloud service. Probably the most important consideration from the customer's perspective is what IAM technologies are already being used and which of the standards are supported by that technology. If a particular cloud service provider forces the cloud service customer to install and use new IAM technology, the costs and risks of this must be factored in to any decision to use the cloud service provider.

[18] Refer to http://datatracker.ietf.org/wg/scim/charter/ for details.

[19] Refer to http://social.technet.microsoft.com/wiki/contents/articles/2735.ad-fs-2-0-content-map.aspx for details.

[20] Refer to https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml for details.

[21] Refer to http://www.rsa.com/rsalabs/node.asp?id=2124 for details.

[22] Refer to http://www.ietf.org/rfc/rfc3280.txt for details.

[23] Refer to http://www.openpgp.org/ for details.

Step 4: Ensure proper protection of data and information

Data are at the core of information security concerns for any organization, whatever the form of infrastructure that is used. Cloud computing does not change this, but cloud computing does bring an added focus because of the distributed nature of the cloud computing infrastructure and the shared responsibilities that it involves. Security considerations apply both to *data at rest* (held on some form of storage system) and also to d*ata in motion* (being transferred over some form of communication link), both of which may need particular consideration when using cloud computing services.

Essentially, the questions relating to data for cloud computing are about various forms of risk: risk of theft or unauthorized disclosure of data, risk of tampering or unauthorized modification of data, risk of loss or of unavailability of data. It is also worth remembering that in the case of cloud computing, "data assets" may well include things such as application programs or machine images, which can have the same risk considerations as the contents of databases or data files.

The general approaches to the security of data are well described in specifications such as the ISO 27002 standard - and these control-oriented approaches apply to the use of cloud computing services, with some additional cloud-specific considerations as described in the ISO 27017 standard (currently under development). Security controls as described in ISO 27002 highlight the general features that need to be addressed, including asset management, access control and cryptography, to which specific techniques and technologies can then be applied.

Security standards to consider for data in motion include:

- *HTTPS* - for regular connections from cloud service customers over the internet to cloud services
- *SFTP* - for bulk data transfers
- *VPN using IPSec or SSL* - preferable for connections from employees of the customer to the cloud service

For data at rest – stored within a cloud service – the principle is that sensitive data should be encrypted. This may be required for compliance with some information security standards such as PCI-DSS and HIPAA. There can be multiple architectural approaches for encryption in cloud computing – storage device level, agent based, file system based and application level. Each approach has its particular characteristics relating to performance and the handling of encryption keys. There is also a question of the granularity of encryption – the whole of a volume, a directory, a file. Which approach to take will partly depend on the capabilities provided by the cloud service provider and partly depend on the security requirements of the cloud service customer.

For each of these encryption approaches, there are many possible encryption algorithms which can be used, but useful guidance includes:

- The algorithm chosen should be recommended by a standard such as the US FIPS 140-2[24].

[24] Refer to http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf for details.

- Encryption keys should be handled appropriately – in particular the keys should not be stored alongside the data. For IaaS and PaaS, it may be the case that the keys are stored by the customer and passed to the application as required. For SaaS, encryption is more in the hands of the provider, in which case appropriate assurance should be sought about key handling. The Key Management Interoperability Protocol[25] (KMIP) provides a standardized way to manage encryption keys across diverse infrastructures. Cloud service customers should inquire if their prospective cloud service providers support KMIP.

Once ISO 27017 is completed (currently expected in 2014), customers are advised to check if their cloud service provider conforms to this standard, since it is specific to cloud computing.

Step 5: Enforce privacy policies

Privacy primarily relates to the acquisition, storage and use of personally identifiable information (PII). There are laws and regulations in many countries which relate to PII. Any cloud service customer must give serious consideration to any PII that they intend to store or process within a cloud service. Typically, privacy implies limitations on the use and accessibility of PII, with associated requirements to tag the data appropriately, store it securely and to permit access only by appropriately authorized users.

Privacy related issues should be dealt with in the cloud service contract and service level agreement. It should be clear how responsibilities are allocated between the provider and the customer and also which jurisdictions are involved. It is likely that the level of responsibility will vary greatly depending on the nature of the cloud service involved. For the provision of a virtual machine as part of an IaaS service, it is likely that the cloud service provider would be unaware of the nature of the data which the customer stores or processes with the service and that all responsibilities lie with the customer, other than basic information security preventing theft and unavailability.

For an application that explicitly deals with PII, offered as a SaaS service by a cloud service provider, then it would be natural to expect that the provider would be responsible for the appropriate protection of the PII within the service – in particular the encryption of the data and the provision of suitable fine-grained access control. In addition to encryption, database activity monitoring as well as database vulnerability scanning are capabilities to look for in a cloud service provider.

There are some specifications and standards which relate to privacy and the handling of PII. One of the established frameworks is the U.S – EU Safe Harbor framework[26], which enables US based companies to certify their compliance to the requirements of the EU data protection directives. This is further supported by commercial certification offerings, such as the TRUSTe Safe Harbor certification seal program[27]. Cloud service customers can use this framework as an assurance that a cloud service provider is treating PII in an appropriate fashion.

[25] Refer to https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip for details.

[26] Refer to http://export.gov/safeharbor/ for details.

[27] Refer to see http://www.truste.com/products-and-services/enterprise-privacy/eu-safe-harbor-seal for details.

The ISO 27018 standard is under development and this standard aims to extend the established ISO 27002 security standard to deal with the handling of PII in the context of cloud computing. Once ISO 27018 is published, cloud service customers should be able to request cloud service providers to establish their conformance to this standard concerning any cloud services which deal with PII.

Step 6: Assess the security provisions for cloud applications

Organizations need to proactively protect their business-critical applications from external and internal threats throughout their entire life cycle, from design to implementation to production. Clearly defined security policies and processes are critical to ensure the application is enabling the business rather than introducing additional risk.

Application security poses specific challenges to the cloud service provider and customer. Organizations must apply the same diligence to application security as they do for physical and infrastructure security. If an application is compromised, it can present liability and perception issues to both the cloud service provider and the consumer, especially if the ultimate end users of the application are customers of the cloud service customer, rather than employees. The Open Web Application Security Project (OWASP) project provides some useful information about application security, including application security for cloud computing.[28]

In order to protect an application from various types of threat, it is typical to define a set of policies which apply to the deployment and provisioning of the application. For cloud computing, it is important to understand the application security policy implications of the different cloud service models. The type of cloud service is very likely to affect the key question of who is responsible for handling particular security controls. For IaaS, more responsibility is likely to be with the customer (e.g. for encrypting data stored on a cloud storage device); for SaaS, more responsibility is likely to be with the provider, since both the stored data and the application code is not directly visible to or controllable by the customer.

For IaaS cloud services, the applications and the complete software stack beneath them are the responsibility of the customer – many of the required security provisions are then also the responsibility of the customer. The customer may inquire about security capabilities available from the provider to help the customer secure their applications (e.g. "security as a service").

For PaaS cloud services, the application code itself is the responsibility of the customer, but the rest of the software stack is in the hands of the provider (for example, patching and dealing with vulnerabilities of the stack is the remit of the provider). The customer needs to enquire of the provider what security capabilities are provided for the software stack and what capabilities must be implemented by the customer (e.g. encryption of data at rest).

For SaaS cloud services, the bulk of the responsibility for securing the services and the associated data lies with the cloud service provider. In these cases, the customer should expect the provider to provide documentation of all the security capabilities provided and also to document any options or features that the customer needs to configure.

[28] Refer to https://www.owasp.org/index.php/Main_Page for details.

Technologies and techniques to consider in relation to cloud applications are:

- Firewalls to control access to applications and systems.
- VPNs to limit access to applications to users with authorization to access the VPN.
- Denial-of-Service countermeasures for any service endpoints that are exposed publicly on the internet.
- Countermeasures for the OWASP Top 10 application vulnerabilities should be considered.[29]

The NIST publication, *Guidelines on Firewalls and Firewall Policy* [2], provides an overview of firewall technologies and discusses their security capabilities and relative advantages and disadvantages in detail. The document makes recommendations for establishing firewall policies and for selecting, configuring, testing, deploying, and managing firewall solutions.

Standards and specifications which allow the cloud service customer to describe and then enforce a set of policies for their applications are somewhat thin on the ground today. These policies include where and how the application is deployed, with particular consideration for scalability options and for describing availability, encryption and integrity requirements.

For IaaS applications, there are some metadata capabilities available with the OVF 2.0 specification[30]. For PaaS (and IaaS) applications, the OASIS TOSCA[31] standard offers capabilities to describe the configuration and requirements of the application, but it is a relatively new standard and currently support by cloud service providers is limited.

Step 7: Ensure cloud networks and connections are secure

A cloud service provider must attempt to allow legitimate network traffic and drop malicious network traffic, just as any other Internet-connected organization does. However, unlike many other organizations, a cloud service provider will not necessarily know what network traffic its consumers plan to send and receive. Nevertheless, consumers should expect a certain amount of external network perimeter and internal network separation measures from their cloud service providers.

In addition to the previously mentioned ISO 27001 and 27002 standards, the ISO/IEC 27033[32] standards provide detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002. Documentation of adherence to the applicable portions of these standards would typically be included as part of an ISO 27002 certification. They are:

[29] Refer to https://www.owasp.org/index.php/Top_10_2013-Top_10 for details.

[30] Refer to http://dmtf.org/standards/ovf for details.

[31] Refer to http://docs.oasis-open.org/tosca/TOSCA/v1.0/cs01/TOSCA-v1.0-cs01.html for details.

[32] Refer to http://www.iso27001security.com/html/27033.html for details.

- ISO/IEC 27033-1 — Network security overview and concepts
- ISO/IEC 27033-2 — Guidelines for the design and implementation of network security
- ISO/IEC 27033-3:2010 — Reference networking scenarios - threats, design techniques and control issues

The United States Federal Information Security Management Act of 2002 ("FISMA") legislation mandates the use of certain security standards for federal government systems, such as FIPS 199 (system classification) and FIPS 200 (minimum security standards). FIPS 200 requires that controls be selected from NIST Special Publication 800-53[33] based on the system classification. While these standards and controls are only required for US federal government systems, other organizations use them as a framework for their own security policies. The "System and Communications Protection" controls listed in Appendix F are the controls that would be most applicable to networking for cloud service providers. A few examples of these controls are:

- *SC-7 Boundary Protection.* Deals with firewalls and other controls.
- *SC-8 Transmission Confidentiality and Integrity.* Deals with protecting data "in motion."

The Federal Risk and Authorization Management Program (FedRAMP) program provides authorizations for cloud service providers to host US federal information systems. There are no new controls for FedRAMP. The FedRAMP security controls are based on NIST Special Publication 800-53 R3 controls for low and moderate impact systems, and contain controls and enhancements above the NIST baseline for low and moderate impact systems that address the unique elements of cloud computing. There are a number of third party assessment organizations that can verify that cloud service providers meet the FedRAMP requirements. [34]

The TM Forum also maintains the *TM Forum Frameworx*[35], which is a suite of best practices and standards that provides the blueprint for effective, efficient business operations. Some of the TM Forum Guidebook documents that cloud service providers might use to create policies are listed below. Note that these documents merely help providers create policies. In order to effectively mitigate risks, the policy must be backed by both skilled employees and a network architecture that has been tested, perhaps via simulated attacks.

[33] The NIST Special Publication 800-53 is available at http://csrc.nist.gov/publications/PubsSPs.html. Note that NIST Publications are recommendations and not standards.

[34] A frequently asked questions page on FEDRamp is available at http://www.gsa.gov/portal/content/118875.

[35] Refer to http://www.tmforum.org/TMForumFrameworx/1911/home.html for details.

- *Quick Start Pack: DDoS Prevention, Version 0.5*.[36] Provides a template policy for a provider to deal with Distributed Denial of Service (DDoS) attacks.
- *CyberOps Metrics*: Guide for DDoS Mitigation, Version0.6.[37] Provides Key Performance Indicators (KPI) for Distributed Denial of Service mitigation.

A relatively new concept in networking is “Software Defined Networks” (SDN), which allows for the network control and forwarding functions to be handled separately. Although the network architecture is different, most of the same security controls apply to SDN. Although there are standards for SDN protocols, such as OpenFlow, as of this writing there are no SDN-specific security standards.

At this point, network security certification remains rare, and only the largest providers are certified compliant with ISO 27002. Nevertheless, even if a cloud service provider has no network security attestation or certification, customers should at least ensure that a cloud service provider has documented and tested processes for:

- Access controls, for management of the network infrastructure
- Traffic filtering, provided by firewalls
- Creating secure Virtual Private Networks (if VPN is offered)
- Intrusion detection / prevention
- Mitigating the effects of DDoS attacks
- Logging and notification, so that systematic attacks can be reviewed

Step 8: Evaluate security controls on physical infrastructure and facilities

An important consideration for security of any IT system concerns the security of physical infrastructure and facilities. In the case of cloud computing, these considerations apply, but it will often be the case that the infrastructure and facilities will be owned and controlled by the cloud service provider and it is the responsibility of the cloud service customer to get assurance from the provider that appropriate security controls are in place. Effective physical security requires a centralized management system that allows for correlation of inputs from various sources, including property, employees, customers, the general public, and local and regional weather.

Cloud service customers are advised to look for cloud service providers that conform to the ISO 27002 standard for physical and environmental security. Although ISO 27002 is not specific to cloud computing, its principles can still be usefully applied to the provision of cloud services. A brief

[36] Refer to http://www.tmforum.org/DocumentCatalog/GB975QuickStartPack/51787/article.html for details.

[37] Refer to http://www.tmforum.org/GuideBooks/GB973CyberOpsMetrics/52074/article.html for details.

description of the security controls contained in ISO 27002 that apply to the physical infrastructure and facilities of a cloud service provider includes:

- *Physical Infrastructure and facilities should be held in secure areas*. A physical security perimeter should be in place to prevent unauthorized access, allied to physical entry controls to ensure that only authorized personnel have access to areas containing sensitive infrastructure. Appropriate physical security should be in place for all offices, rooms and facilities which contain physical infrastructure relevant to the provision of cloud services.

- *Protection against external and environmental threats*. Protection should be provided against things like fire, floods, earthquakes, civil unrest or other potential threats which could disrupt cloud services.

- *Control of personnel working in secure areas.* Such controls should be applied to prevent malicious actions.

- *Equipment security controls.* Should be in place to prevent loss, theft, damage or compromise of assets.

- *Supporting utilities such as electricity supply, gas supply, and water supply should have controls in place.* Required to prevent disruption either by failure of service or by malfunction (e.g. water leakage). This may require multiple routes and multiple utility suppliers.

- *Control security of cabling.* In particular power cabling and telecommunications cabling, to prevent accidental or malicious damage.

- *Proper equipment maintenance.* Should be performed to ensure that services are not disrupted through foreseeable equipment failures.

- *Control of removal of assets.* Required to avoid theft of valuable and sensitive assets.

- *Secure disposal or re-use of equipment*. Particularly any devices which might contain data such as storage media.

- *Human resources security*. Appropriate controls need to be in place for the staff working at the facilities of a cloud service provider, including any temporary or contract staff.

- *Backup, Redundancy and Continuity Plans.* The provider should have appropriate backup of data, redundancy of equipment and continuity plans for handling equipment failure situations.

Assurance may be provided by means of audit and assessment reports, demonstrating compliance to ISO 27002. A number of cloud service providers already claim conformance to 27002. A company can assert on its own behalf as to its compliance with a standard, of course having an independent/qualified third party assert to your compliance is a notably stronger form of attestation.

As stated in Step 1, a new standard under development, ISO 27017, deals with the application of the ISO 27002 specification to the use of cloud services and to the provision of cloud services. Once ISO 27017 is completed, customers are advised to check if their cloud service provider conforms to this standard, since it is specific to security in a cloud computing environment.

Step 9: Manage security terms in the cloud SLA

Since cloud computing typically involves two organizations - the cloud service customer and the cloud service provider, security responsibilities of each party must be made clear. This is typically done by means of a service level agreement (SLA) which applies to the services provided, and the terms of the service contract between the customer and the provider. The SLA should specify security responsibilities and should include aspects such as the reporting of security breaches. SLAs for cloud computing are discussed in more detail in the CSCC document "Practical Guide to Cloud Service Level Agreements, Version 1.0".

Metrics for measuring performance and effectiveness of information security management should be established prior to subscribing to cloud services and should be specified in the cloud SLA. At a minimum, organizations should understand and document their current metrics and how they will change when operations make use of cloud computing and where a provider may use different (potentially incompatible) metrics.

Measuring and reporting on a provider's compliance with respect to data protection is a tangible metric of the effectiveness of the overall enterprise security plan. A *data compliance report* or an *information security certification* should be required from the cloud service provider and reflects the strength or weakness of controls, services, and mechanisms supported by the provider in all security domains.

At this point in time, standards for describing and measuring specific metrics for cloud security do not exist. One-off or periodic provider assessments, such as ISO 2700x, SSAE 16 or ISAE 3402, assure that for the evaluation period, a certain set of controls and procedures was in place. These assessments are a vital component of effective security management. However, they are insufficient without additional feedback in the intervals between assessments: they do not provide real-time information, regular checkpoints or threshold based alerting.

There are a few standards initiatives that are in-process that are taking a closer look at common metrics and management approaches for cloud SLAs, including cloud security metrics. In particular, TM Forum is working on a technical report titled *Enabling End-to-End Cloud SLA Management*. The report provides a set of common approaches for two parties to determine their cloud SLA, define what to measure, the threshold and indicators as well as some architecture design principles for service providers to "join the dots" so that end-to-end cloud SLA management can be achieved with process automation and architecture flexibility to support different business scenarios and customer needs.

Additional resources are available that contain specific information on security metrics. Although these resources are not cloud specific, they provide valuable guidance that applies equally in traditional enterprise environments as well as cloud environments:

- ISO 27004:2009[38]

- NIST Special Publication (SP) 800-55 Rev.1, Performance Measurement Guide for Information Security[39]

- CIS Consensus Security Metrics v1.1.0[40]

The European Network and Information Security Agency[41] (ENISA) has published a guide titled "*Procure Secure: A guide to monitoring of security service levels in cloud contracts*" [3] which breaks down key requirements that a cloud service customer should look for in a cloud service provider to ensure strict adherence to security protocols. It includes a cloud security monitoring framework that covers:

- *What to measure.* Which security-relevant parameters of the service should be monitored throughout the contract?
- *How to measure them.* How the data can be collected in practice.
- *How to get independent measurements.* Which security relevant features of the service can be monitored independently from the provider and how.
- *When to raise the flag.* Considerations for setting reporting and alerting thresholds.
- *Customer responsibilities.* Whose problem is it? What needs to be taken care of by the customer on an on-going basis?

The specific metrics covered in the guide include: s*ervice availability, incident response, service elasticity and load tolerance, data life-cycle management, technical compliance and vulnerability management, change management, data isolation, and log management & forensics.* While not a standard, customers are advised to leverage the guidance provided in this document.

In the Public sector, government agencies may provide guidance on how to address security requirements and terms in cloud SLAs. For example, the U.S. General Services Administration (GSA) has documented areas of concern, within the context of cloud security requirements, which may require additional contract clauses[42]. The guidance details the security terms at the security controls level and provides sample template language that can be used to document technical requirements. The GSA's guidance addresses areas that mirror commercial enterprises' concerns and, thus, can be leveraged more broadly.

[38] See http://www.iso.org/iso/catalogue_detail.htm?csnumber=42106.

[39] See http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[40] See http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.metrics.110.

[41] Refer to http://www.enisa.europa.eu/ for details.

[42] Refer to http://www.gsa.gov/graphics/staffoffices/FedRAMP_Control_Specific_Clauses_062712.pdf for details.

Step 10: Understand the security requirements of the exit process

The exit process or termination of the use of a cloud service by a customer requires careful consideration from an information security perspective. The overall need for a well defined and documented exit process is described in the CSCC document "Practical Guide to Cloud Service Level Agreements, Version 1.0" [4].

From a security perspective, it is important that once the customer has completed the termination process, "reversibility" or "the right to be forgotten" is achieved - i.e. none of the customer's data should remain with the provider. The provider must ensure that any copies of the data are wiped clean from the provider's environment, wherever they may have been stored (i.e. including backup locations as well as online data stores). Note that other data held by the provider may need "cleansing" of information relating to the customer (e.g. logs and audit trails), although some jurisdictions may require retention of records of this type for specified periods by law.

Clearly, there is the opposite problem during the exit process itself - the customer must be able to ensure a smooth transition, without loss or breach of data. Thus the exit process must allow the customer to retrieve their data in a suitably secure form, backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must also be retained until the exit process is complete.

At the end of the exit process, it is good practice for the provider to provide the customer with written confirmation that the process is complete and that the customers' data has been removed from the provider's systems.

At this point in time, standards that specifically focus on the exit process for cloud computing environments, including specific security implications, do not exist. Within the auspices of ISO SC38 WG3, an ad hoc report titled *Cloud Service Delivery Principles and Service Level Agreements* has recently been submitted. The report focuses on the concept of cloud service delivery principles and its associated stages including: stakeholder viewpoints, service selection, negotiation, subscription, onboarding, provisioning, customer support, termination of service, establishment of contract, service level agreements, governance, management, and maintenance. The report performs an analysis of each stage with the goal of identifying any existing gaps or issues.

The ISO report recommends that the termination of use and the exit process for cloud computing are subjects that need to be addressed and that a new work item proposal should be initiated to address gaps in this area. It is unlikely that specific standards and guidance will be provided by this initiative before 2014. In the meantime, customers are advised to negotiate directly with their cloud service provider to ensure appropriate exit process provisions and assurances are included and adequately documented in their cloud SLA.

Cloud Security Standards Recommendations

The table below summarizes the cloud security standards recommendations and certification recommendations for each of the ten evaluation steps highlighted in this whitepaper.

	Standards Recommendations	**Certification Recommendations**
Step 1: Ensure effective GRC processes exist	• Ensure CSP complies with COBIT, ISO 20000, SSAE 16 or ITIL depending on type of workload • Ensure CSP conforms to the ISO 27001 and ISO 27002 standards for information systems security • Once ISO 27017 & ISO 27018 are completed, ensure CSP conforms to these standards	• Insist on ISO 27002 certification today and ISO 27017 certification when it becomes available • For cloud services with impact on financial activities seek SSAE 16 certification
Step 2: Audit operational and business processes	• Ensure CSP complies with SSAE 16 for financial • Ensure CSP conforms to the ISO 27000 series of standards • In the 2014 timeframe, determine if your CSP supports DMTF CADF	• Insist on ISO 27002 certification today and ISO 27017 certification when it becomes available • For cloud services with impact on financial activities seek SSAE 16 certification
Step 3: Manage people, roles and identities	• Ensure CSP supports federated IDs and single sign-on using one or more of the following standards: LDAP, SAML 2.0, OAuth 2.0, WS-Federation, OpenID Connect, SCIM • Ensure CSP provides access control and security policy decisions leveraging a standard such as XACML • Ensure CSP supports one or more of the following standards for security certificates: PKCS, X.509, OpenPGP	• Insist on ISO 27002 certification which provides a *framework* to ensure cloud service provider has proper controls in place to manage people, roles and identities • Insist on 27017 certification when it becomes available
Step 4: Ensure proper protection of data & information	• Ensure CSP supports one or more of the following standards for data in motion: HTTPS, SFTP, VPN using IPSec or SSL • Ensure CSP supports one or more of the encryption standards defined in US FIPS 140-2 • Ensure CSP securely manages security keys using a standard such as OASIS KMIP	• Insist on ISO 27002 certification which provides a *framework* to ensure cloud service provider has proper controls in place to protect customer data and information • Insist on 27017 certification when it

		becomes available
Step 5: Enforce privacy policies	• Ensure CSP supports U.S – EU Safe Harbor framework • Ensure CSP conform with ISO 27018 when finalized	• Leverage commercial certification offerings, such as the TRUSTe Safe Harbor certification seal program • Insist on 27018 certification when it becomes available
Step 6: Assess the security provisions for cloud apps	• Ensure CSP supports technologies and techniques to protect applications in the cloud including Firewalls, VPNs and DoS countermeasures [2]	• Insist on ISO 27002 certification which provides a *framework* to ensure cloud service provider has proper controls in place to protect cloud applications • Insist on 27017 certification when it becomes available
Step 7: Ensure cloud networks and connections are secure	• Ensure CSP supports the ISO/IEC 27033 standards • Related work includes OpenFlow, TM Forum Frameworx, FIPS 199, FIPS 200, NIST SP 800-53	• Insist on 27002 certification which provides detailed guidance on implementing network security controls • Insist on 27017 certification when it becomes available
Step 8: Evaluate security controls on physical infrastructure & facilities	• Ensure CSP conforms to the ISO 27002 standard for information systems security • Once ISO 27017 & ISO 27018 are completed, ensure CSP conforms to these standards	• Insist on ISO 27002 certification today and ISO 27017 certification when it becomes available
Step 9: Manage security terms in the cloud SLA	• Currently no finalized standards to support real-time assessment of security terms in cloud SLA • Related work includes ISO 27004:2009, NIST SP 800-55, CIS Consensus Security Metrics V1.1.0, ENISA • TM Forum actively working on end-to-end SLA Management	• For periodic assessments, insist on ISO 27002 certification today and ISO 27017 certification when it becomes available • For cloud services with impact on financial activities seek SSAE 16 certification (periodic assessment)

Step 10: Understand the security requirements of the exit process	• Currently no finalized standards in this space • Future work in this space proposed for ISO SC38 WG3	• Currently no certifications in this space

Works Cited

[1] Cloud Standards Customer Council (2012). *Security for Cloud Computing: 10 Steps to Ensure Success*. http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf

[2] NIST. *Guidelines on Firewalls and Firewall Policy*. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

[3] ENISA. *Procure Secure: A guide to monitoring of security service levels in cloud contracts.* http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

[4] Cloud Standards Customer Council (2012). *Practical Guide to Cloud SLAs*. http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf

Additional References

- Cloud Security Alliance. *Certificate of Cloud Security Knowledge*. https://cloudsecurityalliance.org/education/ccsk/

- IT Certification Master. *List of Cloud Certifications.* http://www.itcertificationmaster.com/it-certifications/cloud-certifications/

- NIST. *National Vulnerability Database*. http://nvd.nist.gov/

- NIST. *Inventory of Standards Relevant to Cloud Computing*. http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory

- NIST Special Publication 800-144. *Guidelines on Security and Privacy in Public Cloud Computing* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

- U.S. CIO Office. *Recommendations for Standardized Implementation of Digital Privacy Controls*. https://cio.gov/wp-content/uploads/downloads/2012/12/Standardized_Digital_Privacy_Controls.pdf