Cloud Security Standards: What to Expect & What to Negotiate Version 2.0

August, 2016

Contents

Acknowledgements

The major contributors to this whitepaper are: Claude Baudoin (cébé IT & Knowledge Management), Ryan Devlin (McKesson), Chris Dotson (IBM), Mike Edwards (IBM), Maryann Hondo (State Street), Ryan Kean (The Kroger Co.), Shamun Mahmud (GRC Research Associates), John Meegan (IBM), Nya Murray (Trac-Car), Osakpamwan Osaigbovo (IBM), Barry Pardee (QED National), Karl Scott (W. Capra), Anil K. Sharma (IBM), Annie Sokol (NIST), Wisnu Tejasukmana (Schlumberger), Alexander Tumashov (Schlumberger), Mark Underwood (Krypton Brothers), and Pamela Wise-Martinez (Pension Benefit Guaranty Corporation).

What is New in Version 2.0

Version 1.0 of this white paper was published in 2013. In the interval, the cloud security standards landscape has changed significantly with the completion of cloud specific security standards, like ISO/IEC 27017, that are being adopted. The paper has been updated to highlight the status of these standards and associated certifications.

In addition, there are increasingly stringent laws and regulations in many countries which relate to personally identifiable information (PII). An example is the EU General Data Protection Regulation (GDPR) which applies to processing of PII of EU citizens. The paper has been updated to reflect these developments, highlighting standards like ISO/IEC 27018 and associated certifications that help address this area.

Executive Overview

Cloud security standards and their support by prospective cloud service providers and within the enterprise should be a critical area of focus for cloud service customers. The benefits of supporting key security standards are numerous:

- Standards promote interoperability, eliminating vendor lock-in and making it simpler to transition from one cloud service provider to another.
- Standards facilitate hybrid cloud computing by making it easier to integrate on-premises security technologies with those of cloud service providers.
- Standards provide a level of assurance that critical best practices are being followed both internally within an enterprise and by cloud service providers – certifications are available for several security standards.
- Standards support provides an effective means by which cloud service customers can compare and contrast cloud service providers.
- Standards support enables an easier path to regulatory compliance.

The current landscape for information security standards specifically targeted for cloud computing environments is best characterized as maturing. There are several cloud specific security standards initiatives that have recently been published, including ISO/IEC 27017 and ISO/IEC 27018, that provide more detailed guidance and recommendations for both cloud service customers and cloud service providers. In addition, there are a number of *general* IT security standards (such as ISO/IEC 38500 and X.509 certificates) that are applicable to cloud computing environments; customers should be aware of them and insist that their cloud service providers support them.

This paper focuses primarily on information security requirements for public cloud deployment, since this deployment 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, data structures and communication protocols that must be implemented to claim support for the standard. There can be test suites associated with these standards that enable implementers to demonstrate compliance to the standard and there can also be mechanisms to demonstrate interoperability between different implementations. In many cases, such standards allow for extensibility, permitting implementers to include functions that go beyond those defined in the standard.

Certification of cloud services is an important aspect for cloud service customers to review. Certification is often carried out by independent third-party auditors, although in some circumstances, self-certification by the provider is possible. Auditors typically examine the documented policies, procedures and designs of the provider, and then examine the day-to-day operations of the provider to check that these follow the documentation, before providing the certification. It is typical for certification to apply to specific cloud services, rather than to the cloud service provider as a whole – it is important for the cloud service customer to verify the certification for each of the cloud services that they use.

Certification provides assurance to cloud service customers that their critical security requirements are being met. Therefore, cloud service customers should identify the well-established security certifications that are important to their organizations and insist that their cloud service providers demonstrate their conformance to those. 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 be equal to or better than the security provided by their non-cloud 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 service agreement
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 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

Effective governance is essential to guiding management processes and decision making to deliver IT services in accordance with the needs of the organization. Standards to support the 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. General governance standards include:

- **ISO/IEC 38500 – IT Governance** [2]
  The ISO (International Organization of Standardization) 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** [3]
  COBIT (Control Objectives for Information and Related Technology) 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/IEC 20000 and ISO/IEC 27000.

- **ITIL** [4]
  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/IEC 27002 standard (see below).

- **ISO/IEC 20000** [5]
  ISO/IEC 20000 is a series of well-established and internationally recognized standards for IT service management. It is not specific to cloud computing and cloud services, but a new

standard, ISO/IEC 20000-7, is being developed to address the application of ISO/IEC 20000 to cloud computing. In addition, the ISO/IEC 20000-11 specification, under development, will describe the relationship of ISO/IEC 20000 to other frameworks and in particular to ITIL.

- **SSAE 16** [6]
  SSAE (Statement on Standards for Attestation Engagement) 16 is an audit standard which applies to service organizations including cloud service providers. SSAE 16 audits come in three forms: SOC (Service Organization Controls) 1; SOC 2; and SOC 3. SOC 1 is focused on financial reporting controls, while SOC 2 emphasizes Trust Services Principles to assess the effectiveness of technical and operational security controls. SOC 3 is similar to SOC 2 but reports on whether the organization has achieved Trust Services Principles compliance (yes or no) rather than a detailed analysis of capability. Additionally, the SOC 3 report can be freely distributed.

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)** [7]
  CSF is a cross industry reference framework geared at overlaying federal security assessment and authorization (SA&A) security controls into the private industry (specifically critical infrastructure environments). This is emerging as a standard governance framework for cloud computing in private industry.

- **Cloud Security Alliance (CSA) Cloud Controls Matrix** [8]
  The CSA conducts cloud security research, professional education, and provider certification to promote secure delivery and use of cloud computing services. The CSA has published a Cloud Controls Matrix that provides insight into the key security control considerations when assessing cloud provider services. This document is helpful in establishing effective cloud security governance.

In addition to the general standards and frameworks listed above, there are others that operate at country or regional levels or that 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:

Health Care

- **HIPAA** [9]
  The Health Insurance Portability and Accountability Act (HIPAA) is a regulation that requires U.S. health care providers to maintain the confidentiality and security of protected health information (PHI).

Payment Card

- **PCI-DSS** [10]
  The Payment Card Industry Data Security Standard (PCI-DSS) is an industry mandate that defines

the minimum security controls needed to protect customer cardholder data throughout its lifecycle.

Education

- **FERPA** [11]
  Family Educational Rights and Privacy Act is a U.S. federal law that protects student education records. FERPA applies to educational institutions that receive funds from the U.S. Department of Education.

U.S. Federal Government

- **FedRAMP** [12]
  The Federal Risk and Authorization Management Program (FedRAMP) provides a standard methodology to security assessment, authorization, and continuous monitoring of cloud products and services. It should be noted that NIST SP 800-53 is used to establish security standards while FedRAMP certifies that the service provider is compliant with the standards. All federal organizations that use or plan to use cloud services are required to implement the FedRAMP program.

- **FIPS Publication 200** [13]
  The Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," addresses minimum standards that apply to cloud-based systems as well as on-premises systems. Compliance with FIPS-200 is mandatory for all federal systems.

- **FISMA** [14]
  The Federal Information Security Management Act (FISMA) is a compliance framework that requires all federal agencies and their contractors to protect information systems and assets. FISMA delegated the definition of framework security standards to NIST, which uses NIST SP 800-53 (see definition below). These standards are published in FIPS Publication 200.

- **HSPD-12** [15]
  Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," mandates a standardized federal identity credential that is designed to enhance security, reduce identity fraud, and protect the personal privacy of those who are issued government identification. HSPD-12 calls for a mandatory, government-wide standard for secure and reliable ID for all of its employees and employees of federal contractors to access federally-controlled facilities and networks. HSPD-12 compliant identity cards are also known as Personal Identity Verification (PIV) cards. The cards utilize an on-board cryptographic capability with PKI-based public and private keys to perform identity functions and provide one technical means to implement two-factor authentication across systems and applications.

- **NIST SP 800-53 R4** [16]
  NIST Special Publication 800-53 revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security and privacy controls for federal information systems, to include cloud-based systems, and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the U.S. from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.

European Union

- **EU-US Privacy Shield** [17]
  The Privacy Shield Framework provides a set of enforceable protections for the personal data of EU citizens. This Shield replaces Safe Harbor and requires all organizations doing business within the EU to comply.

- **EU NIS Directive** [18]
  The EU Network and Information Security (NIS) Directive applies to cybersecurity and incident response for IT services across EU member states.

If IT governance by the cloud service provider is a significant concern for a cloud service customer, then customers are advised to establish whether a provider complies with one or more of these governance and management standards. Of the standards listed here, ISO/IEC 20000 or SSAE 16 would be the most common to look for, depending on the sensitivity of the data the customer is considering placing into the cloud environment. Cloud service customers must be aware that compliance with standards does not ensure effective security. In addition to confirming compliance, cloud customers must continually review service provider security controls to ensure they are properly defined and enforced.

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*** [19] of standards is probably the most widely recognized and used set of standards relating to the security of ICT (Information and Communication Technology) systems. The core standards are 27001 and 27002, with 27001 containing the requirements relating to an information security management system and 27002 describing a series of controls that address specific aspects of the information security management system.

ISO/IEC 27001 is an advisory standard that is meant to be interpreted and applied to all types and sizes of organizations 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/IEC 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 (that is, there are no notable gaps) it can be asserted that their environment is *compliant* with the standard.

ISO also has standards that give specific guidance for cloud service providers and cloud service customers in the area of Security (ISO/IEC 27017) and separately for the protection of Personally Identifiable Information (PII) in public clouds (ISO/IEC 27018). ISO/IEC 27017, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services* [20], provides guidelines for information security controls applicable to the provision and use of cloud services. Specific guidance is included in ISO/IEC 27017 to clarify cloud service customer and cloud service provider responsibilities, given the split of responsibilities that exists when using and providing cloud services.

ISO/IEC 27018, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* [21], specifies guidelines, control objectives and controls aimed at protecting PII which is stored or processed by public cloud services. ISO/IEC 27018 provides additional guidance to ensure PII is adequately protected in accordance with the principles defined in ISO/IEC 29100 *Privacy Framework* [22]. ISO/IEC 27018 takes into account the often complex regulatory requirements that apply to PII.

Both ISO/IEC 27017 and ISO/IEC 27018 use the set of security controls defined in ISO/IEC 27002 as a base, extending them as necessary for the cloud service environment and for the handling of PII residing in a public cloud.

Cloud service customers are advised to look for cloud service providers that conform to the ISO/IEC 27001 and 27002 standards 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 its compliance with a standard, but having an independent and qualified third party certify compliance is a notably stronger form of attestation. A number of cloud service providers already claim conformance to ISO/IEC 27001, many of them through third-party certifications.

Customers should also seek cloud service providers with ISO/IEC 27017 certification. Major cloud service providers are currently certified and the standard is becoming pervasive throughout the industry. Additionally, customers should look for ISO/IEC 27018 certification when PII is in play. As previously stated, cloud service customers should not rely on certifications alone but should also seek to understand the cloud service providers' policies and processes that impact security (e.g., log retention policy, privileged access policy, change management process, etc.).

Step 2: Audit operational & business processes

Cloud service customers often have a requirement to audit the IT systems and related processes that they use. Audit requirements can stem from the regulatory environment that applies to the customer, or they may arise from business policies or IT security policies adopted by the customer organization. The requirement to audit is likely to apply to the use of cloud services as well as to the in-house systems of the customer. As a result, there is a need to audit the systems and processes of the cloud service provider.

In the case of public cloud services, where the cloud service provider's environment and systems are shared by potentially large numbers of cloud service customers, direct audit by each cloud service customer is likely to be problematic and impractical. It is more often the case that a cloud service provider undergoes periodical third-party audit against one or more audit standards and obtains a certificate or audit report which is made available to all their cloud service customers. However, for some cloud service customers, regulatory requirements may demand a more specific audit. Cloud service customers need to clearly understand their own requirements for audit in order to reflect this into audit requirements for the cloud service provider.

Cloud service customers should check that prospective cloud service providers are open to periodic third party audit – there should be appropriate terms relating to this in the cloud service agreement. The auditors must be able to audit against a specific audit regime, which likely involve inspecting current policies and current controls and also inspecting audit trails in the form of historic log data for the systems used to provide cloud services.

In addition, customers should assess their own application security, forensics, performance objectives and institutional compliance requirements to verify that audits can be successfully achieved with a specific cloud provider.

It is typical for audits to operate using the requirements of one of the common certification schemes or standards. For security controls, the ISO/IEC 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 the form of a SOC 1, SOC 2 or SOC 3 report.

Organizations subject to SEC Rule 613 [23] which choose cloud services to meet scalability or other objectives will be required to comply with various aspects of the consolidated audit trail.

Organizations with responsibility for personal data may have additional audit requirements stemming from guidelines in ISO/IEC 29100, 29151 and 27018 (see Step 5 below). When operating in countries such as Canada, consent rules are explicit under the country's PIPEDA regulation [24], and p*rivacy by design* practices can mandate additional cloud service audit requirements (see OASIS Privacy Management Reference Model (PMRM) [25] and Privacy by Design for Software Engineers (PbD-SE) [26]).

In addition to external auditing, such as that suggested in NIST 800-144 [27], 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) standard [28] 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 rare.[1]

Another development in the cloud services marketplace which addresses aspects of auditing and control of the use of cloud services is the emergence of products and services under the title of "Cloud Access Security Broker." A cloud access security broker (CASB) provides capabilities in four main areas: visibility, compliance, data security and threat protection. An overview of CASBs is given in the Gartner paper *Market Guide for Cloud Access Security Brokers* [30]. There is no standardization relating to CASBs at present, but there is a hope that more standard APIs will emerge over time as this part of the cloud computing marketplace matures.

Cloud customers often possess domain-specific knowledge of risks. Accordingly, customers should develop audit requirements and ensure that cloud provider audit resources can match them. This can entail, for instance, matching of application security audit capabilities to cloud services. Current standards work such as HL7 Fast Healthcare Interoperability Resources (FHIR) [31] patient consent mapping illustrates a higher level of audit sophistication as well as increased granularity. Implementation teams should assess audit requirements based on evolving regulatory and technology needs. An example of critical audit technology requirements is the 50 ms timing concern associated with the US stock market consolidated audit trail (CAT) [32].

Depending on an organization's risk profile, audit needs should be assessed in light of digital forensic requirements required by regulation or as revealed in domain-specific litigation. The NIST Draft NISTIR 8006, *NIST Cloud Computing Forensic Science Challenges* [33] identifies a number of potential audit needs associated with cloud computing forensics.

NIST SP 800-92, *Guide to Computer Security Log Management* [34] lists measures that can be taken to ensure the integrity, accessibility, and manageability of audit data. Though this document has not been specifically targeted for cloud services, it identifies issues such as the need to correlate cloud audit events with intra-organizational Security Information and Event Management (SIEM), prioritization, application-specific audit, and storage hierarchy concerns.

It is imperative that in scenarios where third party audits or internal audits are conducted, cloud service customers have the visibility to the documented results for verification and to highlight any issues that might be identified within the audit report for further clarification and remediation with the cloud service provider.

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!

[1] An unofficial implementation of CADF has been implemented in Python (*pyCADF*) for use with OpenStack [29].

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/IEC 27002 and ISO/IEC 27017 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.

There are a range of IAM security standards that can be utilized for cloud services. 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.

- *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 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** [35]
  The Lightweight Directory Access Protocol (LDAP) is an IETF standard widely used to provide access to directory servers, which includes authentication and authorization services.

- **SAML 2.0** [36]
  The Security Assertion Markup Language (SAML) is an XML based OASIS standard used for the exchange of authentication and authorization data between security domains – in particular between an identity provider and a service provider.

- **OAuth 2.0** [37]
  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** [38]
  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** [39]
  OpenID Connect is a specification that provides an API-friendly layer on top of the OAuth 2.0 protocol.

- **SCIM** [40]
  The System for Cross-domain Identity Management (SCIM) is an IETF standard for managing user identities across domains – and specifically aimed at the needs of cloud services.

- **Active Directory Federated Services (ADFS2)** [41]
  ADFS2 is a proprietary specification from Microsoft supporting single sign-on that is used by many organizations.

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

- **XACML** [42]
  The *eXtensible Access Control Markup Language* (XACML) 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, digital certificates are an important aspect of IAM, in support of public key infrastructure (PKI) and the establishment of trust when using cloud services. Cloud service customers should be aware of the support that the cloud service provider has for digital certificates, including PKCS [43], X.509 [44] and OpenPGP [45].

Access control determines what type of authorizations should be provided to cloud accessible resources 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. The aim should be to have access control granularity at least equivalent to that used for customer in-house systems. 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 supported and which version of the standards is supported by that technology. If a particular cloud service forces the cloud service customer to install and use new IAM technology, the cloud service customer must factor the estimated costs and risks of this change in to any decision to use the cloud service.

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. There is also the question of *data in process* (e.g., data in memory being used by application code), which might be subject to attack in a multi-tenant shared compute environment.

A related discipline of data and information protection is *data governance.* Data governance is the ability of an organization to manage its information knowledge and to answer questions such as: what do we know about our information; where did this data come from; and does this data adhere to the organization's policies and rules. Data governance practices provide a holistic approach to managing, protecting, improving and leveraging information to help an organization gain insight and build confidence in business decisions and operations.

When evaluating a cloud service, cloud service customers should ask questions relating to data for cloud computing 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. Also, 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.

Cloud service customers also need to address the added risk of their data no longer being under their physical control. As data in a cloud service is under the physical control of the cloud provider, a cloud customer needs to ensure that data protection approaches take this additional risk into account. Approaches include full encryption of data at rest and selective encryption of database fields or columns.

Metadata, in turn, could play a role in access controls, data integrity, traceability, PII consent and other aspects of security. However, at this time there are no security specific metadata standards available.

The general approaches to the security of data are well described in specifications contained in the ISO/IEC 27000 series. Security controls described in ISO/IEC 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. These control-oriented approaches apply to the use of cloud computing services, with additional cloud-specific considerations described in the ISO/IEC 27017 standard. Customers are advised to check if their cloud service provider conforms to ISO/IEC 27017 since it is specific to cloud computing.

In addition, ISO/IEC 27040:2015 [46] provides detailed technical guidance on planning, designing, documenting, and implementing data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage.

As highlighted in Step 1, there are a number of industry specific standards that focus on the protection of data including PCI-DSS, HIPAA, FERPA and FISMA. Cloud service customers in these industries should confirm their support by prospective cloud service providers.

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.
- *Transport Layer Security (TLS)* – for secure and private connections between two connected applications [47].

The standards above are all about the encryption of the data transport layer – in some cases, encryption of the data itself may be preferable, in which case, the encryption standards identified by FIPS 140-2 [48] are a useful guide.

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 database, a table, a column, a directory, a file. Which approach to take partly depends on the capabilities provided by the cloud service provider and partly depends 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.

- 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 (KMIP) [49] provides a standardized way to manage encryption keys across diverse infrastructures. Cloud service customers should inquire if their prospective cloud service providers support KMIP.

Step 5: Enforce policies for Protection of Personal Data

The protection of personal data, often referred to as "privacy," primarily relates to the collection, storage and use of personally identifiable information (PII). PII is any information that (a) can be used to identify the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person.

There are increasingly stringent laws and regulations in many countries which relate to PII. An example is the EU General Data Protection Regulation (GDPR) [50], passed into law in May 2016 and which applies to processing of PII of EU citizens. The increasing regulation is partly associated with a continuing series of major, high profile data breaches where sensitive PII of millions of people has been compromised. In addition to breaking laws and regulations, these breaches cause considerable reputational and financial damage to the organizations concerned.

Specific types of PII are also the subject of additional regulations and require more stringent controls applied to them – these are typically called "sensitive" PII and include items such as health records and financial data such as credit card information. Example regulations include HIPAA for health records in the USA and PCI-DSS for credit card data.

Any cloud service customer must give serious consideration to any PII that they intend to store or process within a cloud service. Typically, protection of PII 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. Use of techniques such as data minimization, pseudonymization and anonymization should be considered.

PII protection related issues should be dealt with in the cloud service 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 varies greatly depending on the nature of the cloud service involved. Examples include:

- For the provision of a virtual machine as part of an IaaS service, it is likely that the cloud service provider is unaware of the nature of the data which the customer stores or processes with the service and that most responsibilities lie with the customer, other than information security capabilities preventing theft, unauthorized access and unavailability.
- For an application that explicitly deals with PII, offered as a SaaS service by a cloud service provider, then it is expected that the provider is 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 relation to a SaaS offering.

There are a growing number of specifications and standards which relate to privacy and the protection of PII. One of the most significant for the use of cloud services is ISO/IEC 27018 – "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." As its title implies, it specifically covers public cloud services which are processing PII. ISO/IEC 27018 is based on the ISO/IEC 27001 information security management system standard and on the set of security controls found in the ISO/IEC 27002 standard. These standards provide the underlying security foundation for the processing of PII in a cloud service. ISO/IEC 27018 extends these standards with an additional set of controls based on the privacy principles of the ISO/IEC 29100 standard – *Privacy Framework*, which describes the processing of PII generally and which should itself also be consulted by cloud service customers:

- *Consent and choice*. An obligation on the cloud service provider to co-operate in relation to PII principal's rights.
- *Purpose legitimacy and specification*. PII should not be processed for any purpose not instructed by the cloud service customer (usually as defined in the cloud service agreement)
- *Collection limitation*. The limitation of the amount of PII collected to the minimum necessary for the capability being provided. Not specific to the use of cloud services.
- *Data minimization*. Secure erasure of temporary files.
- *Use, retention and disclosure*. PII disclosure notification.
- *Accuracy and quality*. Ensuring the accuracy and validity of any PII.
- *Openness, transparency and notice*. Disclosure of sub-contracted PII processing.
- *Individual participation and access*. The requirement to provide access to PII by the person to whom the information relates.
- *Accountability*. Notification of a data breach involving PII; retention period for administrative security policies and guidelines; PII return, transfer and disposal.
- *Information security*.
    - Requirement for confidentiality or non-disclosure agreements.
    - Restriction of the creation of hardcopy material.
    - Control and logging of data restoration.
    - Protecting data on storage media leaving the premises.
    - No use of unencrypted portable storage media and devices.
    - Encryption of PII transmitted over public data transmission networks.
    - Secure disposal of hardcopy materials.
    - Unique use of user IDs.
    - Keeping of records of authorized users.
    - User ID management.
    - Contract measures.
    - Control of sub-contracted PII processing.
    - Prevention of access to data on pre-used data storage space.
- *Privacy compliance*. Geographical location of PII; intended destination of PII.

ISO/IEC 27018 is explained further in a whitepaper by BSI [51].

Another useful standard relating to protection of PII is ISO/IEC 29151 – *Code of practice for personally identifiable information protection* [52] (in preparation) – aimed at the organization doing the collecting and processing of PII – typically the cloud service customer. 29151 is useful as a guide to the cloud service customer regarding their obligations with respect to the collection, storage and processing of PII.

Cloud service customers are strongly recommended to consider the PII processing principles and controls described by these standards in the creation of appropriate policies which govern their use of cloud services for PII processing, including the selection and verification of the public cloud services for this processing.

Of some significance in the EU GDPR are:

- The requirement to enable the "data subject" (person the PII relates to) to inspect and correct the PII relating to them
- The requirement to enable the data subject to obtain all their PII in a commonly used electronic data format

There is a need to examine the cloud service holding the PII to see what is necessary in order to satisfy these capabilities in a secure fashion. It may be necessary for the cloud service customer to create some custom interfaces – or the cloud service may have some existing interfaces that can fit the needs.

There are a growing number of cloud services that claim certification against the requirements of ISO/IEC 27018. Cloud service customers can use these certifications as an assurance that a cloud service provider is treating PII in an appropriate fashion.

Other approaches may also be helpful, such as the Cloud Security Alliance Privacy Level Agreement [53], which provides assurances for a given cloud service in relation to PII processing.

Step 6: Assess the security provisions for cloud applications

Organizations need to proactively protect their applications from external and internal threats throughout their entire life cycle, from design to implementation to production. Clearly defined security policies and processes are essential 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 reputation issues to both the cloud service provider and the cloud service customer, 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) provides some useful information about application security, including application security for cloud computing [54]. A multi-part ISO/IEC standard for application security is in preparation – 27034 - *Application Security* [55], with some parts already published and available. NIST SP 800-160 “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems” [56], currently being

developed, provides a set of security considerations in the context of systems engineering. These considerations are applicable to cloud-based applications and systems. There is also a joint publication by SAFECode and Cloud Security Alliance - *Practices for Secure Development of Cloud Applications.* [57]

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 should inquire about security capabilities available from the provider to help the customer secure their applications (e.g., "security as a service" and the provision of capabilities such as firewalls and user authentication).

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.

Ideally, for each application, the cloud service customer needs to establish security requirements and associated control objectives for the application and then map these requirements and controls to the application and the cloud service(s) it is deployed on. Each requirement and security control needs to be addressed either by the cloud service(s) or else implemented by the cloud service customer. If any requirements or controls cannot be addressed, then it is probably the case that the target cloud service(s) are inadequate in some way and alternative cloud services should be considered.

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 [58].

The NIST publication, *Guidelines on Firewalls and Firewall Policy* [59], 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.

Application security 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 [60]. For PaaS (and IaaS) applications, the OASIS TOSCA standard [61] 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.

An important area of consideration is testing applications for security vulnerabilities on a continuing basis. For any publicly exposed application, penetration testing should be a standard procedure. Useful documents relating to information security testing include NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment* [62] and the OWASP Testing Guide v4 [63].

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 customers plan to send and receive. Nevertheless, cloud service customers should expect a certain amount of external network perimeter and internal network separation measures from their cloud service providers.

Traditional perimeter-based network security controls are sometimes infeasible in cloud environments, and in some cases, a corporate firewall may give a false sense of security because there are many ways to get inside the corporate perimeter. Many services that were traditionally behind corporate firewalls may now be accessed directly from the Internet. While broad network access is an acceptable risk for many services, given that other controls are in place, some services may need to be protected by a secondary authentication layer such as a VPN, a bastion host, or a Software Defined Perimeter [i] solution.

There are several security standards that address network security requirements. In addition to the previously mentioned ISO/IEC 27001 and 27002 standards, the ISO/IEC 27033 standards [64] provide more 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/IEC 27001 certification. They are:

- 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) [65] and FIPS 200 (minimum security standards). FIPS 200 requires that controls be selected from NIST Special Publication 800-53 based on the system classification. While these standards and controls are only required for US federal government systems, other organizations also use them as a framework for their own security policies. The "System and Communications Protection" controls 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) 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 R4 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 [66].

When a cloud service customer evaluates the network security provided with a cloud service, many cloud service providers are now certified to a standard such as ISO/IEC 27001 or FedRAMP, or can provide a report on controls such as a SOC 2 report. It is important to perform an examination of the provider's documentation in order to ensure that network controls are in scope. Many reports or certifications only cover physical controls. If a cloud service provider has no attestation or certification that covers network security, customers should at least ensure that the provider has documented and tested processes for:

- Identity and access controls, for management of the network infrastructure
- Proper vulnerability management (patching) of the network infrastructure
- Appropriate network segmentation, which separates networks of different sensitivity levels (for example, where sensitive personal information is stored or processed) or different types (for example, a separate administration network)
- Traffic filtering, provided by traditional firewalls or web application firewalls
- Intrusion detection / prevention
- Mitigating the effects of DDoS attacks

- Logging and notification, so that systematic attacks can be reviewed
- Security Information and Event Management (SIEM), for holistic security event monitoring, management and response.

Step 8: Evaluate security controls on physical infrastructure and facilities

A complete security assessment includes consideration of the security of physical infrastructure and facilities. In the case of cloud computing, these considerations apply, but it usually the case that the infrastructure and facilities are owned and controlled by the cloud service provider. 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/IEC 27002 standard for physical and environmental security. Although ISO/IEC 27002 is not specific to cloud computing, its principles can still be usefully applied to the provision of cloud services. A brief description of the security controls contained in ISO/IEC 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 events 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. Controls may include background checks, security clearances, security awareness training, etc.
- *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/IEC 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, ISO/IEC 27017 deals with the application of the ISO/IEC 27002 specification to the use of cloud services and to the provision of cloud services. 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.

The ANSI/TIA-942 data center infrastructure standard [67] also provides information to planners regarding the protection of data center assets whether by means of physical security or fire prevention. Within its guidelines, it recognizes the importance of providing manageable access control to data center facilities and monitoring of people and their actions. Using the Uptime Institute Tier framework [68] as a basis, the ANSI/TIA-942 standard makes recommendations on improving the physical security of the data center. These include criteria such as video surveillance recording frame rates, access control levels and hardware, and site selection.

In addition to the above standards, there are regulations that apply to the physical data center facilities such as Sarbanes-Oxley, HIPAA and PCI-DSS. These regulations not only mandate that certain access restrictions be in place for data center facilities, but also require the reporting and auditing of access be provided—potentially in real time.

Step 9: Manage security terms in the cloud service agreement

Since cloud computing involves two or more organizations – the cloud service customer and one or more cloud service providers – it is critical to understand which party is responsible for what in terms of security. The cloud service agreement signed with each provider is where these responsibilities must be specified. In addition:

- The cloud service agreement should include rules about the reporting of security breaches.
- Service Level Agreements (SLAs) should specify metrics for measuring performance and effectiveness of information security management.

The CSCC provides guidance to cloud service customers about the agreements they will sign with providers in two key documents: the *Practical Guide to Cloud Service Agreements* [69] and the white paper entitled *Public Cloud Service Agreements: What to Expect and What to Negotiate* [70]. Both documents track the evolution of cloud service agreement terms as both customers and providers learn to better define their respective responsibilities.

Key Security Aspects to Consider

Security is one area where cloud service agreements have clearly evolved in recent years. However, there are still frequent ambiguities in the following areas.

Roles and Responsibilities. While the customer expects the provider to secure the resources (data and applications) rented by the customer, the provider also expects the customer not to introduce vulnerabilities in the form of unapproved users, uploading of viruses, etc. Cloud architectures that include federated identity or virtual private networks make the issue more complicated.

Each of the three cloud service models (IaaS, PaaS, or SaaS) results in a distinct allocation of responsibilities between the cloud service provider and customer.

Symmetrical Obligations. Most agreements impose stringent security obligations on the cloud service customer to protect the provider, and there are often serious consequences if these obligations are not met. However, it is important that the customer have recourse against unwarranted suspension of services, and the cloud service provider should accept a similar level of responsibility to protect the customer.

Metrics. Metrics related to the performance and effectiveness of information security management should be part of the SLA. To provide a necessary baseline, customers should understand and document their prior in-house metrics, what changes are acceptable or not upon migration to a cloud service, and where a provider may use different (potentially incompatible) metrics. Refer to the following resources for specific information on security metrics:

- ISO/IEC 27004, *Information Security Management Measurement* [71]
- ISO/IEC 19086, *Cloud Computing Service Level Agreement (SLA) Framework and Technology* (in four parts, all in preparation) [72]
- NIST Special Publication 800-55 Rev. 1, *Performance Measurement Guide for Information Security* [73]
- CIS Consensus Security Metrics v1.1.0 [74]

Notification. Providers must notify customers in a timely manner of the occurrence of any breach of their system. The provider should include in the notification any specific pertinent information that can help the customer protect itself.

Recovery. In the case of a successful attack, the cloud service agreement should specify the measures that the provider will take to stop the security breach, restore access to the service as quickly as

possible, investigate the accident and make appropriate improvements, and keep the customer informed throughout the process.

Compensation. Typical cloud service agreements limit compensation after any service interruption, including one related to security, to the rental price of the lost hours of service, which is a small fraction of the actual loss suffered by the customers. Barring a higher commitment from the provider, the customer should investigate the availability of cyberattack/data breach insurance policies.

Subcontractors. If the cloud service provider uses a third party to provide some of the services it delivers (for example, if a SaaS provider relies on a separate IaaS provider for storage or backup), the security obligations of the subcontractor must be at least equal to those of the primary provider.

Personnel. The employees of the cloud service provider who have privilege access to the customer's information (including files, databases, passwords, backup media, etc.) as a result of their normal duties should be vetted to the extent permitted by employment laws.

Facilities. The physical security of the location containing the computing and storage resources (including logs and backups) is as important as cybersecurity. Cloud service providers should have appropriate controls in place for physical security, with a supporting certification such as ISO/IEC 27001.

Data Protection and Data Residency. While the concepts of data protection (or privacy) and data residency are distinct from security, they overlap with it, and the same paragraphs of a cloud service agreement may address all three concerns rather indistinctly. Lack of protection of personally identifiable information (PII), or lack of awareness and control of where data is located, may become security issues if they facilitate access by unauthorized parties. The customer must understand whether such an impact exists, given the nature of the data it stores in the cloud.

Certification to a suitable standard like ISO/IEC 27018, *Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors* is preferable. Otherwise, a *data compliance report* should be required from the cloud provider, reflecting the strength or weakness of controls, services, and mechanisms supported by the provider in all security domains. Alternatively, the provider should obtain an independent certification of the cloud service against one of the data protection standards.

Standards

Established standards can help cloud service customers and providers agree on the security practices to adopt and monitor. These are likely to include ISO/IEC 27017, *Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services*. In certain domains (finance, health, government, defense, etc.) there may be additional standards to be followed.

In the area of software development (which is relevant to Software as a Service), there are norms for secure coding that should be followed by the SaaS provider, or by its development contractors, to decrease the risk of vulnerabilities. One of those norms is the Common Weakness Enumeration project, supported by a number of commercial and open-source assessment tools [75].

The use of such standards by cloud service providers, including certifications they have obtained, should be transparent to the customers.

In terms of security metrics, several efforts are now underway or completed, but they do not yet amount to a unified approach:

- The Cloud Security Alliance (CSA) has established a Security, Trust and Assurance Registry (STAR) [76] to make accessible to customers the security controls provided by various cloud service providers.
- In the financial industry, the Payment Card Industry Data Security Standard (PCI DSS) is commonly used to assess providers.
- For U.S. Government agencies, the FedRAMP program, established by the General Services Administration (GSA) and based on NIST SP800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) is generally used. The GSA has documented areas of concern about cloud security requirements, which may require additional contract clauses[2]. The guidance details the security terms at the security controls level and provides sample template language that can be used to document technical requirements. While intended for the government, the document mirrors commercial enterprises' concerns and can therefore be leveraged more broadly. Notably, however, this program has come under heavy criticism for the long and bureaucratic process required to qualify. A "FedRAMP Fast Forward" industry advocacy group has been formed to propose changes.
- The U.S. Defense Information Systems Agency (DISA) has published a Department of Defense Cloud Computing Security Requirements Guide. [77]
- The TM Forum, a global association of digital businesses, has published TR178 version 2, "Enabling End-to-End Cloud SLA Management." [78] The report provides a set of common approaches for two parties to determine their cloud SLA, define what to measure, the thresholds 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.
- The European Network and Information Security Agency (ENISA) has published "Procure Secure: A guide to monitoring of security service levels in cloud contracts" [79], which lists key requirements that a cloud service provider should meet in terms of security protocols. It includes a cloud security monitoring framework that covers what to measure, how to collect the data, how the customer can independently monitor security features, how to set reporting and alerting thresholds, and who is responsible for what. The specific metrics covered in the guide include: service availability, incident response, service elasticity and load tolerance, data life-cycle management, technical compliance and vulnerability management, change management, data isolation, and log management and forensics. While not a standard, customers are advised to leverage the guidance provided in this document.

Note that one-off or periodic provider assessments, such as ISO/IEC 2700x, SSAE 16 or ISAE 3402, assure that a certain set of controls and procedures was in place at a given point in time, but they do not provide real-time information, regular checkpoints or threshold-based alerts. Therefore, they must be

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

augmented by additional feedback in the intervals between assessments. For example, the CSA STAR allows progressive degrees of assurance based on self-assessment, discrete third-party assessments, or continuous monitoring.

There are many additional resources that contain valuable guidance on security metrics, but which are not cloud-specific. They include ISO/IEC 27004:2009, NIST Special Publication (SP) 800-55 Rev.1, Performance Measurement Guide for Information Security, and CIS Consensus Security Metrics v1.1.0.

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 Agreements*."

From a security perspective, it is important that once the customer has completed the exit process, "reversibility" or "the right to be forgotten" is achieved – that is, 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 (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. Essentially, cloud service providers should provide transition assistance to allow customers to move services internally or to a new cloud service provider.

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.

The ISO/IEC 19086 standard on Cloud Computing Service Level Agreement Framework deals with elements relating to the exit process that appear in the cloud service agreement, although it is still in preparation at this time. 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 service agreement.

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/IEC 20000, SSAE 16 or ITIL depending on type of workload • Ensure CSP conforms to the ISO/IEC 27001 and ISO/IEC 27002 standards for information systems security • Ensure CSP conforms to ISO/IEC 27017 & ISO/IEC 27018 standards (ISO/IEC 27018 is applicable when PII is present) • Consider additional standards when regulatory or industry mandates (e.g., FERPA, HIPAA) are applicable	• Insist on ISO/IEC 27001 certification • Seek ISO/IEC 27017 or equivalent certification • For cloud services with impact on financial activities seek SSAE 16 certification • Regulatory and industry certifications as applicable
Step 2: Audit operational and business processes	• Ensure CSP complies with SSAE 16 for cloud services with financial activities • Ensure CSP conforms to the ISO/IEC 27000 series of standards	• Insist on ISO/IEC 27001 certification • Seek ISO/IEC 27017 or equivalent certification • 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/IEC 27001 certification which provides a *framework* to ensure cloud service provider has proper controls in place to manage people, roles and identities • Seek ISO/IEC 27017 or equivalent certification

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 /IEC 27001 certification which provides a *framework* to ensure cloud service provider has proper controls in place to protect customer data and information • Seek ISO/IEC 27017 or equivalent certification
Step 5: Enforce privacy policies	• Ensure CSP supports EU-US Privacy Shield • Ensure CSP conforms with ISO/IEC 27018	• Leverage commercial certification offerings, such as the EU-US Privacy Shield certification program • Seek ISO/IEC 27018 or equivalent certification
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	• Insist on ISO/IEC 27001 certification which provides a *framework* to ensure cloud service provider has proper controls in place to protect cloud applications • Seek ISO/IEC 27017 or equivalent certification
Step 7: Ensure cloud networks and connections are secure	• Ensure CSP supports the ISO/IEC 27033 or FIPS199/200 standards	• Insist on ISO/IEC 27001 certification , FedRAMP certification, or a SOC2 report that covers logical network controls
Step 8: Evaluate security controls on physical infrastructure & facilities	• Ensure CSP conforms to the ISO/IEC 27002 standard for information systems security • Ensure CSP conforms to ISO/IEC 27017 & ISO/IEC 27018 standards	• Insist on ISO/IEC 27001 certification • Seek ISO/IEC 27017 or equivalent certification

Step 9: Manage security terms in the cloud service agreement	• Track the emerging ISO/IEC 19086 standard • On security metrics, refer to ISO/IEC 27004:2009, TM Forum TR 178, NIST Special Publication 800-55, CIS Consensus Security Metrics V1.1.0, and ENISA Procure Secure • For SaaS CSPs, make sure the developers use the CWE list to remove vulnerabilities • Verify the CSP's presence in the CSA STAR registry • For payment card services, use PCI DSS to assess the CSP • Government customers should look at implementing the FedRAMP program	• For periodic assessments, insist on ISO/IEC 27001 certification and seek ISO/IEC 27017 or equivalent certification • For cloud services with impact on financial activities seek SSAE 16 certification (periodic assessment) • For personal data protection, seek ISO/IEC 27018 or equivalent certification
Step 10: Understand the security requirements of the exit process	• The emerging ISO/IEC 19086 standard contains language on the exit process	• Currently no certifications in this space

Works Cited

[1] Cloud Standards Customer Council: *Security for Cloud Computing: 10 Steps to Ensure Success* http://www.cloud-council.org/deliverables/security-for-cloud-computing-10-steps-to-ensure-success.htm

[2] ISO/IEC 38500: http://www.38500.org/

[3] COBIT: http://www.isaca.org/COBIT/Pages/default.aspx

[4] ITIL: http://www.itil-officialsite.com/

[5] ISO/IEC 20000: http://en.wikipedia.org/wiki/ISO/IEC_20000

[6] SSAE 16: http://ssae16.com/

[7] NIST Cybersecurity Framework: http://www.nist.gov/cyberframework/

[8] CSA Cloud Controls Matrix: https://cloudsecurityalliance.org/group/cloud-controls-matrix/

[9] HIPAA: http://www.hhs.gov/ocr/privacy/

[10] PCI-DSS: https://www.pcisecuritystandards.org/security_standards/

[11] FERPA: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[12] FedRAMP: http://www.fedramp.gov

[13] NIST FIPS PUB 200 (2006): Minimum Security Requirements for Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[14] FISMA: http://csrc.nist.gov/groups/SMA/fisma/index.htmlfor

[15] HSPD-12: https://www.dhs.gov/homeland-security-presidential-directive-12

[16] NIST Special Publication 800-53: http://csrc.nist.gov/publications/PubsSPs.html

[17] EU-US Privacy Shield: https://www.commerce.gov/privacyshield

[18] NIS Directive: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[19] ISO/IEC 27000-series: http://www.27000.org/

[20] ISO/IEC 27017, *Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services* http://www.iso.org/iso/catalogue_detail?csnumber=43757

[21] ISO/IEC 27018 (2014). *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

[22] ISO/IEC 29100 (2011). *Privacy Framework* http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123

[23] SEC Rule 613: https://www.sec.gov/divisions/marketreg/rule613-info.htm

[24] PIPEDA Act: https://www.priv.gc.ca/leg_c/r_o_p_e.asp

[25] OASIS Privacy Management Reference Model (PMRM): https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm

[26] OASIS Privacy by Design for Software Engineers (PbD-SE): https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pbd-se

[27] 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

[28] CADF: http://www.dmtf.org/standards/cadf

[29] pyCADF: https://pypi.python.org/pypi/pycadf

[30] Gartner (2015): *Market Guide for Cloud Access Security Brokers*: http://www.gartner.com/document/3155127?ref=AutoReg

[31] HL7 FHIR: https://www.hl7.org/fhir/

[32] US Securities and Exchange Commission (2016): *SEC Seeks Public Comment on Plan to Create a Consolidated Audit Trail*: https://www.sec.gov/news/pressrelease/2016-77.html

[33] NISTIR 8006, *NIST Cloud Computing Forensic Science Challenges* http://www.nist.gov/itl/itl-cloud-computing-forensic-science.cfm

[34] NIST SP 800-92, *Guide to Computer Security Log Management* http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[35] LDAP: http://tools.ietf.org/html/rfc4510

[36] SAML 2.0: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[37] OAuth 2.0: http://oauth.net/2/

[38] WS-Federation: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

[39] OpenID Connect: http://openid.net/connect/

[40] SCIM: http://datatracker.ietf.org/wg/scim/charter/

[41] ADFS2: http://social.technet.microsoft.com/wiki/contents/articles/2735.ad-fs-2-0-content-map.aspx

[42] XACML: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[43] PKCS: https://tools.ietf.org/rfc/rfc3447.txt

[44] X.509: http://www.ietf.org/rfc/rfc3280.txt

[45] OpenPGP: https://www.ietf.org/rfc/rfc4880.txt

[46] ISO/IEC 27040: http://www.iso.org/iso/catalogue_detail?csnumber=44404

[47] Transport Layer Security (TLS) Protocol: https://tools.ietf.org/html/rfc5246

[48] US FIPS 140-2: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[49] KMIP: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

[50] Regulation 2016/679 of the European Parliament and of the Council: EU *General Data Protection Regulation* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[51] BSI (2015). *Whitepaper: ISO/IEC 27018 – Safeguarding Personal Information in the Cloud* http://www.bsigroup.com/Documents/iso-iec-27018/ISOIEC-27018-Safeguarding-information-in-the-cloud-whitepaperDec2015.pdf

[52] ISO/IEC 29151 (In preparation). *Code of practice for personally identifiable information protection* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62726

[53] CSA Privacy Level Agreement V2: *A Compliance Tool for Providing Cloud Services in the European Union* https://downloads.cloudsecurityalliance.org/assets/research/pla/downloads/2015_05_28_PrivacyLevelAgreementV2_FINAL_JRS5.pdf

[54] OWASP: https://www.owasp.org/index.php/Main_Page

[55] ISO/IEC 27034 Multi-part standard (Various dates, some parts still in preparation)
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44378
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=55582
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=55583
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67741
http://www.iso.org/iso/catalogue_detail.htm?csnumber=55585
http://www.iso.org/iso/catalogue_detail.htm?csnumber=60804
http://www.iso.org/iso/catalogue_detail.htm?csnumber=66229

[56] NIST Special Publication 800-160 (draft):
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

[57] SAFECode and Cloud Security Alliance (2013): *Practices for Secure Development of Cloud Applications*:
http://www.safecode.org/publication/SAFECode_CSA_Cloud_Final1213.pdf

[58] OWASP Top 10 Application Vulnerabilities: https://www.owasp.org/index.php/Top_10_2013-Top_10

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

[60] OVF 2.0: http://dmtf.org/standards/ovf

[61] TOSCA: http://docs.oasis-open.org/tosca/TOSCA/v1.0/cs01/TOSCA-v1.0-cs01.html

[62] NIST Special Publication 800-155 (2008). *Technical Guide to Information Security Testing and Assessment*
http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[63] OWASP (2016). *OWASP Testing Guide v4*
https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

[64] ISO/IEC 27033: http://www.iso27001security.com/html/27033.html

[65] NIST FIPS PUB 199 (2004): *Standards for Security Categorization of Federal Information and Information Systems*: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[66] FEDRamp FAQ: http://www.gsa.gov/portal/content/118875

[67] ANSI/TIA 942: http://www.tia-942.org/

[68] Uptime Institute Tier Framework: https://uptimeinstitute.com/tiers

[69] Cloud Standards Customer Council: *Practical Guide to Cloud Service Agreements*
http://www.cloud-council.org/deliverables/practical-guide-to-cloud-service-agreements.htm

[70] Cloud Standards Customer Council: *Public Cloud Service Agreements: What to Expect and What to Negotiate*
http://www.cloud-council.org/deliverables/public-cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

[71] ISO/IEC 27004:2009, *Information Security Management Measurement*
http://www.iso.org/iso/catalogue_detail.htm?csnumber=42106

[72] ISO/IEC 19086, *Cloud computing Service Level Agreement Framework*. Multipart (in preparation):
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67545
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67546
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67547
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242

[73] NIST SP 800-55 Rev. 1: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

[74] CIS Consensus Security Metrics:
http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.metrics.110

[75] MITRE *Common Weakness Enumeration:* http://cwe.mitre.org

[76] CSA STAR: https://cloudsecurityalliance.org/star/

[77] DISA *TR178 version 2, Enabling End-to-End Cloud SLA Management*:
http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf

[78] TM Forum *TR178 version 2, Enabling End-to-End Cloud SLA Management*:
https://www.tmforum.org/resources/technical-report-best-practice/tr178-enabling-end-to-end-cloud-sla-management-v2-0-2/

[79] ENISA: *Procure Secure: A guide to monitoring of security service levels in cloud contracts*
https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

Additional References

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

- Cloud Security Alliance. *Software Defined Perimeter Working Group SDP Specification 1.0*
  https://cloudsecurityalliance.org/download/sdp-specification-v1-0/

- Cyber Security and Information Systems Information Analysis Center (CSIAC).
  https://www.csiac.org/

- 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

- 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

