



BUILDING CUSTOMER TRUST IN CLOUD COMPUTING WITH TRANSPARENT SECURITY

White Paper
November 2009

Abstract

Potential users of cloud services often fear that cloud providers' governance is not yet mature enough to consistently and reliably protect their data. As the trend toward cloud-based services continues to grow, it has become clear that one of the key barriers to rapid adoption of enterprise cloud services is customer concern over data security (confidentiality, integrity, and availability). This paper introduces the concept of transparent security and makes the case that the intelligent disclosure of security design, practices, and procedures can help improve customer confidence while protecting critical security features and data, thereby improving overall governance. Readers will learn how transparent security can help prospective cloud computing customers make informed decisions based on clear facts. For the purpose of discussion and debate, a model leveraging the ISO 27000 series standards is presented as a commonly understood framework for disclosure.

Table of Contents

Introduction.....	3
Governance, Security, and Transparency.....	5
Transparency as a Basis For Informed Decision Making	8
What is Transparent Security?	9
Transparent Security Principles	10
Standards as a Means to Transparency and Assurance.....	11
Security Control Objectives.....	12
Primary Benefits of a Standards-based Approach.....	13
Conclusion	14
For More Information	15
Appendix A—NIST Definition of Cloud Computing.....	16
Definition of Cloud Computing.....	16
Essential Characteristics.....	16
Service Models	17
Deployment Models.....	18
Appendix B—Overview of ISMS	19
Step 1—Establish the ISMS	19
Step 2—Implement and Operate the ISMS	20
Step 3—Monitor and Review the ISMS	20
Step 4—Maintain and Improve the ISMS	21
Appendix C—Leveraging ISO 27002 as a Transparency Framework	22

Chapter 1

Introduction

Cloud computing promises greater flexibility in business planning along with significant cost savings by leveraging economies of scale in the IT infrastructure. It also offers a simplified capital and expenditure model for compute services as well as increased agility for cloud customers who can easily expand and contract their IT services as business needs change. Yet many enterprise customers are hesitant to buy into cloud offerings due to governance and security concerns. Many potential users of cloud services lack confidence that cloud providers will adequately protect their data and deliver safe and predictable computing results¹.

As the most recent evolution in computing architecture, cloud computing is simply a further extension of the distributed computing model. Its key characteristics, such as multi-tenancy, massive scalability, elasticity, pay-per-use, and self-provisioned resources, are also those that may create new governance challenges for both cloud providers and their customers². Today's cloud computing solutions may also provide a computing infrastructure and related services in which the consumer has limited or no control over the cloud infrastructure³, thus creating a greater need for customers to assess and control risk.

Customers must trust the security and governance of the cloud environment in order to have confidence that their data will be protected and its integrity maintained. Many potential cloud customers are also looking for some level of assurance that appropriate security measures are indeed being properly implemented in the daily operations of the cloud infrastructure. These potential customers want to make informed decisions about whether their data will be sufficiently protected and whether they will be able to comply with specific regulations when using a cloud service. In short, they want the security of the cloud offering to be transparent. Transparent security would entail cloud providers disclosing adequate information about their security policies, design, and practices, including disclosing relevant security measures in daily operations.

One of the best ways to help customers understand the cloud security environment is for cloud service providers to develop a common way to disclose relevant practices, principles and capabilities using a common framework. Cloud providers and customers can create a governance framework by leveraging the existing ISO 27001 and ISO 27002 standards⁴ to provide an approach that can naturally be applied in a cloud environment.

¹ Tim Mather, Subra Kumaraswamy, and Shahed Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance* (O'Reilly Media, Inc., 2009), p 244.

² *IBID*, p 7-10.

³ Appendix A describes the various cloud service and deployment models and the level of control that the consumer has in each model.

⁴ More information about ISO 27001 and ISO 27002 is available at www.iso.org.

Together, ISO 27001 and 27002 provide requirements for creating controls to implement and use security best practices. These practices are specific enough that they can be audited to provide assurance that security design, technologies, and procedures are indeed being implemented in conformance with the standards. More importantly, they provide a common framework for discussing, analyzing and planning how best to leverage cloud offerings to meet business and risk requirements for both the cloud provider and the cloud customer.

Chapter 2

Governance, Security, and Transparency

Modern governance and information security require a broad-based approach that addresses all aspects of server processing, data storage, and communications in today's distributed computing environments. Vendors, service providers, and others routinely make claims about the security of their products or services. However, experience shows that threats and security vulnerabilities usually exist, and that claims about security are frequently not backed by sufficient details about what the IT environment actually protects and why that protection should be considered sufficient.

Transparency, if it exists at all, is often an afterthought. While some IT service providers may produce a certification or merely disclose that they possess such a certification document, some cloud service providers offer no assurances at all. They may simply offer legal terms and conditions that leave the user with "as is" non-assurances regarding information protection while also attempting to transfer all liability to the customer. This is obviously a losing situation for customers and one that could potentially affect a provider's business. Relevant details that could help customers determine whether a cloud-based service offering is a fit with their governance strategies and security requirements are scant or often absent in the current marketplace. As a result only unwary, small, or risk-taking organizations tend to dive into these sorts of cloud computing offerings. Governance officials at these organizations are torn between adopting new business models and taking unquantifiable risks. This culture of non-transparency can change, however.

Governance, information security, and transparency are inter-related concepts. Together, they can turn an otherwise confusing and shifting information-based commercial landscape into a pragmatic framework. "Governance" in this context is the superset of security, privacy, and regulatory requirements, and commercial imperatives that can help an organization assess risk, manage day-to-day processes, and move forward with some degree of control over assets and ethics. "Information security" is the collection of people, processes, and technology that help an organization provide confidentiality, integrity, and availability for its precious information assets. Finally, in this context, "transparency" is viewed as revealing enough information to enable reasonable strategic business decisions while respecting an organization's need for confidentiality.

Extensive disclosure about governance and security practices goes against the grain of conventional thinking, where practices, procedures, and perspectives relating to security have typically remained secret, or at least confidential, within a service provider. Historically, this may have been acceptable to customers, but with the maturity levels of today's customer security teams and programs, this is no longer the case. Much of the information that was historically considered "confidential" is now

common knowledge and should be shared with customers. Cloud providers must understand this point and adapt accordingly by providing customers more information about the security provided in their services, hence becoming more transparent.

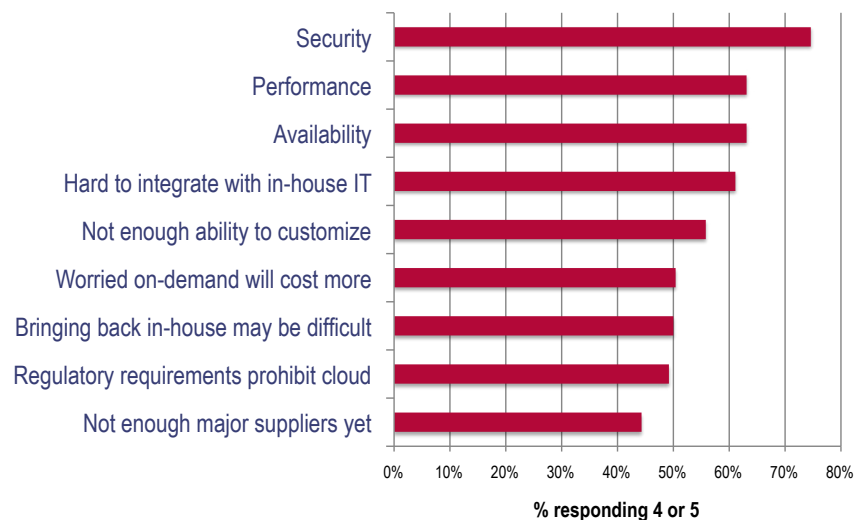
Correct deployment and governance over conditions can enable cloud service providers to achieve a high degree of security along with adequate protection of customer data. Nonetheless, the lack of transparency to cloud users can create governance challenges and, often as important, customer satisfaction or reputation problems for both cloud providers and their customers. The technical, legal, and personnel issues related to operating a cloud environment can be quite different from traditional IT environments and are often complex. Users of cloud services may need to maintain traditional and comprehensive controls to meet all of their security, integrity, and availability requirements. For example, if a user desires confidentiality mechanisms to prevent the disclosure of information, but the cloud provider does not offer such a mechanism, then the user must take responsibility for its implementation.

In light of the issues described above, and the fact that cloud services are still a relatively new phenomenon, cloud users want to understand the details of the security environments of cloud providers. They may want assurances that their information will be protected in a way that will enable expected service levels and meet their data security requirements.

As shown in Figure 1, an enterprise panel survey by IDC in 2008 showed that security was ranked as the biggest challenge or issue with cloud computing.

Q: Rate the **challenges/issues ascribed to the ‘cloud/on-demand’ model**

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008, n=244

Figure 1. A 2008 IDC survey showed security as the top issue in cloud computing.

Before putting their enterprise data into a cloud environment, organizations must be confident that the cloud provider is using appropriate technologies, practices, and processes to deliver accurate, reliable, and predictable results for storing, transmitting, and manipulating data. Some customers also fear that security is not practiced at an adequate level to satisfy their own compliance and governance challenges.

These fears can be addressed through the principles and practices of transparent security on the part of the cloud provider as well as assurances about the security of the cloud provider's implementation and operating procedures. Chapter 3 covers some specific transparent security principles recommended by Sun.

A solid security design and implementation coupled with transparency about security can also present an image of thought leadership to the marketplace. Getting security right in the beginning (and thinking through how it will be made transparent) can help improve market acceptance, thereby leading to more rapid adoption.

Chapter 3

Transparency as a Basis For Informed Decision Making

Cloud providers can win customer confidence or trust by being more transparent with customers, providing them with sufficient information to make informed decisions about how their data will be protected and, if necessary, how compliance with specific regulations can be met. This is the business imperative often called “trust” in the commercial context. In particular, cloud computing customers want to be able to trust not only the accuracy and reliability of the computing results delivered by the cloud provider, but also the integrity and confidentiality of their data. In short, cloud providers must produce enough reliable information to allow customers and users of services to make reasonable informed decisions. It is generally acceptable for providers to not address all customer security requirements in services that are used by multiple customers. However, in order to help effectively manage customer expectations, providers should be transparent about what has been implemented.

Looking back to the early days of the Web privacy movement, one can see a parallel to what is happening today in cloud computing. When Web privacy first began getting a lot of attention, privacy practices varied widely throughout the industry. There were many ways in which information could be collected and used for good or ill without the knowledge of the data subject. Users had little insight into the practices and procedures of Web site owners. Furthermore, fair processing principles, laws and regulations were often far beyond the typical users’ experience or expertise.

Although there is some debate about the efficacy of privacy policies and practices as a means to protect private information, both Web service providers and users have a far greater depth of dialog and understanding today than they did ten years ago. Practices, procedures, and new technologies have continued to emerge as a result of the increased demand for transparency in data processing. A similar analogy can be drawn for the emergence and prevalence of distributed computing modes, including cloud computing.

Cloud customers need some assurance that their data will be properly protected if processed by cloud providers. In situations where a vendor, such as an outsourcing firm or application service provider, had custody or other fiduciary responsibility over data, non-disclosure agreements, due diligence and elaborate, heavily negotiated contracts would be deployed as a proxy for trust. Where these techniques are unavailable because they are not offered or not feasible in a slim margin business model, assurance can be provided by releasing some details about how the services work, the security methods that are being implemented, and how they can be verified. Otherwise, customers are left to somehow tolerate an unexplored and largely unknown risk.

A middle ground position today may be to allow for the presumption that if security standards are followed, a third party audit of the security environment can verify that the design, practices, and policies are indeed implemented as claimed. This technique can give some customer confidence about the services and security capabilities. It also allows the providers to spend more time and resources operating and improving the services themselves, rather than spending that time addressing individual customer concerns about security in the services.

What is Transparent Security?

Transparent security can be defined as appropriate disclosure of the governance aspects of security design, policies, and practices. A security policy explains the high level approach to security and typically represents an organization's executive management position on security and risk. Making the policy publicly available is a good step toward transparent security, but does not go far enough to build customer confidence.

Taking transparency to the next level requires disclosing how the policy is being implemented. For example, the policy might state that user data will be protected from unauthorized access both while being stored in the cloud and while in transit. The security design might then go into more detail by specifying that file-level encryption will be used along with an identity management implementation that restricts access to stored data. Security practices might also drill down further, describing the processes for proper management of encryption keys. The actual implementation would then choose a specific encryption algorithm such as Advanced Encryption Standard (AES), and a specific identity management solution such as Sun™ Identity Manager software.

Much of the information in this example scenario could be disclosed to the outside world without giving hackers undue advantage or creating a security risk for the provider and customers. For example, a hacker would not necessarily gain additional insight into how to crack the encrypted files just by knowing that the encryption algorithm was based on AES. Similarly, the perpetrators of security fraud schemes generally know the basics about security architecture, so it would not be any help to them to find out that a firewall was in place. Disclosing an architecture diagram that spells out exactly where the firewalls exist inside the cloud could, however, give attackers an edge and thus would not be wise.

On the other hand, disclosing general information about security policies, design, and practices might help a potential customer feel more confident about the cloud provider's capacity for protecting information. While, it may be best to disclose as much information as possible, there is a natural tendency to keep some information confidential simply because it has always been done this way. This default tendency to not disclose information should be eliminated unless there is a tangible risk identified and keeping secrecy can be expected to maintain or decrease risk.

Transparent Security Principles

The following transparent security principles help identify the types of information that should and should not be disclosed. The following conditions are examples of when disclosure is recommended:

- **Principle 1— Disclosure of common security policies and practices.** Common security features such as the use of firewalls and encryption of data in transmission or at rest should be disclosed because they are considered basic security features that most security people would expect to be in place anyway.
- **Principle 2— Disclosure when mandated.** When disclosure is imperative due to a legal or regulatory requirement, then this disclosure must be performed.
- **Principle 3— Security architecture.** Security architectural details that may either help or hinder security management should be disclosed. For example, the implementation of secure by default configuration should be disclosed. However, if these types of details also create a security risk as described in other items below, disclosure would not be appropriate.
- **Principle 4— Governance.** Governance responsibilities of the customer versus those of the cloud provider should be clearly articulated so that customers are clear on what they must do themselves to help protect their data.

The following are additional principles in which disclosure is NOT recommended:

- **Principle 5— Do not exacerbate risks.** Do not disclose anything that could create risk to the datacenter or to the integrity of data stored in the datacenter.
- **Principle 6— Do no harm.** If disclosure could create potential harm for a customer or partner, it should be avoided. For example, identifying a specific customer by name or giving out information that would allow the customer to be identified could pose a privacy threat as well a potential breach of contract with customers.
- **Principle 7— Manage liability.** Avoid disclosures that could create undue liability for the cloud provider. For example, promising a level of security that might prove difficult to achieve would create a potential liability, possibly resulting in a claim of damages by a customer.
- **Principle 8— Withholding information when mandated.** If disclosure would result in breach of a legal or regulatory requirement, it should be avoided. For example, in the European Union, the provider can disclose the location of data, but cannot lawfully transfer certain types of personally identifiable information outside the borders of the European Union.

Chapter 4

Standards as a Means to Transparency and Assurance

An effective vehicle for achieving transparency and enabling assurance is through the use of structured governance and security frameworks. One such security framework is an Information Security Management System (ISMS) as defined in the ISO 27001 standard. (An overview of an ISMS can be found in Appendix B.) Architecting a cloud computing environment that is guided by existing analogous industry standards and practicing “Transparent Security Principles” can greatly enhance customer confidence and can help promote better decision making and well-reasoned information asset planning. “Trust me, I am Brand X” cannot be the end of the transparency discussion. Instead, timely, clear and relevant information that allows for decision making as dynamic as new technology platforms and business plans should be provided.

A comprehensive framework such as an ISMS as a part of a greater governance strategy is critical for addressing security and compliance and can provide a reliable means for enabling assurance. Furthermore, leveraging industry standards that can be potentially verified by a third party auditor gives customers additional chances to understand the risk of the cloud computing environment and how it may fit in with current IT resources. Thus standards can provide an important baseline upon which cloud providers and customers can measure results and achieve assurance.

In particular, ISO 27001 and ISO 27002 are good starting points from which to build a foundation for transparent security. As internationally accepted security standards for IT environments, ISO 27001 and 27002 together provide a framework, as represented by an ISMS and the associated security control objectives, to demonstrate how to maintain security best practices and how to implement a managed approach to business information protection, including risk and compliance. Although there are certainly a number of efforts underway to create a “cloud specific” standard, the ISO 27001 and 27002 standards that cover IT security today provide an approach that is compatible with cloud environments because these standards cover the basic categories of lifecycle controls found in every other standard. They are also well understood by security and governance communities and auditors, and they allow for some degree of flexibility to meet the realities of cloud environments. Finally, the ISO 27000 series contemplates the use of people, process and technology as equally important components for implementing controls rather than favoring one of these critical areas over another.

Most importantly, following the guidance of the ISO 27001 standard and using an ISMS is the foundation for addressing security from both an IT systems and governance perspective. ISO 27001 certification is evidence that the cloud provider has implemented an ISMS that covers everything from a high level security policy to specific control mechanisms for securing, monitoring, and managing the IT systems. The details of the specific security controls are noted in the ISO 27002 standard as security control objectives.

Security Control Objectives

The ISO 27002 standard describes a set of security control objectives that reflect systemic security principles. These principles cover granular topics such as self-preservation, defense in depth, least privilege, compartmentalization and proportionality. In general, security control objectives are used collectively to create a comprehensive security architecture, security processes and practices. These are sustained over time via the implementation and use of an ISMS. There are eleven primary focus areas for security control objectives:

- Security policy
- Organizing information security
- Asset management
- Human Resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Due to the dynamic nature of cloud environments and the distributed nature of data, it is necessary to have a comprehensive security framework based upon security control objectives that are flexible and responsive to one's particular security and compliance requirements. These security control objectives, when used within the context of a cloud environment, allow one to manage risk, implement compensating control, and address compliance requirements. Collectively, these allow customers to create a path to certification that will establish a level of assurance appropriate to a particular environment.

Appendix C provides an overview of the security control objective focus areas as defined in ISO 27002 and identifies the primary ways that Sun recommends a cloud service provider to be transparent about these controls. It provides guidance for how to evaluate the level of transparency in a cloud and further discusses what specific information should be released for each security control objective focus area as well as why Sun feels it is important to disclose that information.

Primary Benefits of a Standards-based Approach

Overall, the primary benefits of using ISO 27001, ISO 27002, and related standards as a means to increase transparency and assurance include:

- Provides credibility due to the wide acceptance of these international standards
- Offers a comprehensive set of security best practices across data, systems, and procedures. As such, it can help the organization to formalize all operational controls and provide a governance infrastructure for design and implementation of a coherent security architecture.
- Helps increase customer trust by providing a framework that can be independently certified and audited by an external and recognized international certification body. Outside verification helps the organization attest to the sufficiency of controls and demonstrate their commitment to the high standards of security and governance.
- Simplifies implementation of compliance efforts since an ISMS is structured to be utilized in most IT environments.
- Helps ensure appropriate levels of confidentiality, integrity and accountability that are also needed for other compliance regimes.
- Allows the provider to better understand and manage customer expectations related to security of services that are provided.
- Potentially reduces the amount of time and resources spent by both providers and customers related to compliance assurance and risk management activities.

Chapter 5

Conclusion

Cloud users cannot justify turning over control of their data to a cloud provider based solely on economic savings and increased agility. They must also have some degree of confidence that their data will be properly protected and that IT services will be reliably, accurately, and predictably delivered. Cloud providers can build customer trust by leveraging the ISO 27001 and 27002 information security standards and by following a set of “Transparent Security Principles.” Customers and users of cloud services, in turn, can begin to develop a more reasonable risk profile and make better, more informed choices.

Transparent security as described in this paper can create a competitive advantage that makes the cloud offering more attractive to users. Potential benefits include:

- Improved trust, resulting in faster adoption of cloud services.
- Increased security maturity as needed to enable compliance.
- Reduced risk of security vulnerabilities.
- Increased awareness of security gaps through the process of implementing security principles and best practices as noted in the ISO 27001 and 27002 standards.
- Reduced time and resources to address compliance assurance activities of customers.

Much like the many levels of availability that information systems can offer, there are many levels of security for an IT environment. Security should always be balanced against cost, risk, and convenience of use. Cloud customers want cloud security that is sufficient to enable them to entrust their data to the cloud provider without incurring too much cost or making user access inconvenient.

One of the biggest promises of cloud computing has been an ability to deliver a low cost information resource solution. It can provide economies of scale by delivering the same service to many users. However, cloud computing should not be exclusively about cutting costs. Rather it can also be about broad advantages, including cost-effective security. If security is implemented in a way that adds significant cost to the cloud infrastructure, it could reduce the economic viability of the cloud, creating a roadblock to adoption.

To help minimize costs, the level of protection offered by the cloud provider should be built commensurate to the potential risk to users. An enterprise customer, for example, would experience greater ramifications from corrupted or lost data than would a consumer who stores his or her calendar in a cloud.

Because security is a key requirement for today’s cloud users, it should also be looked upon as a means of differentiation and an opportunity to meet a customer need that may not be well met by the rest of the marketplace. In particular, providing adequate details about the security that is implemented and giving prospective customers assurance that it is carried out effectively, can create a compelling competitive advantage for the cloud provider.

For More Information

For additional information on cloud computing and related security technologies, visit the Web sites in Table 1 or contact a local Sun representative.

Table 1. Web links for additional information.

Web Site URL	Description
<i>sun.com/cloud</i>	Sun cloud computing vision and offerings
<i>sun.com/security</i>	Sun security solutions
<i>www.iso.org</i>	ISO 27001 and ISO 27002 information security standard
<i>sun.com/offers/details/CloudComputing.xml</i>	Sun Cloud Computing Infrastructure and Architecture white paper

Appendix A

NIST Definition of Cloud Computing

The following definition of cloud computing along with the descriptions of different service models and deployment models is taken from the National Institute of Standards and Technology (NIST) document entitled, “Draft NIST Working Definition of Cloud Computing,” by Peter Mell and Tim Grance. The full August 2009 version of this draft document can be found at

csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

Definition of Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics

Cloud environments are defined to have the following essential characteristics:

- *On-demand self-service*
A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.
- *Broad network access*
Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- *Resource pooling*
The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- *Rapid elasticity*
Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- *Measured Service*

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models

There are three primary models for delivering cloud services:

- *Software as a Service (SaaS)*

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- *Platform as a Service (PaaS)*

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

- *Cloud Infrastructure as a Service (IaaS)*

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

Cloud services are generally architected in one of the following four ways:

- *Private cloud*
The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud*
The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- *Public cloud*
The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud*
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Appendix B

Overview of ISMS

According to the ISO 27001 standard, “The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.” This underlying objective is fundamental to how the ISMS works and presumes a risk-based approach to the development, implementation and ongoing management of a security environment. Sun’s objective for discussing and promoting ISMS is that such an approach, when performed properly, allows for a great degree of transparency in the evaluation of threats, the measurement of those threats in terms of cost/benefit, and the determination of cost-effective controls as appropriate.

An ISMS enables transparency by providing a governance framework and security architecture, which is based upon the internationally recognized ISO 27001 standard. It spans the entire data lifecycle from data generation to transmission, storage, and end-of-life destruction of the data. It not only covers the security of deployed hardware and software components, but also covers operational procedures that affect security. The purpose of the ISMS is to enable the organization to develop, implement and maintain a comprehensive security program that addresses various governance and compliance requirements. When such a program is based upon ISO 27001, demonstrating transparency is greatly simplified.

Implementing an ISMS is organized into four primary tasks or steps as described below.

Step 1—Establish the ISMS

Perhaps the most difficult phase of any project is its initiation and this is true of an ISMS as well. Establishing an ISMS requires first developing a scope statement that defines the boundaries of the ISMS in terms of business scope, organizational needs for security, privacy, governance and compliance, and a high-level view of the relevant assets and technology in use. The purpose of the scope statement is to place realistic boundaries around the overall ISMS effort.

The primary tasks that are undertaken during the establishment of the ISMS include:

- Defining a security policy as a means for management intentions about security to be properly documented.
- Performing a risk assessment of the organization’s assets relative to information processing (this can be a quantitative or qualitative assessment).
- Identifying security control objectives for the treatment of risks as defined in ISO 27002 or a similar standard such as NIST 800-53.

- Determining and accepting any residual risk and obtaining management buy-in for the ISMS.
- Creating a statement of applicability that describes the justification for the selection of various control objectives as well as all exclusions and their justification. This is essentially the architecture elaboration step.

During this first step, it is important to maintain a high level of transparency because this is where the threat profile and trust model are identified. All parties involved in the ISMS effort should participate openly to help achieve the most definitive and comprehensive results.

Step 2—Implement and Operate the ISMS

The second step of the ISMS involves implementing and operating the security controls identified in the initial step. The critical task in this step is the creation of the risk treatment plan. This plan includes consideration of the various threats identified as well as a translation of security control objectives into actionable tasks for the implementation of specific security measures. This is essentially the engineering and configuration step.

The other tasks involved in this step are the identification and implementation of the means to measure the effectiveness of the control mechanisms such that one can generate comparable and reproducible results. This then allows prompt detection of security events and helps formulate an appropriate response to a security incident.

Transparency of the ongoing operation and management of the IT environment and associated control mechanisms is very important in a cloud environment. Since the cloud typically hosts customer data, customers will want the ability to evaluate how well the overall environment is managed.

Step 3—Monitor and Review the ISMS

The monitoring and review step of the ISMS is an ongoing function in which the effectiveness of the ISMS effort is measured. As such, transparency is also a key component of this function. Monitoring and review of the ISMS is performed via both regular ongoing system audits as well as independent and regular risk assessments. The overall intention is to provide an ongoing assessment of the effectiveness of specific ISMS control mechanisms and of the entire ISMS over time.

Also included in this step are the performance management reviews that help ensure that the overall scope of the ISMS is appropriate. If updates to the ISMS are necessary, they should be made to the overall security plan that is utilized to drive the ISMS. This step should also set up and support a continuous improvement model to make the ISMS a living process as described in Step 4.

Step 4 — Maintain and Improve the ISMS

To the extent that the ISMS is a living process and represents a continuous improvement model, it must be maintained and improved to address new and different threats that arise over time. This step requires that an improvement mechanism be documented, approved, and used. The technical aspect of this step involves the identification of appropriate corrective and preventative actions as well as a means to ensure that any modifications or improvements achieve their desired objectives.

The characteristic of this step that reflects transparency is the requirement to “Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.” Communicating improvements to the ISMS allows for the vetting of the recommended improvements and provides a feedback channel as necessary.

Appendix C

Leveraging ISO 27002 as a Transparency Framework

Table 2 provides an overview of the security control objective focus areas as defined in ISO 27002 and identifies the recommended disclosures for transparent security as well as the primary objectives and benefits of disclosure.

Table 2. Security control objectives and related disclosure items.

Security Control Objective	Description	Transparency Objectives [What Should Be Disclosed]	Benefits [Why]
Security policy	The security policy is a short, high-level policy statement about information security. It lays down the key information security directives and mandates for the entire organization.	<ul style="list-style-type: none"> • Disclose as much of the security policy as possible. • Disclose relevant corporate and IT standards and guidelines that describe the company's security stance, how the organization is accountable, and how employees are kept informed, etc. • Disclose customer rights and responsibilities. 	<ul style="list-style-type: none"> • Show that provider security policies align with business policy, security, and compliance requirements. • Demonstrate provider is consistent with industry accepted standard practices.
Organizing Information Security	An information security governance structure should span both the internal organization as well as govern the introduction of third party products or services and dealings with customers.	<ul style="list-style-type: none"> • Disclose the appropriate org charts, titles and charters and how information security is managed across the organization. 	<ul style="list-style-type: none"> • Determine that there is an independent information security function and accountability built into the organization.
Asset Management	Asset management is a means for an organization to identify, organize and manage their information resources.	<ul style="list-style-type: none"> • Disclose both manual and automated mechanisms that allow one to determine where their data is, who is accessing it, and how. 	<ul style="list-style-type: none"> • Determine what is possible for customer driven asset management. • Determine that discrete functions exist for asset management. • Evaluate jurisdictional requirements based on locations.

Security Control Objective	Description	Transparency Objectives [What Should Be Disclosed]	Benefits [Why]
Human Resources Security	The organization should have appropriate terms and conditions of employment, manage system access rights and should undertake suitable security awareness training.	<ul style="list-style-type: none"> • Disclose applicable HR and personnel management policies, standards, and procedures. 	<ul style="list-style-type: none"> • Create reasonable expectations regarding the reliability of personnel.
Physical and Environmental Security	IT assets should be physically protected against malicious or accidental damage or loss due to environmental factors or intrusions.	<ul style="list-style-type: none"> • Disclose controls and techniques over physical equipment, premise security, and environmental factors. 	<ul style="list-style-type: none"> • Create reasonable expectations of control, preservation and management over tangible assets. • Offer additional assurance for certain customers who have specific physical security requirements.
Communications and Operations Management	Security controls for systems and network management include a broad range of topics from network security management to operational procedures.	<ul style="list-style-type: none"> • Disclose control capabilities and standards used to secure data throughout its lifecycle, including data in transit, at rest, and disposal. • Customers should be made aware of techniques and procedures used to manage and monitor the system and network infrastructure. 	<ul style="list-style-type: none"> • Attest to the correct and secure operation of cloud infrastructure facilities. • Match specific customer requirements to communication and operations management capabilities. • Understand the need for compensating controls.
Access Control	Access control covers authentication and authorization to control access to data and processing resources.	<ul style="list-style-type: none"> • Disclose whether authorization and authentication schemas exist. • Provide sufficient details about technology attributes, platforms or access control standards. 	<ul style="list-style-type: none"> • Match specific customer requirements to access control capabilities. • Understand the need for compensating controls.
Information Systems Acquisition, Development and Maintenance	Information systems acquisition, development and maintenance processes for specifying, building/acquiring, testing, implementing, and maintaining IT systems.	<ul style="list-style-type: none"> • Disclose standards and processes used to ensure the security and integrity of the system acquisition and development process. 	<ul style="list-style-type: none"> • Understand the level of due diligence used in these processes. • Understand the various security and integrity controls used within these processes.

Security Control Objective	Description	Transparency Objectives [What Should Be Disclosed]	Benefits [Why]
Information Security Incident Management	Incident management covers both procedures required to manage incidents consistently and effectively as well as proper reporting of information security events, incidents, and weaknesses.	<ul style="list-style-type: none"> • Disclose policies and standards for incident management. • Disclose methods for informing customer and/or public regarding incidents. 	<ul style="list-style-type: none"> • Understand customer’s level of involvement and timing for disclosure of incidents and their resolution. • Understand provider’s posture on security incident response.
Business Continuity Management	Describes the relationship between IT disaster recovery planning, business continuity management and contingency planning. It also includes controls designed to minimize the impact of security incidents.	<ul style="list-style-type: none"> • Disclose policies and standards for disaster recovery, continuity and business resumption. • Disclose applicable service levels regarding availability and priority of data and processing resources. 	<ul style="list-style-type: none"> • Determine if availability and prioritization of recovery and continuity processes are satisfactory to the desired service levels.
Compliance	Includes not only compliance with legal requirements, but also with security policies and standards.	<ul style="list-style-type: none"> • Disclose applicable certifications, assessments or objective evidence that would indicate levels of compliance. 	<ul style="list-style-type: none"> • Determine levels of accountability of a provider against applicable requirements.

