CHAPTER

Evaluating Cloud Security: An Information Security Framework

9

INFORMATION IN THIS CHAPTER

- Evaluating Cloud Security
- Checklists for Evaluating Cloud Security
- Metrics for the Checklists

Cloud security represents yet another opportunity to apply sound security principles and engineering to a specific domain and to solve for a given set of problems. Up to this point in the book, we have surveyed a number of aspects of cloud security. In Chapter 4, we examined the architectural aspects of securing a cloud. In Chapter 5, we considered the requirements for cloud data security. Chapter 6 presented key strategies and best practices for cloud security, Chapter 7 detailed the security criteria for building an internal cloud, and in Chapter 8, we presented security criteria for selecting an external cloud provider.

This chapter builds on that previous material and presents the foundation for a framework for evaluating cloud security. This material is intended to go beyond and augment the security criteria we introduced in Chapter 8. It should benefit activities that precede the evaluation, certification, or accreditation of a cloud. We start by reviewing existing work in this area, and then we will put forward a set of checklists of evaluation criteria that span the range of activities that together support information security for cloud computing. The goal of this chapter is to provide the reader with an organized set of tools, which can be used to evaluate the security of a private, community, public, or hybrid cloud. Evaluating the security of a hybrid cloud may best be done by managing the evaluation of the two or more cloud instances using one set of checklists per instance. By example, if the hybrid consists of a private cloud and a public cloud, simply evaluate the private components using one set of checklists and evaluate the public components into their separate realms. When done in this manner, you can more readily compare public cloud alternatives.

Securing the Cloud. DOI: 10.1016/B978-1-59749-592-9.00009-9

EVALUATING CLOUD SECURITY

Most users of a cloud, whether it is a private or a public cloud, have certain expectations for the security of their data. Similarly, the owner and operator of a cloud share responsibility for ensuring that security measures are in place and that standards and procedures are followed. We can capture our expectations and responsibilities for security by stating them formally in documented requirements. By example, the NIST 800-53 security controls (these were discussed in Chapter 6) detail specific requirements for federal government systems. Systems that are fielded by government agencies must generally comply with these and related NIST requirements. The Cloud Security Alliance *Controls Matrix* takes a similar approach in detailing security requirements for cloud implementations, and there is a growing trend by commercial users to adopt such generally accepted requirements. A good starting point when you need to measure the presence and effectiveness of the security of a cloud includes having a list of required or recommended security controls.

To begin, there are two aspects to security controls in cloud implementations. The first has to do with the presence of the control. The second aspect is the effectiveness or robustness of the control. In other words, it is not enough that a security control is present—but that control also needs to be effective. Going further, one can describe this as the degree of trust (or assurance) that can be expected from these controls. For instance, a cloud may implement encrypted communications between the cloud and an external user—but if we are evaluating the effectiveness of encrypted communications, then we also need to verify that the control is properly designed, implemented, and verified.

Measuring the presence and/or effectiveness of security controls (against security requirements) is largely what security evaluations are intended to do. Security evaluations have broad value as guidance for planning or developing security and for verifying that required controls are properly implemented. But evaluations also have utility for procurement of cloud services; for instance, a CSP may choose to publish the high-level results of a third party security evaluation. In addition, if we are to compare the security of two or more clouds, then that will entail having a common set of criteria for evaluation.

On the basis of the sensitivity of data or the expected risk of a system, we should undergo an initial requirements phase where appropriate security controls are identified. If we subsequently perform a thorough assessment of the decision process that led to identifying those controls and couple that assessment with a security evaluation of the effectiveness of those controls that were implemented, then we should have a fairly good understanding of whether an overall cloud service has a sound security posture versus the risk it is subject to.

Figure 9.1 depicts the relationship between requirements, security evaluation of a cloud, the cloud implementation, vulnerability remediation, and continuing configuration management controls.

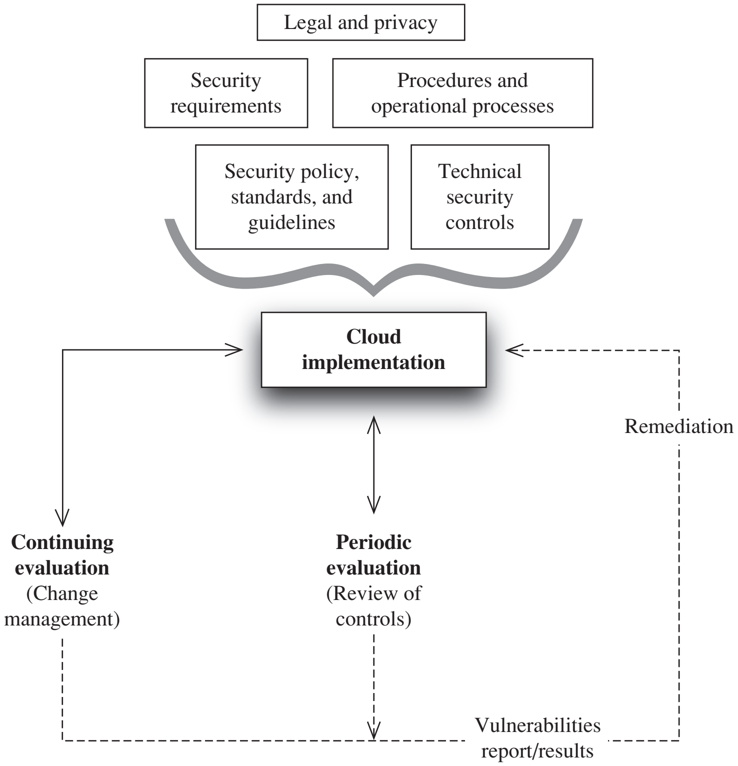
Legal and privacy
Security requirements
Procedures and operational processes
Security policy, standards, and guidelines
Technical security controls
Cloud implementation
Remediation
Continuing evaluation (Change management)
Periodic evaluation (Review of controls)
Vulnerabilities report/results

FIGURE 9.1

From requirements and evaluation to ongoing security remediation.

Existing Work on Cloud Security Guidance or Frameworks

In the few years since cloud computing arrived as a new model for IT, several efforts have already taken place to offer guidance for cloud security. These include:

- **Cloud Security Alliance (CSA)** The CSA has been very active in various efforts, including:
- **Cloud Controls Matrix (CCM)** This is "designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The Cloud Controls Matrix provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains."[1]
- **Consensus Assessments Initiative Questionnaire** This effort is "focused on providing industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency."[2]

- **Security Guidance for Critical Areas of Focus in Cloud Computing** V2.1 published in December 2009 presented security guidance for a number of areas in cloud computing; these include architecture, governance, traditional security, and virtualization.
- **Domain 12: Guidance for Identity & Access Management** V2.1 published in April 2010 discusses the major identity management functions as they relate to cloud computing. This work forms a cornerstone of the CSA's *Trusted Cloud Initiative*.
- **CloudAudit** Seeks to give cloud adopters and cloud operators the tools to measure and compare the security of cloud services. It does this by defining "a common interface and namespace that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments."[3]
- **European Network and Information Security Agency** Leading the security guidance efforts in Europe, ENISA has produced several guiding publications for securely adopting cloud computing, these include:
- **Cloud Computing: Information Assurance Framework** Published in November 2009. Presents a set of assurance criteria that address the risk of adopting cloud computing.
- **Cloud Computing: Benefits, Risks and Recommendations for Information Security** Published in November 2009.
- **The Federal CIO Council's** *Proposed Security Assessment and Authorization for U.S. Government Cloud Computing*.[4] The core importance of this document is that it adopts the NIST 800-53R3 security controls for cloud computing in low- and moderate-risk systems.
- **The Trusted Computing Group (TCG)** In September 2010, the TCG formed the *Trusted Multi-Tenant Infrastructure Work Group*, which is intended to develop a security framework for cloud computing. The Trusted Multi-Tenant Infrastructure Work Group will use existing standards to define end-to-end security for cloud computing in a framework that can serve as a baseline for compliance and auditing.

All of these efforts are relatively new and have yet to gain broad acceptance. More so, they are either initial activities that are intended to serve as a starting point for more formal work or the product of community efforts toward a common framework for cloud security. In other words, there is a great deal of uncertainty in this area. That presents a difficulty for cloud adopters who need to evaluate the security of their private or community clouds and also for users who need a means to evaluate the security of a cloud service.

Today, users do not yet have a common and standard means to evaluate cloud security. In fact, much of the pre–cloud computing world has not adopted security evaluation frameworks outside those realms where regulation requires a security benchmark or where evaluation is mandated. But cloud security is a fast moving area, and all of the above efforts have taken place between 2009 and the end of 2010. The adoption of these efforts is accelerating in several ways, especially in the government space with FedRAMP. By its very nature, adoption of public clouds is a change agent in security. There is a fast shaping trend here, and one can expect to see real progress in the near term. This is an example of how cloud computing is stimulating better security in business areas where otherwise there was great concern over security but little improvement until the rise of public clouds.

TOOLS

Many tools are used for security testing. These include the following categories:

- Port scanning for open and responding services
- SNMP scanning
- Device enumeration or cataloging
- Host vulnerability scanning
- Network device analysis
- Password compliance testing and cracking

There are several basic tools that have stood the test of time; these include NMAP for port scanning and Nessus for host vulnerability scanning. In addition, there has been a more recent crop of powerful tools that allow for extensive defense testing to identify quality, resiliency and related security vulnerabilities. These tools offer test suites for a broad range of cloud network security needs.

CHECKLISTS FOR EVALUATING CLOUD SECURITY

The intent of developing a cloud security evaluation checklist is to have a uniform means to verify the security of a cloud and also to obtain assurance from a CSP about their security. However, as stated in this chapter's introduction, such checklists can also be used by prospective customers or users to compare cloud security for different providers.

The remainder of this section presents checklists that form the heart of a framework for evaluating cloud security. The questions in these checklists are derived from several sources that include the CSA Cloud Controls Matrix,[5] the ENISA Cloud Computing Information Assurance Framework,[6] and NIST's 800-53R3.[7]

WARNING

Security testing, especially penetration testing and vulnerability testing, can easily produce a false sense of security. The problem is twofold:

- First, such tests are based on current knowledge of vulnerabilities and can't account for zero-day exploits that periodically arise. New vulnerabilities are discovered on a daily basis. Every once in a while, vulnerabilities are even exposed for very mature systems. Again, multiple layers of defense—defense-in-depth—is the best strategy against exposure to a zero-day exploit.

(*Continued*)

(*Continued*)

- Second, a sound bill-of-health in penetration or vulnerability testing cannot be taken as a measure of overall security—including procedures and the broad range of operational controls that any information security program depends on.

In other words, security testing—and especially penetration testing—only test the target system at a point in time and only to a limited extent. Systems and configurations tend to change over time, and new vulnerabilities can become exposed years after a system is fielded, tested, and approved. The bottom line is that these sorts of tests should be viewed as very superficial and should not be relied on to ascertain security. Which begs the question: Should they be performed at all? Security engineers generally agree that such tests have value. But, remember this: your opponents may have more time and interest in "testing" your systems than you do, so take testing seriously but don't rely on it.

One application for the checklist is that a cloud owner can use it to guide a security evaluation of their cloud. If cloud providers use such a checklist as a framework to report on the security of their clouds, then prospective tenants and users could compare the relative security of multiple clouds. The checklist can also be used by a public cloud customer to ask a series of questions that are relevant to their business needs. Not all these questions will be relevant for all uses or business relationships.

Each of the following sections is organized around a set of closely related controls or requirements. Figure 9.2 presents an overview of the evaluation checklist sections and lists the groups of controls or requirements for each section.

Foundational Security

A security *policy* defines the organization's requirements or rules for security. Security policy delineates the constraints and requirements that individuals and groups must operate under, and it serves as a statement of management's intent for security. Actions that are taken in regard to security should be clearly traceable to the security policy. Several classes of policy may exist, including an overall security policy as well as additional policies that address more limited areas (such as an *acceptable use policy*). Policy is focused on achieving desired results, and not on specific implementations.

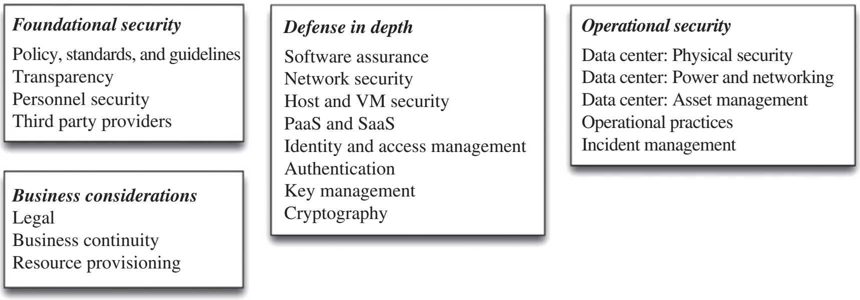

FIGURE 9.2

Overview of evaluation checklist.

Augmenting such policies are other statements of requirements for specific areas. These are usually defined as *standards* and cover such specific areas as technical controls or specific hardening requirements. Standards state mandatory actions that support policy. *Guidelines* are a third class of documentation that is less formal and more oriented toward procedural best practices. These are recommendations or descriptions of practices that support the objectives of a security policy by describing a framework to implement procedures. In other words: A policy states *why*, a standard states *what*, and a guideline states *how*. Checklist 9.1 covers foundational security elements related to policy, standards, and guidelines.

Checklist 9.1 Policy, Standards, and Guidelines[8–10]

Policy, Standards, and Guidelines

- Has a security policy been clearly documented, approved, and represented to all concerned parties as representing management's intent?
- Has the security policy had legal, privacy, and other governance review?
- Has the security policy been augmented by security standards and/or guidelines?
- Has the policy been augmented by a privacy policy?
- Are the security and privacy policies, as well as standards and guidelines, consistent with industry standards (such as 27001, CoBIT, and so on)?
- Are third party providers held to the same policies and standards?

Checklist 9.2 covers evaluation criteria that are focused on CSP transparency.

Checklist 9.2 Transparency[11–13]

Transparency

- Does the CSP provide customers with a copy of the governing policies, standards, and guidelines?
- Are customers notified of changes to governing policies, standards, and guidelines?
- Does the CSP provide customers visibility into third party compliance audits?
- Does the CSP provide customers visibility into penetration tests?
- Does the CSP provide customers visibility into internal and external audits?
- Does the CSP provide customers visibility into CSP asset management and repurposing of equipment?

Personnel security for a cloud is a foundation upon which operational security resides. The intent of personnel security is to avoid several classes of security risk and to create an environment that reinforces the objectives that are stated in security policy. Checklist 9.3 lists evaluation criteria related to personnel security.

Checklist 9.3 Personnel Security[14–16]

Personnel Security

- Are there policies and procedures for:
- Hiring employees who will have access to or control over cloud components?
- Pre-employment checks for personnel with privileged access?

- Are personnel security policies consistent across locations?
- Do they apply to online cloud systems and data as well as to offline systems that either stored data or to offline systems that will be provisioned for online use?
- Is there a security education program, and if so, how extensive is it?
- Is personnel security frequently reviewed to determine if employees with access should continue to have access?
- Are personnel required to have and maintain security certifications?
- Does physical access to the CSP's facility require background checks?

The use of subcontractors or third party providers can create undue risk for customers unless such providers follow and operate in accordance with CSP policies. Checklist 9.4 details criteria for third party providers.

Checklist 9.4 Third Party Providers[17–19]

Third Party Providers

- Are any services or functions provided by a third party?
- If any part of a cloud is subcontracted or otherwise outsourced, does the providing party comply with the same policy and standards that the CSP enforces?
- If used, are third party providers audited for compliance with the CSPs policies and standards?
- Does the CSP security policy (or equivalent) and governance extend to all third party providers?

Business Considerations

Various business considerations bring with them the need for security consideration. Business considerations include legal, business continuity, and resource provisioning. Evaluation criteria for these are listed in Checklists 9.5, 9.6, and 9.7; Checklist 9.5 covers legal criteria.

Checklist 9.5 Legal[20–22]

Legal

- Where—in which jurisdiction—will data be stored?
- Where—in which jurisdiction—is the CSP incorporated?
- Does the CSP use third party providers who are not located in the same jurisdiction?
- Does the CSP subcontract any services or personnel?
- Does the CSP use a customer's data in any manner that is not part of the service?
- Does the CSP have a documented procedure for responding to legal requests (such as a subpoena) for customer data?
- In the event of a subpoena, how does the CSP produce data for a single customer only without providing non-subpoena data?
- Is the CSP insured against losses, including remuneration for customer losses due to CSP outages or data exposure?

Business continuity can be critical for customers who use cloud-based services in a mission critical manner. Criteria associated with business continuity are listed in Checklist 9.6.

Checklist 9.6 Business Continuity[23–25]

Business Continuity

- Does the CSP have a formal process or contingency plan that documents and guides business continuity?
- What are the service recovery point objective (RPO) and recovery time objective (RTO)?
- Is information security integral to recovery and restoration?
- How does the CSP communicate a disruption of services to customers?
- Is there a secondary site for disaster recovery?

Business continuity is a complex topic that warrants far greater coverage than possible in a cloud security book. The interested reader is encouraged to research several related topic areas; these include business continuity planning along with contingency and disaster recovery planning. There are many sources for these areas, including:

- ANSI/ASIS SPC.1-2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use American National Standard
- The National Institute of Science and Technology (NIST) Special Publication 800-34 *Contingency Planning Guide for Information Technology Systems*
- Good Practice Guidelines can be downloaded from: www.thebcicertificate.org/bci_gpg.html
- And the Business Continuity Institute is located at www.thebci.org

EPIC FAIL

As reported by the German online newspaper *Zeit Online* on February 18, 2011,[26] an error in the cloud provider's payment system paralyzed a German company's access to their public cloud SaaS e-mail and online documents. Although the actual facts in this case are not fully clear at the time this chapter was written, it should serve as a warning: Any cloud provider's accounting or customer management systems could be in error and in an extreme case this might result in a *business* denial-of-service.

Such an accounting error is certainly not unique in the world of billing and debt collection, but in a communications system—such as the Internet—or in a cloud services situation, the error can conceivably occur, and the consequences felt very quickly without the victim having any prior billing warning. The cloud services model brings a second complicating factor: Many cloud services largely rely on self-service interfaces, with little recourse from traditional human customer service representatives.

In the radio.de case, it appears that the CSP abruptly cut off access to radio.de's office software and relevant documents. Radio.de apparently could not reach the CSPs regional office in Dublin, and e-mails to the CSP did not solve the problem for a few days. The facts

(*Continued*)

(*Continued*)
in this specific case are not at all clear, so the CSP will go unidentified here. However, if you outsource your critical business functions, make certain that any similar situation can be more quickly resolved with the CSP. That will entail doing your homework before you form a business relationship with a CSP, and it will entail maintaining contact with the provider so that you are always aware of any changes in contact methods or details. Finally consider this: If your disaster recovery plan is stored on the CSPs systems, you really don't have a CSP disaster recovery plan at all.

Resource provisioning has to do with assuring that the cloud service will be sufficiently resourced as customer demand increases. To do this, a CSP would need to take certain measures to successfully deliver on their SLAs. For instance, the CSP might have procedures in place to add servers or storage as demand increases. Checklist 9.7 lists evaluation criteria for resource provisioning.

Checklist 9.7 Resource Provisioning[27–29]

Resource Provisioning

- What controls and procedures are in place to manage resource exhaustion, including processing oversubscription, memory or storage exhaustion, and network congestion?
- Does the CSP limit subscriptions to the service in order to protect SLAs?
- Does the CSP provide customers with utilization and capacity planning information?

Defense-in-depth

The integrity and security of an operational cloud depends on the integrity of components that comprise it. Software is a primary vector for vulnerabilities and exploits. To begin, Checklist 9.8 lists evaluation criteria for software assurance.

Checklist 9.8 Software Assurance[30–32]

Software Assurance

- What controls are in place to maintain integrity of operating systems, applications, firmware updates, configuration files, and other software?
- What industry standards, guidelines, or best practices are followed?
- What controls or guidelines are used to obtain or download software and configuration files?
- What guidelines or procedures are used to maintain software integrity?
- Is penetration or vulnerability testing used on each release?
- How are identified vulnerabilities remediated?

One very powerful technique for improving software security is to empower developers during the development process itself by giving them access to security testing tools. Such tools range from static code analysis through web security testing. A best practice is to have the development environment closely mirror the eventual testing, staging, and production environments. With development, this is not always easy, but the fewer deltas between environments the better the transition and the fewer security surprises your developers will encounter. (When test, staging, and production environments vary widely, errors and costs will rise dramatically as well.)

TIP

One software testing technique is known as *fuzzing*. This technique involves injecting invalid and unexpected data to the input of a program or system. Using this technique, even random data can result in program crashing or entering a state whereby a security control can be made to fail. Two areas are especially fruitful for this testing, one is file formats, and the other is network protocols. Fuzz data can be sent as events, command line input, or mutated packets. One of the strengths of using fuzzing is that it can illuminate severe and exploitable bugs.

The most significant aspect of a cloud's security may well be the network implementation. Architectural and isolation choices that are made here will have far reaching benefits or consequences. Network choices start with the physical network, equipment functionality, and extend to network virtualization and monitoring. The degree of isolation between different classes of traffic (customer access, customer-to-customer, operations and management, external access, and so on) will drive other security requirements at the systems and VM levels. Checklist 9.9 lists criteria for network security.

Checklist 9.9 Network Security[33–35]

Network Security

- What controls are in place to manage externally sourced and internally sourced attacks, including distributed denial of service (DDoS)?
- For customers, how is isolation managed between VMs by the hypervisor?
- For customers, how is isolation managed between VMs by network hardware and routing?
- What standards or best practices are used to implement virtual network infrastructure?
- How are MAC spoofing, ARP poisoning, and so on protected against?
- How is isolation managed between customer accessed/routable systems and cloud management systems and infrastructure?
- Is cloud customer processing dependent on off-cloud tenant components such as LDAP?
- Does the CSP perform periodic penetration testing against the cloud?
- If so, is penetration testing done both from external to the cloud and from inside the cloud and the cloud infrastructure?
- Does the CSP perform vulnerability testing of the cloud infrastructure, cloud management, and also customer accessible components?
- How are identified vulnerabilities tracked and addressed?
- Is vulnerability information made available to customers?
- Does the CSP allow customers to perform vulnerability testing against the customer's own VMs or other containers?

The kinds and degree of security controls that are required to protect hosts and VMs are to a large extent driven by the network architecture. There are trade-offs on the one hand between extreme network isolation and control and on the other hand with the desire for maximum flexibility in operation. The greater the flexibility, the more compensating controls are needed at the host and VM levels. Checklist 9.10 lists evaluation criteria for host and VM security.

Checklist 9.10 Host and VM Security[36–38]

Host and VM Security

- Are customer VMs encrypted and/or otherwise protected when stored?
- Are VM images patched before they are provisioned?
- How and how frequently are VM images patched after being provisioned?
- To which standards or guidelines are VM images hardened before being provisioned?
- What are the procedures for protecting hardened and patched VM images?
- Can a customer provide his/her own VM image?
- Does the CSP include any authentication credentials, and if so, what are they used for?
- Do hardened and patched VM images include operating firewall instances by default? (And if so, what are the allowed services/ports?)
- Do hardened and patched VM images include operating IDS or intrusion prevention systems (IPS)?
- If so, does the CSP have access to these in operation (and if so, how)?
- Do hardened and patched VM images include any form of network, performance, or security instrumentation that the CSP or tenant has access to?
- How is isolation ensured between server colocated VMs for different customers?
- How is communication implemented between VMs for the same customer?
- How is security ensured for user data in storage systems?
- How is security ensured for user data in motion between storage systems and customer VMs?
- How is security ensured for user data and user interaction between a VM and a non-cloud user system?
- Does the CSP provide information to customers to guide customer security so that it is appropriate for the virtualized environment?

CSPs are generally responsible for the platform software stack, including security. Although a CSP may be reluctant to provide details about the security of a PaaS stack, a CSP should be transparent about their security practices and the scope of security controls. Checklist 9.11 lists evaluation criteria for PaaS and SaaS security.

Checklist 9.11 PaaS and SaaS Security[39–41]

PaaS and SaaS Security

- How does the CSP isolate multitenant applications?
- How does the CSP isolate a user's or tenant's data?
- How does the CSP identify new security vulnerabilities in applications and within the cloud infrastructure?
- Does the CSP provide security as a service features for PaaS (such as authentication, single sign on, authorization, and transport security)?

- What administrative controls does the CSP provide to a tenant/user and do these support defining/enforcing access controls by other users?
- Does the CSP provide separate test and production environments for customers?

Identity and access management are critical elements of security for a cloud. Checklist 9.12 lists evaluation criteria for identity and access management, along with authentication.

Checklist 9.12 Identity and Access Management[42–44]

Identity and Access Management

- Do any CSP controlled accounts have cloud-wide privileges (if so, which operations)?
- How does the CSP manage accounts with administrator or higher privilege?
- Does the CSP use 2-man access controls, and if so, for which operations?
- Does the CSP enforce privilege separation (for instance, RBAC), and if so, what roles are used to limit which privileges (security, OS admin, identity, and so on)?
- Does the CSP implement break-glass access, and if so, under what circumstances are they allowed and what is the process for post-clean up?
- Does the CSP grant tenants or users administrator privileges, and if so, what are the limits to this?
- Does the CSP verify user identity at registration, and if so, are there different levels of checks depending on resources to which access is granted?
- How are credentials and accounts deprovisioned?
- Is deprovisioning of credentials and accounts done in a cloud-wide atomic-operation manner?
- How is remote access managed and implemented?

For CSP supplied customer-use identity and access management systems:

- Does this support federated identity management?
- Is the CSP's system interoperable with third party identity provider systems?
- Can a customer incorporate single sign on?
- Does this system support separation of roles and LPP?

How does a CSP verify their identity to a customer under the following scenarios:

- When the CSP communicates out-of-band to a customer or user?
- When a customer interacts with the CSP via an API?
- When a customer uses a cloud management interface?

Authentication

- How is authentication implemented for high-assurance CSP operations?
- Is multifactor authentication used?
- Is access to high-assurance operations limited to only operations cloud-networks and only from whitelisted IP addresses?
- Does intrusion detection/anomaly detection detect multiple failed logins or similarly suspicious authentication or credential compromise activities?
- What procedures are invoked if a customer's credentials or account is compromised?

Key management and cryptography must be handled in precise and correct ways otherwise cryptographic security is quickly undermined. Checklist 9.13 lists security criteria for these areas.

Checklist 9.13 Key Management and Cryptography[45–47]

Key Management

- For keys that the CSP controls:
- How does the CSP protect keys, and what security controls are in place to effect that?
- Are hardware security modules used to protect such keys?
- Who has access to such keys?
- How are those keys protected for sign and encrypt operations?
- What procedures are in place to manage and recover from the compromise of keys?
- Is key revocation performed in a cloud-wide atomic-operation?

Cryptography

- For what operations (and where) is encryption used?
- Are all encryption mechanisms based on third party tested and evaluated products?
- Does security policy clearly define what must be encrypted?

To this point in the checklists, we have covered evaluation criteria for foundational security, business considerations, and defense-in-depth. The final group of checklists addresses operational security issues.

Operational Security

Many concerns around public clouds have to do with the fact that physical security of IT is in a third party's control. With a public cloud, a physical breach will affect multiple customers. Checklist 9.14 lists evaluation criteria for data center physical security and data center power and networking.

Checklist 9.14 Data Center: Physical Security and Power and Networking[48–50]

Data Center: Physical Security

- What are the requirements for being granted physical access to the CSP's facility?
- Do non-employees require escort in the facility?
- Is entry into the facility constrained by function and entry location? (Examples: shipping and receiving, housekeeping)
- Is the facility divided into zones such that each requires access permissions?
- Is strong authentication (for example, multifactor card and pin or card and biometric) required for physical access?
- Is all access monitored and documented?
- Are all entry locations alarmed and monitored?
- Is video monitoring complete for all common areas of the facility?
- How long is video retained?
- How often is a risk assessment performed for physical security?
- Does the CSP require that all deliveries or equipment removals be performed by the CSP within the facility (that is, is there a separate shipping facility outside the physical perimeter of the cloud facility itself)?

Data Center: Power and Networking

- Is power and networking secured within the facility?
- Are environmental systems (lighting, AC, fire detection) implemented to industry standards?

- Is air conditioning sized to withstand extended periods of extreme conditions?
- Is the facility exposed to moderate or higher risk of environmental or weather damage?
- Does the facility receive power from multiple power sources?
- Does the facility provide backup power generation for a period or time that is adequate to recover from loss of a primary power source?
- Does the facility have adequate UPS for short or temporary outages?
- Does the facility have multiple Internet connections, and are these from different tier 1 providers?

A CSP must maintain a current and complete list of all information resources that are used to implement and operate the cloud. The state-of-the-practice (ITIL) is to use a CMDB to maintain such information. The state-of-the-art is to have that process automated by using the CMDB as the centralized repository with which all other cloud management functions interoperate. Checklist 9.15 lists criteria for data center asset management.

Checklist 9.15 Data Center Asset Management[51–53]

Data Center Asset Management

- Does the CSP maintain a current and complete inventory of all hardware, network, software, and virtual components that comprise the cloud?
- Does the CSP automate such inventory tracking and management?
- Does the CSP maintain a record of all assets that a customer has used or on which a customer has stored data?
- Does the CSP support asset categories of different sensitivity levels, and if so, how are these isolated or separated from each other?
- Does the CSP maintain segregation or physical separation of assets at different sensitivity levels?

Effective security is an ongoing process that entails well-defined procedures and roles for all personnel. To be effective, such procedures must anticipate various kinds of events. Procedures should offer enough guidance to allow personnel to navigate a broad range of failure in systems, processes, and other circumstances. Such events and responses must be captured with learned lessons integrated into updated procedures. Chapter 10 will provide a deeper treatment of this topic, but here we will outline the kinds of controls that guide operational practices and security. Checklist 9.16 lists evaluation criteria for operational practices.

Checklist 9.16 Operational Practices[54–56]

Operational Practices

- Is there a formal change control process, and are the procedures clearly documented?
- Does change control include a means to guide decisions as to what changes require a reassessment of risk?
- Are operating procedures clearly documented and followed?
- Are there separate environments for development, testing, staging, and production?

- What system and network security controls are used to secure end user or tenant applications and information?
- What security controls are used to mitigate malicious code?
- What are the backup procedures (who does this, what gets backed up, how often is it done, what form does it take, and are backups periodically tested)?
- Where are back ups stored, and for how long are they kept?
- Will the CSP securely delete all copies of customer data after termination of the customer's contract?
- Under what circumstances are customer resources sanitized using industry best practices (for example, degaussing)?
- Does the CSP have documented security baselines for every component that comprises the cloud infrastructure?

The goal of incident management and response is to minimize or contain the impact of events. Incident management should be well defined in order to support and guide the CSPs and the customer's ability to reduce the consequence of unanticipated events or situations. Checklist 9.17 lists evaluation criteria for the area of incident management.

Checklist 9.17 Incident Management[57–59]

Incident Management

- What information is captured in audit, system, and network logs?
- How long is it retained, and who has access to it?
- What controls are used to protect these logs from unauthorized access and to preserve the chain of custody of such materials?
- How and how often are logs reviewed?
- How and how often are logs checked for integrity and completeness?
- Are all systems and network components synchronized to a single time source (NTP)?
- Does the CSP have a formal process to detect, identify, and respond to incidents?
- Are these processes periodically tested to verify that they are effective and appropriate?
- Are log and other security data maintained to comply with legal requirements for chain-of-custody control, and do the data and controls comply with legally admissible forensic data?
- What is the escalation process for incident response?
- Does the CSP use intrusion detection, security monitoring, or SEIM to detect incidents?
- Does a CSP accept customer events and incident information into their security monitoring and incident management process?
- Does the CSP offer transparency into incident events, and if so, what kind of information is shared with customers and users?
- How are security events and security logs protected and maintained?
- How long are security logs retained?
- Who has access to such logs?
- Does the CSP allow customers to implement a host-based IDS in VMs?
- If so, can a customer send such VM IDS data to the CSP for processing and storage?
- How are incidents documented as they take place?
- How are incidents analyzed after the incident has ended?
- Can the CSP provide a forensic image of a customer VM?
- Does the CSP report statistics on incidents to customers?

METRICS FOR THE CHECKLISTS

The checklists alone have utility to judge the security of a cloud, but what prospective public cloud customers and owners of a private cloud want to know are:

- How secure is the implementation?
- Is the CSP meeting best practices for security?
- How well does the CSP meet discrete security controls and requirements?
- How does this service compare with other similar services?

Looking at checklists 9.1 to 9.17, there is a good deal of variation in how controls can be implemented and how they can be measured. This makes it very difficult to identify metrics for each question. Existing approaches for measuring security meet this challenge by both detailing fine grained security controls for specific realms (such as NIST 800-53R3) and specifying which of these controls apply to systems operating at different levels of assurance or sensitivity. But even then, the actual evaluation of the security of an implementation is time consuming and expensive and requires expertise.

The resulting Certification and Accreditation (C&A) of a system is a snapshot in time and must be repeated as the system evolves and undergoes change. Typically, these evaluations are paper exercises that involve a great deal of effort. What is needed is an evolution to this process itself, and cloud computing will demand greater automation simply due to the nature of the contract between IT and cloud consumers.

What would this look like? To begin with, the information and the evidence *artifacts* that are collected about security, systems, and processes must be organized in a C&A repository that is more like a database than a traditional formal document. The importance of collecting and organizing this information is that it supports statements and claims about how discrete security controls are met.

Having such information in database form makes it useful to multiple entities. In a cloud implementation, multiple parties use the same infrastructure and controls. A security evaluation should enable the reuse of information about such controls as well as information about their effectiveness. Cloud computing really does change the game for security, and it is already becoming clear that the adoption of cloud will drive the development of not only better security to meet the demands of elasticity and on-demand self-service but also for the measurement and evaluation of security.

SUMMARY

The rise in public computing utilities has brought increased need for better security. By their very nature, competitive public cloud services are faced with the need to provide cost-effective services and features sets that enable ease of adoption. But equally important is the need for a public cloud service to be seen as an appropriate and safe solution to meeting IT requirements. And in that, CSPs have few alternatives than to undergo evaluation of their product using commonly accepted criteria. Likewise with private clouds, even if security requirements are included from the earliest design stages, and even when sound principles are followed in building and fielding a private cloud, the proverbial proof is still in the *evaluation pudding*.

The security checklists in this chapter are intended to guide readers in developing their own lists for verifying the security of either a CSP or a private cloud. At the time this book was being written, there were several ongoing activities around developing industry or government guidelines around this need. Readers are encouraged to research the state of such work by following the various leading groups that are involved in these activities. It is not at all clear how successful any of these groups will be, and already today there is a good deal of collaboration between groups such as the CSA and CloudAudit/A6. It is certain that this is a rapidly evolving area, and it is very likely that the unique characteristics of the cloud computing model will drive far greater automation in the ongoing verification of such evaluation criteria.

NOTE

Readers who are interested in cloud security evaluation are advised to join the following groups:

- The Cloud Security Alliance:
  - www.cloudsecurityalliance.org
  - www.linkedin.com/groups?mostPopular=&gid=1864210
  - http://groups.google.com/group/cloudsecurityalliance
- CloudAudit:
  - www.cloudaudit.org/
  - http://groups.google.com/group/cloudaudit
- The Trusted Computing Group:
  - www.trustedcomputinggroup.org/solutions/cloud_security
  - www.linkedin.com/groups?mostPopular=&gid=3254114
- CloudSecurity.org (http://cloudsecurity.org/forum/index.php) is not very active but has potential as an independent forum for collaboration in testing cloud security.

It seems that every few weeks, Linked In and Google Groups are adding a new cloud group, and more than a few of these are focused on security. With all these cloud security groups, one of the best ways to stay informed is to join the major high-level cloud interest groups and follow general trends in the field. Periodic research via web searching should identify other specific interest area groups as they arise.

Endnotes

1. CSA-GRC-Stack-v1.0-README.pdf. http://www.cloudsecurityalliance.org/.
2. Ibid.
3. Ibid.

4. Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft version 0.96, CIO Council, US Federal Government; 2010.
5. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
6. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009 [accessed 24.03.11].
7. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
8. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
9. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
10. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
11. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
12. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
13. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
14. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
15. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
16. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
17. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
18. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
19. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
20. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
21. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
22. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
23. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
24. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
25. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
26. Asendorpf D. "Ab in die Wolken", Zeit Online, 2011; http://www.zeit.de/2011/08/Cloud-Computing; 2011 [accessed 24.03.11].
27. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
28. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
29. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
30. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
31. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.

32. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
33. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
34. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
35. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
36. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
37. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
38. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
39. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
40. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
41. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
42. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
43. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
44. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
45. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
46. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
47. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
48. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
49. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
50. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
51. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
52. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
53. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
54. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
55. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
56. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.
57. Controls Matrix (CM), Cloud Security Alliance V1.0; 2010.
58. Catteddu D, Hogben G. Cloud Computing Information Assurance Framework, European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/; 2009.
59. NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; 2009.