cloud security alliance℠

SecaaS Implementation Guidance

Category 5 //
Security Assessments

September 2012

Contents

Foreword

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. We are reaching the point where computing functions as a utility, promising innovations yet unimagined. The major roadblock to full adoption of Cloud Computing has been concern regarding the security and privacy of information.

Much work has been done regarding the security of the cloud and data within it, but until now, there have been no best practices to follow when developing or assessing security services in an elastic cloud model—a model that scales as client requirements change.

One mission of the Cloud Security Alliance is to provide education on the uses of Cloud Computing to help secure all other forms of computing. To aid both cloud customers and cloud providers, the CSA SecaaS Working Group is providing Implementation Guidance for each category of Security as a Service, as delineated in the CSA's SecaaS Defined Categories of Service. Security as a Service was added, as Domain 14, to version 3 of the CSA Guidance.

Cloud Security Alliance SecaaS Implementation Guidance documents are available at https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/.

We encourage you to download and review all of our flagship research at http://www.cloudsecurityalliance.org.

Best regards,

Jerry Archer	Alan Boehme	Dave Cullinane
Nils Puhlmann	Paul Kurtz	Jim Reavis

The Cloud Security Alliance Board of Directors

Letter from the Co-Chairs

Security as a Service is a specialized area categorized two years ago as growing rapidly and in unbound patterns. Vendors were struggling. Consumers were struggling. Each offering had its own path. We felt it was urgent to address the needs and concerns common to the implementation of Security as a Service in its many forms.

The Defined Categories of Service helped clarify the functionalities expected from each Category. In this series, we hope to better define best practices in the design, development, assessment and implementation of today's offerings.

We want to thank all of the many contributors worldwide who have worked so hard to produce these papers providing guidance for best practices in Cloud Computing Security. Many have been with the Security as a Service Working Group since the beginning; many others joined in this effort. Each has spent countless hours considering, clarifying, writing and/or editing these papers. We hope they help move forward toward those unimagined innovations.

Sincerely,

Kevin Fielder and Cameron Smith
SecaaS Working Group Co-Chairs

Acknowledgments

Co-Chairs

John Hearton, Secure Mission Solutions
Wolfgang Kandek, Qualys

Contributors

Lenin Aboagye, Apollo Group
Sudhir Babu, PwC
Aradhna Chetal, The Boeing Company
David Howe, Symantec
Michael Knutson, Celgene
Chinmoy Rajpal
Ameen Sharif, Fauji Fertilizer Company Limited
Chris Simpson, Bright Moon Security
Andrew Wild, Qualys

Peer Reviewers

Bernd Jäger, Colt
Jean Pawluk
Roshan Sequeira, ISIT AE FZ

CSA Global Staff

Aaron Alva, Research Intern
Vicki Hahn, Technical Writer/Editor
Luciano JR Santos, Research Director
Kendall Scoboria, Graphic Designer
Evan Scoboria, Webmaster
John Yeoh, Research Analyst

1.0 Introduction

Organizations rely upon information and information technology to support business decisions and processes, as well as ensuring compliance with legal, regulatory and statutory requirements. To ensure that these business objectives are achieved, organizations must ensure the confidentiality, integrity and availability of information assets. Security assessments through an independent external or internal body provide a vital interface between the Board (responsible for governance) and the executive management (responsible for day to day management).

Overall, Security Assessments play an important role in helping an organization understand the effectiveness of the controls deployed. They provide input for a dashboard reporting the current security posture of the organization, enhance the efforts of the organization in protecting their vital assets, align business goals to IT goals, and provide assurance to all concerned stakeholders in meeting the strategic and tactical goals of the organization.

Security assessments are third-party or internal audits (by an independent department of an organization) of on-premise or cloud-based systems. Traditional security assessments for infrastructure or applications and compliance audits are well defined and supported by multiple standards such as NIST, ISO, HIPAA, GLBA, PCI and CIS. Over the last several years, security as a service (SecaaS) solutions have been developed that provide and support security assessments in which a cloud-hosted solution performs the assessments and stores the resulting data. Today, a relatively mature technology exists, and tools for a number of security assessment areas have been implemented using the SecaaS delivery model. In the SecaaS delivery model, subscribers get the typical benefits of this cloud computing variant - elasticity, negligible setup time, low administrative overhead, and pay-per-use with low initial investment.

There are many choices for an assessment framework standard and there is no "one size fits all" solution for security assessments. One could reasonably expect that as cloud technology and governance evolves, a much smaller subset will emerge with a cloud focus. The Cloud Security Alliance (CSA) is taking a leading role in promoting a cloud-based assessment framework that maps well with others currently in widespread use today, such as ISO 2700X, PCI DSS, or COBIT.

CSA provides a security guidance framework that can be used to help assess the security of cloud-based business processes, and ensure the continued confidentiality, integrity and availability of those processes. CSA's Cloud Control Matrix provides an excellent cross-reference document that maps closely to many standard security frameworks, including: COBIT 4.1; HIPAA/HITECH; ISO/IEC 27002-2005; NIST SP800-53 R3; FedRAMP; PCI DSS

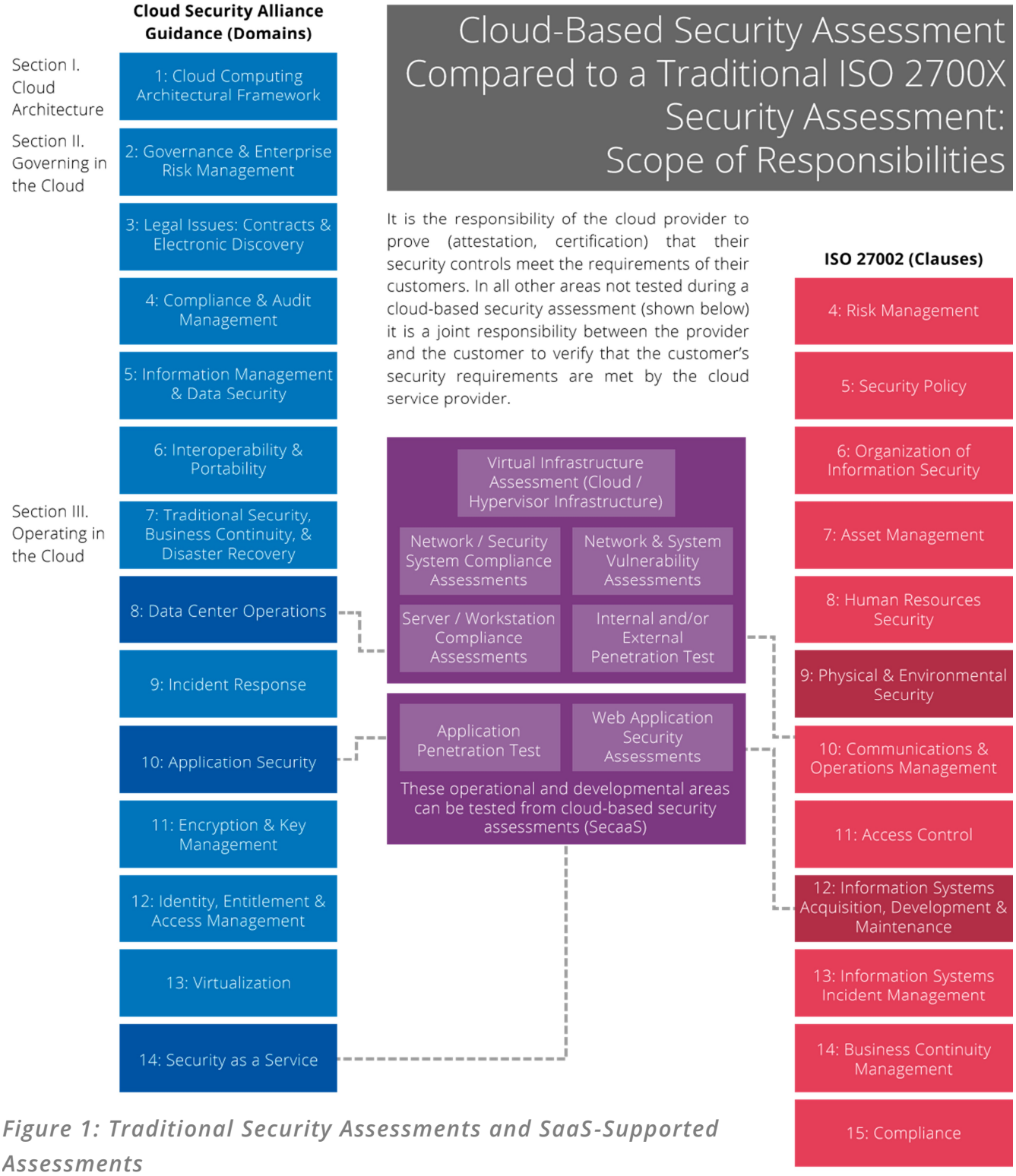

Figure 1: Traditional Security Assessments and SaaS-Supported Assessments

v2.0; BITS Shared Assessments SIG v6.0 and BITS Shared Assessments AUP v5.0; GAPP (Aug 2009); Jericho Forum; and NERC CIP.

Traditional Security Assessments follow a specific methodology such as ISO 27000. SaaS-based Security Assessments can be used to execute some of the assessment activities in the Communications and Operations Management and Applications sections.

This document provides guidance on the evaluation and use of SaaS-based services to conduct security assessments on both enterprise and cloud-based networks, infrastructure and applications.

1.1 Intended Audience

The target audience of this document is Chief Information Security Officers, Information Security Officers, IT security managers, technical assessors and auditors who are responsible for performing security assessments on their or their client organizations' infrastructure and applications.

Section 2 presents a high-level overview of the processes and procedures inherent in a cloud-based assessment service offering.

Section 3 is of particular interest to all levels of personnel involved in the assessments decision. Considerations and concerns that should be part of the decision making discussion are laid out in detail.

Section 4 enters into a more in-depth technical discussion of both the architecture and the implementation process.

1.2 Scope

This document discusses the following security assessment areas:

- Network and System Vulnerability Assessments
- Server/Workstation Compliance Assessments
- Network/Security System Compliance Assessments
- Virtual Infrastructure Assessment (Cloud/Hypervisor infrastructure)
- Web Application Security Assessments
- Internal/External penetration testing
- Security Controls Assessments

2.0 Requirements Addressed

Organizations face a number of challenges when ensuring the confidentiality, integrity and availability of their information and information technology assets. In addition, depending on their industry, they may have to respond to external auditing standards. Security assessments can help organizations manage many of these challenges, including:

- Proving Adherence to Regulatory Standards
- Securing Computing Architectures
- Assuring Accurate Inventory
- Securing Baseline Configurations
- Verifying Process Flow
- Comprehensive Logging
- Continuous Monitoring

Cloud-based security assessments provide the information necessary for an intelligent, risk-based decision making process, while relieving IT staff of the operational burdens of managing the assessment tool infrastructure. Organizations must establish policies, processes, and procedures, and implement controls to ensure the confidentiality, integrity and availability of the information and information technology upon which their critical business processes depend. This section provides an executive level overview of the processes and requirements of cloud-based security assessments.

2.1 Common Requirements

Information often is the most important asset within a business, and data security is a high priority for executive management. Security assessments are key to maintaining data security, and therefore are of interest to many executives. Companies also hold regulatory responsibility for adequately protecting personal information both for employees and customers, again elevating the importance of securing data.

Key business processes and the assets that run them should be identified prior to the start of an assessment. All parties should agree to and document any and all rules of engagement to be used during the assessment, for example asset exclusions, time windows, level of attacks, social engineering techniques, etc.

Assessments usually are safe to run even on production systems, but a service provider should have mechanisms in place to be able to stop an assessment at any time if something happens that could be destructive to a server or workstation, or disruptive to key business processes. Both parties should sign an appropriate Non-Disclosure Agreement (NDA). The NDA should limit disclosure of all information obtained, either in preparation for the assessment or through the assessment results, to only those with a verified need to know.

2.2 Data Access

The data that results from cloud-based security assessment services is very sensitive in nature and must be properly safeguarded. Cloud-based security assessment services must ensure the confidentiality of this sensitive data and ensure that only authorized parties can access the data. Data must be secured at all stages: at creation, in storage, in transit in processing, or at deletion. Additionally, because cloud-based security assessment services are typically offered as multi-tenant solutions, SecaaS providers must offer adequate attestation (see Section 4.1.3) for the isolation of tenant data.

The customer of the cloud-based service should retain sole ownership of any data that results from the use of the service, and there should be a mechanism for the customer to request the data for purposes of moving to another cloud-based service or to an enterprise-based service. Data retention properties should be configurable by the service customer. To ensure the security of data entrusted to a security assessment service, there should be a process for ensuring for the permanent destruction/deletion of the data upon request, as well as at the end of the assessment or at a predetermined time following the assessment.

Organizations should determine whether normal user authentication meets their needs or if there is a need to require stronger authentication protocols such as multi-factor authentication. Service providers should be able to produce detailed records or logs for user sessions and have the ability to store the records/logs to meet typical industry log retention standards.

Authentication credentials are extremely confidential and a cloud-based security assessment service provider should be able to ensure the confidentiality of these credentials. Credentials that are no longer required should be deleted after use. A log of deleted users, as well as the roles that they possessed, should be held for log retention standards compliance.

Cloud-based security assessment services are able to assess any system that is accessible via the Internet, but frequently there are systems that are internal to an organization that require assessments. These internal systems are often isolated from the Internet by security policies enforced by network security appliances such as firewalls. Cloud-based security assessment services usually offer a solution for assessing internal systems using appliances or software agents.

Network and system vulnerability assessments attempt to identify vulnerabilities through the use of IP scanning techniques, combined with a detailed understanding of vulnerabilities. The assessments include the identification of systems and associated vulnerabilities, as well as information about the potential impact on the network or enterprise.

2.3 Tools

As with all assessment activities, understanding the tools that the provider will use is important. If the provider is using a cloud-based tool, the guidance in this section applies directly. However, this guidance may still be helpful even in cases where traditional tools are being used.

Coordinate with the cloud provider to conduct testing in accordance with CSA Guidance. Determine if the cloud hosting provider offers such a service. If not, understand the limitations of performing such actions in hosted cloud environments. Scope and limitation will vary based on which stack of the SPI model the cloud-hosted application seems to fit.

Compliance scanning attempts to verify the compliance status of the devices in your environment. Server and workstation compliance assessments allow for the discovery of server/workstation configurations, as well as the comparison of the results against industry best practices and any customized configuration standards. Typical server/workstation compliance assessments include:

- The ability to conduct authenticated scans or a resident agent to detect the server/workstation configuration.
- The ability to compare discovered configurations with industry best practices or custom configuration standards to determine compliance.
- The ability to periodically check authorized or unauthorized changes in the configuration of a system.

Similar to server/workstation system compliance assessments, network and security system compliance assessments audit the configuration of security appliances (firewalls, IDS/IPS, WAF, Routers, Switches, etc.) against both industry best practices and custom configuration standards.

Other considerations should include support for a wide range of network and security devices, and the ability to assess not only the device configuration, but also any specific security or network policies implemented by the device (routing policies, firewall policies, IDS policies, etc.).

Cloud and virtual environments typically have their own management interface that is used to configure the environment. As with any type of computer system, there are best practices and, often times, defined organizational configuration standards for the use of cloud and virtual environments. Virtual infrastructure assessments seek to identify configurations and compare them to industry defined best practices or custom defined configuration standards. Service providers should allow for the ability to view and manipulate the data found during an assessment, as well as the provide access to the mechanisms used within assessments, to allow for validation of compliance with all standards and/or vulnerabilities scanned against.

A vendor should be able to access the management interface for the cloud/virtualization solution in place (e.g., VMware, vCenter, Amazon EC2, Azure, etc.) to retrieve configuration information automatically. A service provider also should be able to compare configurations with vendor/industry best practices, as well as custom created configuration standards.

Web application security assessments automate the process of scanning web applications for security vulnerabilities. Testing web applications is a complex task, especially if the web application utilizes multiple cloud services or a combination of public and private cloud resources (i.e., Rackspace hosting, S3 storage, etc.). Additionally, there may be layered dependencies (e.g., front end, database server, content distribution network) that require testing. Web application security assessments should cover aspects from the guidelines of the Open Web Application Security Project (OWASP) SysAdmin, Audit, Network Security (SANS) Institute, the Open Source Security Testing Methodology Manual (OSSTMM), and should include known Common Vulnerabilities

and Exposures (CVEs), irrespective of whether it is a third-party testing a cloud web application or a cloud-based assessment tool testing the web application.

3.0 Implementation Considerations and Concerns

Security assessments can be a complex task. The use of a SecaaS security assessment provider can simplify the execution of certain types of security assessments. However, there are considerations and concerns that should be taken into account when implementing a SecaaS security assessment. This section details some considerations and concerns that should be part of the decision-making conversation. This list is not meant to be all-inclusive, but is meant to trigger appropriate discussion.

3.1 Considerations

At multiple points during the software development lifecycle, there are requirements to do a variety of security assessments. As an organization determines which type of assessment environment to use, discussion should include the considerations below.

3.1.1 Accuracy and Coverage

Cloud service providers should offer reasonable assurance for the accuracy and coverage of the assessment. Assurance should be well supported with effective and efficient procedures and methodology. Coverage or assessment boundaries should be identified and verified by both the customer and provider. This enables and pinpoints security concerns and provides for the creation of a security mediation methodology.

An important consideration for any assessment is the minimization of false positives and false negatives. Service providers should explain how they ensure accuracy and minimize false positives and false negatives.

Assessment tools should support common standards or industry best practices such as CVE for vulnerability assessments, OWASP top 10 for web application assessment, NIST/CIS/FDCC/SANS guidelines and controls for compliance assessments.

3.1.2 Security Assessments of Public Cloud Environments/Systems

In some cases, the terms of service for an organization's use of a public cloud service (IaaS) may prohibit, restrict or limit the ability of a customer to launch a security assessment. Public cloud service providers may require advance notice and authorization before a security assessment is conducted. These restrictions are typically put in place to minimize the possibility of a disruption to another tenant in the public cloud.

As a potential consumer of a cloud-based security assessment as a service, you should consult with the specific terms of service for your public cloud service before conducting a security assessment against the environment.

3.1.3 Data Ownership

Service providers should offer a mechanism for users of the service to request their organization's data for the purposes of moving to another cloud-based service or to an enterprise-based service. This should be done in

such a manner that the information can be transferred in a secure fashion that adheres to industry standards such as an ODBC-like connector, a secure flat file or any similarly secure manner of transfer.

Data retention policies for all data stored by the service provider should be easily configurable.

Service providers should be able to provide instructions as to how organizations can request destruction/deletion of their data as well as the processes used to destroy/delete the customer's data.

Organizations may consider the data resulting from security assessments as sensitive, and may want attestation from the service provider of the proper disposal of their data in accordance with established procedures.

Additional consideration may be needed for the disposal of data residing on backup media. Because of the multi-tenant architecture, some service providers may not be able to delete a specific customer's data until a tape rotation cycle is complete, which could be as long as a year.

3.1.4 Integration with GRC Tools

In many organizations, governance, risk and compliance (GRC) is managed through dedicated tools. These tools often benefit from the results of security assessment services to manage the remediation of any findings, as well as the use of security assessments as part of a security program. Cloud-based security assessment services should provide a mechanism to integrate with GRC tools and share assessment results through an XML file, or an ODBC-like connector.

Due to the sensitive nature of the information that may be found during a security assessment, organizations also should consider how secure a mechanism they should use. Service providers should be able to provide multiple mechanisms which integrate with GRC tools to allow for different levels of security in relation to the handling and transfer of the data that is being provided to the GRC tools.

3.1.5 Programmatic Access and Control of the Service

Cloud-based security assessment services should provide the ability to perform assessments and provider automated reports. This is typically provided through a feature rich Application Programming Interface (API). The API should allow for the automation of all features and capabilities that are available through the standard interface. The API should provide a mechanism for the import and export of assessment configurations, as well as the resulting data. The API also should provide documentation on which parts of the database schema can be opened to allow for data exportation.

Changes to the API required to avoid potential loss of information deemed sensitive in nature by the customer should be especially well documented. Any automation tools should be well documented and readily made available to customers for evaluation.

3.1.6 Updates

Because they leverage a cloud architecture, SecaaS security assessment solutions should provide continuous updating to both the software itself and the libraries used in the assessments, vulnerabilities, controls, etc. Enquire as to how updates are performed, and the frequency of updates.

3.1.7 Standardized Ratings

Cloud-based security assessments should strive to use standardized ratings and identifiers in assessment reports. Standards exist in some areas, while in others they are still being discussed. Customers should look for support of Common Vulnerability Enumeration (CVE) and Common Vulnerability Scoring System (CVSS) (version 2 or later) in the vulnerability assessment areas, OWASP Top 10 in the web application security area, and support for FDCC and CIS in the configuration assessment areas.

3.2 Concerns

Concerns may include things such as points where data could be unencrypted, security or cloud vendor access to the data, separation of duties, and separation of logs when in multi-tenancy environments. The concerns listed below are not exhaustive of the possibilities, but are meant to trigger appropriate discussions of potential areas of concern when considering cloud-based security assessments as a service.

3.2.1 Legality & Non-Disclosure Agreement

Cloud-based service providers must ensure, to the reasonable extent possible, that the organization or person requesting assessment of a particular cloud resource or application is a bona-fide and legitimate representative of that resource (company or organization) and has the requisite authority to ask for such a security assessment.

The customer of a cloud-based security assessment service should ensure that no law, rule, or regulation exists which restricts sharing the confidential data of its users with another company/organization (internal or external/foreign). The consumer also should know of any deviations or relaxations allowed and their associated circumstances.

3.2.2 User Authentication and Account Management

The following are items that a customer should address within a Non-Disclosure Agreement with a cloud-based security service provider. This is not a definitive list, but rather a set of recommendations specific to the data that can be accessed, collected, and created during the course of a security assessment.

- Defined time limits on the confidentiality duration of all data collected, stored and/or reported against. This should include any and all by-products that might come from the customer's data and/or any document created in the process of the assessment.
- A detailed description of all parties (roles) who may access the customer's data, as well as to what extent each party is able to access said data.

- Validation that the NDA covers all forms that the data may take within the assessment process, to include reports and by-products of the data gathered, produced, and reported against.
- A statement identifying any and all individuals (roles) who can make changes to the NDA with regard to accessing the customer's data.
- Any special requirements which allow deviation from the NDA should be appropriately noted.

3.2.3 Data Security

Cloud-based security assessment service providers should be able to show they secure data during all stages of the data lifecycle. Service providers should be able to show how they secure data during each of its stages: in transit, in processing, and at rest. Service providers must offer adequate attestation for the isolation of tenant data. The following should be validated when assessing service providers:

- How providers are isolating the data.
- If providers are storing data in database containers, details as to how each container is secured.
- Measures in place to prevent data being presented to unauthorized users.
- That users and administrators cannot gain unauthorized access to their information.

3.2.4 Security Assessment Credentials

Data used in security assessments and the related details that result from a security assessment are sensitive in nature and should be handled appropriately. Only authorized individuals should be allowed access. Cloud-based security assessment service providers should be able to ensure that only authorized personnel are allowed to use the service to conduct security assessments, or review assessment information.

Service providers should ensure secure management of user accounts for employees, customers, and third-party organizations (such as auditors) accessing or using the cloud-based security assessment service. Account management features should include account creation, deletion and account permissions and roles, as well as the ability to approve or deny the creation of new accounts at the customer level.

Consumer organizations should determine whether normal user authentication meets their needs, or if there is a need to require stronger authentication protocols such as two (2) factor or multi-factor authentication. Service providers should be able to produce detailed authentication and activity records or logs for user sessions, and have the ability to store the records/logs to meet industry log retention standards.

Service providers must be able to provide, at a minimum, the following control mechanisms to be able to attest that credentials given/used during the Security assessments are held in a confidential manner:

- Who has access to the account credentials provided during the assessment.
- How passwords given to the service provider are stored in a secure fashion, such as being hashed with an appropriate algorithm.
- Validation that account credentials and passwords are deleted upon request of the user and/or the end of the assessment period.

- Validation that a log of deleted users, as well as the roles that they possessed, is being held for log retention purposes.

3.2.5 Secure Communication

Each organization should evaluate its requirements for how secure the communication between external products and the service provider should be. Below are some questions that should be answered before deciding on a service provider.

- Is any/all of the communication between external products and the service provider via automation tools, such as APIs, done in a secure fashion? If not, can it be configured to allow for said communication to be done securely?
- Is the database schema opened up to allow for direct communication with the automated tools? If so, are there mechanisms in place to restrict what portions of the schema can be used?
- Are there mechanisms in place to ensure that the automation tools cannot gain access to parts of the schema and/or any data in general that the customer may deem sensitive in nature and does not want to allow access to by automated tools?

3.2.6 Penetration Testing

Penetration testing is potentially the most disruptive assessment type. As cloud computing has changed the concept of a well-defined security perimeter, and many cloud services are located and consumed outside the organizational security perimeter, the lack of a well-defined perimeter will impact how penetration tests are conducted

When conducting penetration testing assessments of a cloud environment, special consideration must be given to the multi-tenant nature of the environment and the potential disruption to other organization's systems.

Organizations may not be able to conduct a full end-to-end internal penetration test of a cloud hosting provider, and may have to rely on attestation by the provider that testing is conducted. Organizations should understand what type of testing they will be allowed to conduct before selecting a cloud provider's security initiatives.

Testing should be coordinated in advance with the hosting provider. Notify the cloud provider of testing procedures to prevent the triggering of the Incident Response process of the provider.

4.0 Implementation

Section 4 is a highly technical discussion of the architecture of a security assessment implementation, and guidance and steps required for the successful implementation of security assessments as a service. This material is written for system architects, designers and developers, and those charged with the implementation of cloud-based Security Assessments.

4.1 Architecture Overview

Security assessments that are provided as a service from a cloud platform may have different architectures. However, all will share some common architectural components. From the consumer's viewpoint, SecaaS security assessments are seen as SaaS. However, companies providing SecaaS security assessment services can have a variety of different architectural models including private clouds, IaaS or PaaS.

Service providers can deliver their services from a private cloud in which the infrastructure comprising Security as a Service is fully owned and managed by the provider of the service. In this model, while the service itself may be a public, multi-tenant cloud SaaS offering, the underlying infrastructure is a private cloud.

Service providers also can deliver their services from a public cloud in which the infrastructure of the SecaaS platform relies upon a public cloud IaaS or PaaS delivery model. Some SecaaS service providers integrate SaaS delivered solutions into their architecture for security assessment services platforms.

Some public cloud service providers are reacting to customer concerns about security assessments and are building security assessment capabilities into their IaaS public cloud infrastructure offerings. This architecture provides the consumer of public cloud services with security assessment capabilities without having to install software or virtualized assessment appliances, and may reduce costs for the consumer by eliminating the compute and storage costs for the security assessment appliance.

4.1.1 Internet vs. Internal Enterprise Assessments

Cloud-based security assessment services are able to assess any system that is accessible via the Internet, but internal assessments by cloud-based security assessment services often are implemented through the use of managed appliances or software agents that are deployed within the enterprise. Customers of a cloud-based security assessment service should consider the following when selecting a service provider with regard to understanding Internet vs. internal assessments:

- Service providers that use appliances should be able to validate that their appliances are able to hold and transfer all data in a secure manner.
- Service providers should deploy any and all appliances in such a manner that all access to the appliances can be controlled, logged, and reported.

Service providers should be able to validate that their appliances have the ability to ensure for the permanent destruction/deletion of all data on the device upon request, as well as at the end of an assessment.

4.1.1.1 Appliance and Agent Architecture

Customers should determine if the SecaaS solution provider's architecture provides the scalability necessary for the security assessment to be conducted. The nature of the cloud provides inherent scalability, but specific vendor architecture will impact the overall scalability. While the bulk of the platform that provides SecaaS security assessment services will rely upon a cloud-based platform, there may be components of the architecture that are outside of platform. For example, in order to provide security assessment services for internal systems, components of the security assessment platform may need to be deployed inside the customer's environment.

Access to the internal environment can be accomplished through the use of hardware or software. Hardware-based solutions for assessing the internal environment typically involve the deployment and installation of an appliance that has network visibility to the internal systems to be assessed.

Security assessment appliances can be physical devices or virtualized appliances that can be installed into a customer's virtualized environment. Appliances usually can support the assessment of thousands of systems, and scalability is accomplished by introducing additional appliances. Appliances typically are managed by the SecaaS service provider, which results in minimal system management impact to the customer organization.

Software-based solutions for assessing the inside environment typically involve the use of "agent" software that is installed on all of the customer's internal systems to be assessed. Agent-based solutions have the advantage of not requiring the installation of any hardware, and the agent has more detailed visibility of the system. However, installing an agent on every system has operational impact to the organization. The number of systems involved may require the use of a mature software distribution process, which may complicate system management issues, as responsibilities for security assessment and system management usually are not within the same organizational group. Additionally, agent-based solutions may require thorough testing to ensure compatibility with the host system.

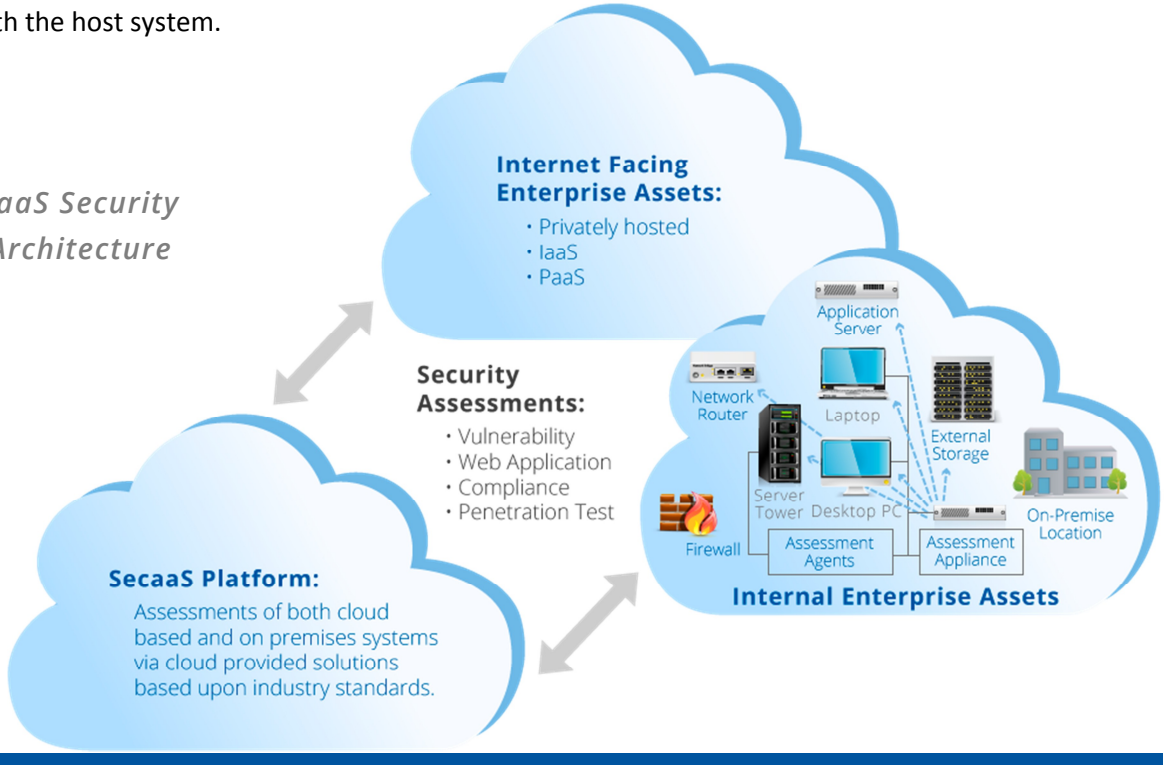

Figure 2: SecaaS Security Assessment Architecture

4.2 Guidance and Implementation Steps

Implementation of cloud-based security assessments are focused on planning and rollout phases, but have only minimal components of physical implementation steps. Organizations should focus on defining the objectives for the assessment and development of the processes for making use of the resulting data.

An accurate inventory and mapping of the security and compliance state of the network devices, systems, and applications is essential for the conscious management of risk for an organization's critical information and systems.

4.2.1 User Authentication and Account Management

Organizations should keep the following guidelines in mind when selecting a cloud-based security assessment service:

- Account management features should allow for the creation, deletion and management of account permissions and roles in an easy to use web format.
- The service provider should offer the ability to approve/deny the creation of new accounts at the customer level.
- User authentication needs must be clearly definable, and stronger authentication protocols such as two-factor or multi-factor authentication must be supported.
- The service provider should be able to provide detailed authentication and activity records/logs for user sessions in a format which the can be viewed at any time by the customer.
- The service provider should have the ability to store the records/logs to meet industry log retention standards.

4.2.2 Network and System Vulnerability Assessments

Vulnerability management is the process of systematically identifying and remediating vulnerabilities in devices that are connected to a network. Vulnerability management services typically include asset discovery; asset classification; scanning profile management; vulnerability scanning; analysis, correlation and prioritization of vulnerability scanning results; reporting; remediation management; verification of remediation through scanning; workflow management and scheduled scanning.

Vulnerability assessment is commonly regarded as either external or internal. External vulnerability assessment is conducted from the Internet against publicly routable IP networks. Internal assessments are conducted from inside an organizations environment, typically inside the perimeter security appliances (firewalls).

The implementation of a vulnerability management SecaaS is typically not technically challenging. In fact, the ease of implementation is one of the principle advantages of using SecaaS vulnerability management. Many of the implementation steps are similar to those required for an enterprise vulnerability management solution.

4.2.2.1 Identify the Scope of the Program/Assessment

Which systems and networks will you conduct security assessments against? Will you assess your entire infrastructure, or will you start with a subset of your infrastructure? If you are replacing an Enterprise vulnerability management program with SecaaS, you probably will replicate exactly what you have done with the Enterprise solution. If this is a new vulnerability management program, you may want to start with a subset of your infrastructure to develop the internal processes and procedures necessary to have a successful program.

4.2.2.2 External Only, or Internal and External

Decide if you will assess only Internet facing (external) systems, or if you wish to assess internal systems too. Assessing internal systems typically requires the deployment of scanning appliances into your internal environment. Sizing the number of scanning appliances necessary is often dependent upon the network architecture of your environment. Some SecaaS security assessment solutions can benefit from additional scanning appliances resulting in reduced scanning times.

If you decide to conduct internal scanning, you also will need to decide if you will use authenticated scans inside the environment. Authenticated scans require that the scanning system have a set of credentials to allow more access to the system, which provides more information. However, you will need to understand how the SecaaS provider manages, protects and stores the authenticated scanning credentials. Some SecaaS vulnerability management vendors offer the ability for the scanning appliances to obtain the authenticated scanning credentials as needed from credential vault systems. In this case, the SecaaS provider does not retain the credentials, and the authentication vault provides a centralized point of control.

4.2.2.3 Integration with Existing Tools

SecaaS vulnerability management tools often integrate with other IT tools such as inventory management systems, GRC management tools, workflow management (ticket) tools and others. You may be able to integrate the SecaaS vulnerability management solution with several other tools, providing more information and a greater level of integration with business processes.

4.2.3 Server/Workstation Compliance Assessments

Organizations should decide whether a pure cloud-based assessment will be able to give them a complete assessment, or if an appliance should be used to allow for assessing their environment both externally and internally.

Service providers should:

- List all supported devices and products and, if applicable, provide minimal configurations settings needed for a successful assessment for each device.
- Have the ability to conduct authenticated/anonymous scans or use a resident agent to detect server/workstation configurations.
- Have the ability to compare discovered configurations with industry best practices or custom configuration standards to determine compliance.

- Validate that compliance controls have the ability to map to industry standards to demonstrate that each mechanism used during the assessment complies with each portion of the standards being assessed against.
- Allow customers the ability to create custom standards templates and import/export custom templates.
- Allow customers the ability to conduct both ad hoc and scheduled assessments to scan for baseline configuration compliance and/or vulnerability detection, both at scheduled intervals and as assessments on demand.
- Have the ability to import vulnerability results from third-party vulnerability scanners.
- Allow for data to be collected, stored and transferred in a secure fashion regardless of whether collected with or without an agent. This is typically done using one or both of the following technics:
    - An agent-based solution which can secure all data both in-transit and at rest.
    - An appliance that can collect the data on the customer's internal network, then store and transfer all data collected, in a secure fashion, to the service provider.
- Allow for the ability to use GRC tools and third-party data sources to validate non-technical controls within the assessment.

4.2.4 Network/Security System Compliance Assessment

Organizations should decide whether a pure cloud-based assessment will be able to give them a complete assessment or if an appliance should be used to allow for assessing their environment both externally and internally.

Service providers should:

- List all supported devices and products and, if applicable, provide minimal configurations settings needed for a successful assessment for each device.
- Support a wide range of network and security devices.
- Have the ability to assess not only the device configuration, but also any specific security or network policies implemented by the device (routing policies, firewall policies, IDS policies, etc.).
- Have the ability to assess against device-specific vulnerabilities and/or use vulnerability information collected from third-party scanners within the assessment process.
- Be able to provide a report or dashboard like interface through which to view the results of the assessment, as well as the overall risk level assigned, based on the assessment results.

4.2.5 Web Application Security Assessments

Web application security assessments automate the process of scanning web applications for security vulnerabilities. Traditional approaches include black-box testing where the web application is tested from the vantage point of an outside attacker, without knowledge of its architecture and source code, white-box testing where the focus of the testing is on the source code for the web application and hybrid testing where both outside testing and source code analysis are combined.

Cloud-based web application assessment tools, with few exceptions, focus on the black box approach. For these tools, the following guidelines should be included in your evaluation.

- Detection: the assessment tool should address the most common areas of deficiencies, which include cross-site scripting flaws, file-inclusion issues, direct object references, directory traversal, information leakage, session management and SQL injection issues. A detailed list of top issues for assessment tools to detect can be retrieved at OWASP at their Top 10 ranking and the SANS Top 25 Software Errors (CWEs).
- Completeness: the assessment tool should be able to exercise the web application under test as completely as possible. The reach of the crawler in the assessment tool is important to the efficiency of the assessment that ultimately includes also its support to follow the navigation links used by modern web programming techniques (CSS, JavaScript).

4.2.6 Overall Testing

Web applications testing is a fast moving field that is still under heavy development, with few accepted standards. Web application themselves have been changing quickly and extensively, making comprehensive testing a complex task, especially if the web application utilizes multiple cloud services or a combination of public and private cloud resources (i.e. Rackspace hosting, S3 storage, etc.). Additionally there are usually layered dependencies between front-end, application servers and databases that might require independent testing.

4.2.7 Virtual Infrastructure Assessment (Cloud/Hypervisor Infrastructure)

In some cases, the ability to assess the security of a cloud or virtualized environment is similar to a network and system vulnerability assessment. However, the assessment tool must have an understanding of the underlying virtualization technology, and support the identification of potential vulnerabilities within the virtualization/cloud management layer.

Virtual Infrastructure Assessments are typically aimed at the management components of the virtual environment. These assessments can be conducted against an environment managed by the organization or a third-party provider.

Conducting a security assessment of a third-party provider's virtual infrastructure is a complex task. Many providers will limit the ability of consumers to test the virtual infrastructure because the testing could adversely impact other customers and possibly identify weaknesses of other customers in a multi-tenant environment. Specific guidance is listed below.

First, identify and understand the type of virtualization being used by the provider. This will allow you to identify the best assessment methodology. The best security practices for that type of virtualization should be identified. The controls listed in those best practices should be assessed. Ideally, a consumer will have this data prior to migration to the cloud.

Regardless of the virtualization platform, the following areas should be assessed:

- Access controls to the virtualization management system
- Personnel with access to the control or management systems for the hypervisor
- Remote access to the control or management systems for the hypervisor
- Virtual operating system isolation (virtualized systems should be isolated from each other)
- Active but unused services on the hypervisor (e.g., unused hardware, clipboard, file sharing, etc.)
- Physical security measures, to protect from unauthorized access
- Patch levels for the hypervisor, ensuring the most current patches are in place (particularly security patches)
- Virtual switch configurations
- Security practices and vendor guidance for the virtualization system in use

4.2.8 Reporting and Sharing Resulting Data

Customers of a cloud-based security assessment service should keep the following in mind when selecting a service provider with regard to Reporting and Sharing Resulting Data:

- Service providers should provide the resulting assessment data in both formatted humanly readable and exportable machine readable versions in non-proprietary formats, like Cyberscope, Security Content Automation Protocol (SCAP), Common Vulnerability Reference Format (CVRF) or Extensible Markup Language (XML).
- Customers looking to implement recurring assessments, or continuous monitoring and auditing systems, should verify that the service provider has the ability to store historic data in a secure environment, provide trend analysis and compare the data to current assessments.
- Service providers should provide the ability to identify who can view and/or export data, as well as the type of data that can be viewed and/or exported.
- Security/risk ratings should seek to combine the results of multiple security assessment types to present an overall risk rating that can be used as an indicator of the overall security posture of an organization. There are several commonly accepted rating systems such as the Common Vulnerability Scoring System (CVSS).
- When selecting a cloud-based security assessment, the provider's rating method should be aligned with the current organizational security/risk rating system. While service providers may use proprietary rating systems, systems that provide only proprietary ratings should be avoided. Instead, service providers should incorporate either industry standard rating systems, or a combination of proprietary rating systems, industry standard rating systems, and custom ratings to allow organizations to tailor risk scoring to their organization and organizational business processes.
- Reports should include detailed descriptions of all rating systems used during the assessment process, as well as any deviations to standard ratings made by the customer.

5.0 References and Useful Links

5.1 References

Cloud Security Alliance. (2011). CSA Defined Categories of Service 2011. Retrieved from https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

Industry Consortium for Advancement of Security on the Internet. (2012). The Common Vulnerability Reporting Framework (CVRF) v1.1. Retrieved from http://www.icasi.org/cvrf-1.1

Qualys. (2008) Vulnerability Management for Dummies. Retrieved from http://www.qualys.com/forms/ebook/vulnerability_management_dummies/

The Open Web Application Security Project. (2011). OWASP Testing Guide V4. Retrieved from https://www.owasp.org/index.php/Category:OWASP_Testing_Project

US Department of Commerce, National Institute for Standards and Technology. (2008). Technical Guide to Information Security Testing and Assessment. NIST SP-800-115. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

US Department of Commerce, National Institute for Standards and Technology. (2008, January). Software Assurance Tools: Web Application Security Scanner Functional Specification. NIST SP 500-269. Retrieved from http://samate.nist.gov/docs/webapp_scanner_spec_sp500-269.pdf

US Department of Commerce, National Institute for Standards and Technology. (2008, January). Creating a Patch and Vulnerability Management Program. NIST SP 800-40. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

US Department of Commerce, National Institute for Standards and Technology. (2011, January). Guide to Security for Full Virtualization Technologies. NIST SP 800-125. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

5.2 Useful Links

Other trusted links that may be of use to those seeking (cloud-based) security assessment information or advice.

ISECOM Software Testing Checklist (Stick)
http://www.isecom.org/research/stick.html

ISECOM Attack Surface Metrics
http://www.isecom.org/research/ravs.html

Penetration Testing Execution Standard (PTES)
http://www.pentest-standard.org/index.php/Main_Page

Open Vulnerability Assessment Language (OVAL)
http://oval.mitre.org/

Security Content Automation Protocol (SCAP)
http://scap.nist.gov/

Open Source Security Testing Methodology Manual (OSSTMM)
http://www.isecom.org/research/osstmm.html

A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0
http://www.first.org/cvss/cvss-guide.html

CSA - Defined Categories of Security as a Service 2011
https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

CSA - Security Guidance for Critical Areas of Focus in Cloud Computing V.3
https://cloudsecurityalliance.org/research/security-guidance/

NIST SP-800-115 - Technical Guide to Information Security Testing and Assessment
http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

ISO 27K Standards
http://standards.iso.org/ittf/PubliclyAvailableStandards/

FedRAMP – Federal Risk and Authorization Management Program
http://www.gsa.gov/portal/category/102371

NERC – Reliability Standards - Critical Infrastructure Protection (CIP)
http://www.nerc.com/page.php?cid=2%7C20

Cyberscope, NIST
http://scap.nist.gov/use-case/cyberscope/

Shared Assessments
http://sharedassessments.org/about/

PCI Data Security Standard (DSS)
https://www.pcisecuritystandards.org/security_standards/index.php

NIST SP 800-40 - Creating a Patch and Vulnerability Management Program, version 2.0
http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

Vulnerability Management, Park Foreman, CRC Press, 2010
http://www.crcpress.com/product/isbn/9781439801505

CVE – Common Vulnerabilities and Exposures, Mitre
http://cve.mitre.org/

The Common Vulnerability Reporting Framework (CVRF) v1.1, ICASI
http://www.icasi.org/cvrf-1.1

Security Content Automation Protocol (SCAP)
http://scap.nist.gov/

Open Vulnerability Assessment Language (OVAL)
http://oval.mitre.org/

A Complete Guide to the Common Vulnerability Scoring System (CVSS)
http://www.first.org/cvss/cvss-guid

FDCC – Federal Desktop Core Configuration
http://nvd.nist.gov/fdcc/index.cfm

OWASP Testing Guide
https://www.owasp.org/index.php/Category:OWASP_Testing_Project

NIST SP 500-269 - Software Assurance Tools: Web Application Security Scanner Functional Specification
http://samate.nist.gov/docs/webapp_scanner_spec_sp500-269.pdf

CWE - Common Weakness Enumeration, Mitre
http://cwe.mitre.org/top25/index.html

SANS – Top 25 Most Dangerous Software Errors
http://www.sans.org/top25-software-errors/

Open Source Security Testing Methodology Manual (OSSTMM)
http://www.isecom.org/research/osstmm.html

ISECOM Software Testing Checklist (Stick)
http://www.isecom.org/research/stick.html

ISECOM Attack Surface Metrics
http://www.isecom.org/research/ravs.html

NIST SP 800-125, Guide to Security for Full Virtualization Technologies
http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

Penetration Testing Execution Standard (PTES)
http://www.pentest-standard.org/index.php/Main_Page

