



OPEN DATA CENTER ALLIANCESM USAGE: SECURITY MONITORING

LEGAL NOTICE

© 2011 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.

This “Open Data Center AllianceSM Usage: Security Monitoring” is proprietary to the Open Data Center Alliance, Inc.

NOTICE TO USERS WHO ARE NOT OPEN DATA CENTER ALLIANCE PARTICIPANTS: Non-Open Data Center Alliance Participants only have the right to review, and make reference or cite, this document. Any such references or citations to this document must give the Open Data Center Alliance, Inc. full attribution and must acknowledge the Open Data Center Alliance, Inc.’s copyright in this document. Such users are not permitted to revise, alter, modify, make any derivatives of, or otherwise amend this document in any way.

NOTICE TO USERS WHO ARE OPEN DATA CENTER ALLIANCE PARTICIPANTS: Use of this document by Open Data Center Alliance Participants is subject to the Open Data Center Alliance’s bylaws and its other policies and procedures.

OPEN CENTER DATA ALLIANCESM, ODCASM, and the OPEN DATA CENTER ALLIANCE logoSM are service marks owned by Open Data Center Alliance, Inc. and all rights are reserved therein. Unauthorized use is strictly prohibited.

This document and its contents are provided “AS IS” and are to be used subject to all of the limitation set forth herein.

Users of this document should not reference any initial or recommended methodology, metric, requirements, or other criteria that may be contained in this document or in any other document distributed by the Alliance (“Initial Models”) in any way that implies the user and/or its products or services are in compliance with, or have undergone any testing or certification to demonstrate compliance with, any of these Initial Models.

Any proposals or recommendations contained in this document including, without limitation, the scope and content of any proposed methodology, metric, requirements, or other criteria does not mean the Alliance will necessarily be required in the future to develop any certification or compliance or testing programs to verify any future implementation or compliance with such proposals or recommendations.

This document does not grant any user of this document any rights to use any of the Alliance’s trademarks.

All other service marks, trademarks and trade names referenced herein are those of their respective owners.



OPEN DATA CENTER ALLIANCESM USAGE: SECURITY MONITORING

EXECUTIVE SUMMARY

In many organizations today, there is a significant push towards introducing cloud computing into the enterprise. The hope is that the cloud's multi-tenant, shared infrastructure will enable greater computing efficiency and flexibility. At the same time, organizations require that compute platforms are secure and comply with all relevant rules, regulations and laws. These requirements must be met whether using a dedicated service available via a private cloud or a service shared with other subscribers via a public cloud.

There's no margin for error, or security breaches. According to a research study conducted by the Ponemon Institute and Symantec, the average organizational cost of a data breach in 2010 increased to \$7.2 million, and the cost of lost business was about \$4.5 million. It is the high cost of breaches — and inadequate security monitoring capabilities offered as part of cloud services — that pose a barrier to the wider adoption of cloud computing and create resistance within organizations to public cloud services.

The Open Data Center AllianceSM recognizes that security is the biggest challenge organizations face as they plan for migration to cloud services. Organizations must be able to monitor and verify that their security requirements are being met. This Usage Model is designed to provide organizations with a standard monitoring framework and relevant interfaces that will let them query the status of security and compliance within the services they procure from providers.

PURPOSE

The Security Monitoring Usage Model requests that the industry develop and drive adoption of a standard interface that permits the organization subscribing to the cloud services to query the actual security status of specific elements of a provider's services. In an Infrastructure as a Service (IaaS) offering, these may include security status of a virtual machine. In a Platform as a Service (PaaS) or Software as a Service (SaaS), the patch status of a piece of software may be important. In both of these cases (PaaS and SaaS), applications are provided through the cloud and their update status would need to be monitored.

It is envisioned that this Usage Model will support the monitoring (via a standard interface) of the security levels described and contained within the Provider Security Assurance Usage Model. This would provide the subscriber with a real-time assessment of their security posture and allow the subscriber to determine if the service meets the security requirements specified in its service agreements.

The Alliance supports early efforts in this area (such as those being developed by CloudAudit and the Cloud Security Alliance, or CSA) and seeks to aid these groups in assisting in the creation of common standards that meet the requirements of this Usage Model and the principles of the Alliance.

Access to this information would be secured to each subscriber to prevent the data from being used by unauthorized parties to exploit the cloud environment. Furthermore, the output would be provided in a standardized form to allow individual enterprises to collect data from multiple vendors and conveniently combine these feeds into their own enterprise reporting systems. The Alliance requests that industry standards organizations develop a framework, format and syntax for this standardized form to allow standards-based automation tools to be developed to support this usage.

The data will be maintained by the provider in real time, allowing the subscriber to ascertain security levels at any given point in time. The onus is ultimately on the subscriber to ensure its compliance reporting meets all geographical and industry-based regulations.

It should be noted that this Usage Model addresses similar concerns to the CloudAudit (A6 API) standard currently in development with the CSA. It also shares elements with usage cases and standards under development at the National Institute of Standards and Technology (NIST).

The Alliance will work closely with CloudAudit and NIST to align the Alliance requirements with these activities. The Alliance believes that the technical standards required to make this provider security monitoring usage robust and effective are in their infancy. We encourage interested parties to actively participate in driving a complete set of compliance monitoring standards to meet local, national, global and industry technical requirements. We also encourage solution providers to create implementations of solutions based on open standards that organizations subscribing to cloud services, the providers of those services, and regulators can assess for compliance with this Usage Model and the industry specifications as they develop.

TAXONOMY

Actor	Description
Cloud-Subscriber	A person or organization that has been authenticated to a cloud and maintains a business relationship with a cloud.
Cloud-Provider	An organization providing network services and charging Cloud-Subscribers . A (public) Cloud-Provider provides services over the Internet.
Cloud-Compliance-Agency	An accredited entity that is responsible for ensuring the compliance to cloud security standards. A Cloud-Compliance-Agency may also be a third party trusted by the Cloud-Subscriber . They could then determine and monitor the security state of the Cloud-Provider and respond to the Cloud-Subscriber when requested.
Cloud-Standards-Body	An entity responsible for setting and maintaining the cloud security standards as defined in this Usage Model.

Note: Actors shown in normal case are identical to those provided within NIST Usage Models; those shown in italics are created specifically for the Alliance Usage Model detailed below. The descriptions provided for the NIST actors are taken directly from NIST (and have not been modified) and may, in some cases, be for reference only and may not be used within the Alliance Usage Models. Where the description for the NIST actor is seen as inappropriate for Alliance use, a new actor class has been created.

USAGE REQUIREMENTS

With a Security Monitoring Usage Model, particularly one integrally tied to security assurance functions, controls are a vital component. As such, it is helpful to assign greater import and focus in functions that have incrementally higher demonstrated security benefit on the basis of how a function is implemented. Two of the critical attributes from an implementation perspective include:

- Tamper-resistant functions providing generally stronger levels of control and assurance against “spoofing” of results. This is, as expected, an incremental benefit for the integrity of the security process and may provide enhanced auditability of the security environment through hardened features or discrete and immutable reporting elements.
- Providing dedicated capabilities with specific resources reserved for specific customers. This promises to eliminate some of the concerns of “shared” resources—though such a model would likely assume increased costs and perhaps limitations on scalability for the **Cloud-Subscriber** as well as the **Cloud-Provider**.

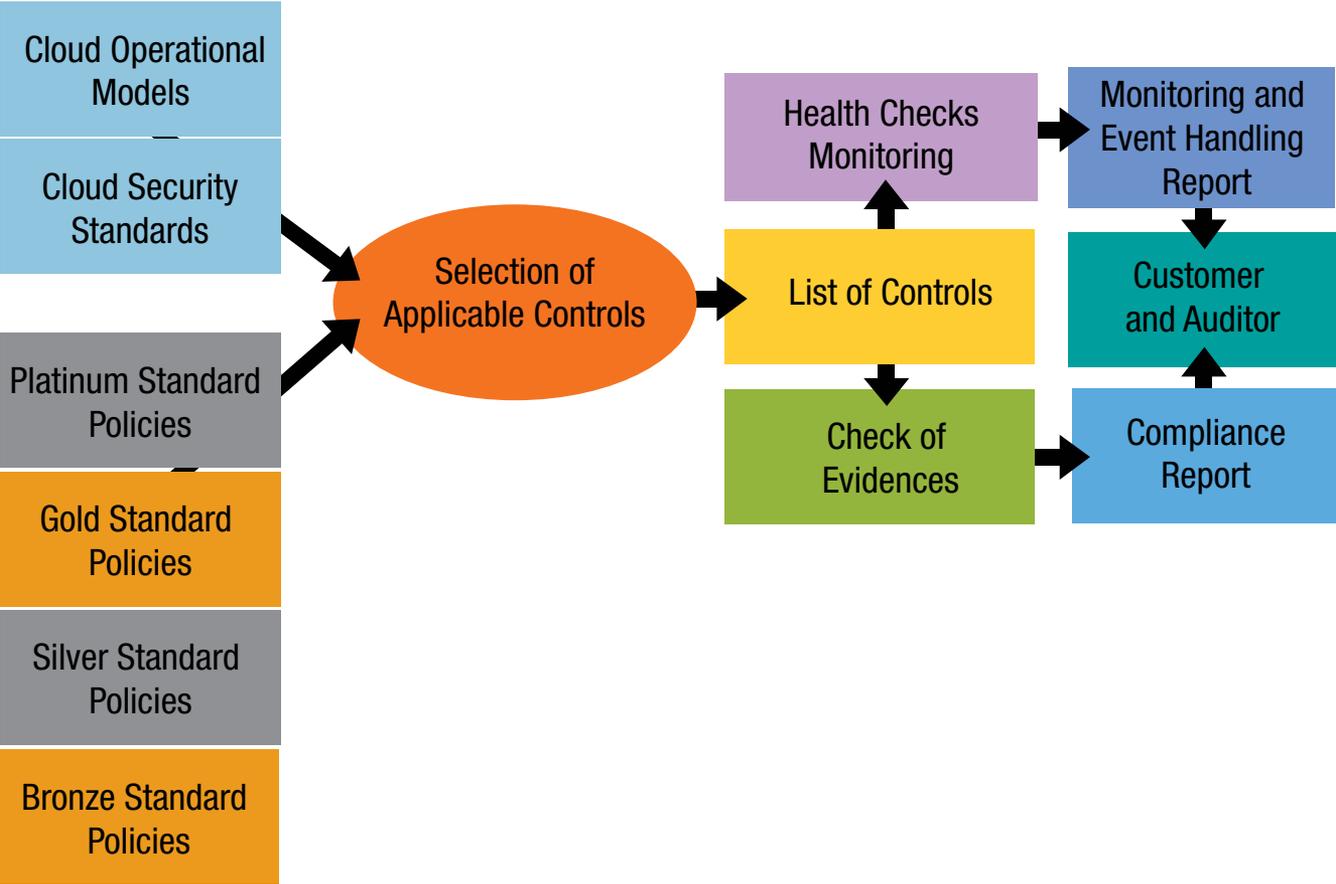
These attributes often will be seen as capabilities that differentiate different classes of services in the Provider Security Assurance Usage Model. It will therefore be useful for the **Cloud-Subscriber** in the Security Monitoring Usage Model to be able to determine that a **Cloud-Provider** is delivering these capabilities at the contracted levels. This will likely require the development or evangelization of Application Programming Interface (API) sets or other mechanisms that are capable of gaining low-level platform (server, networking infrastructure and even facilities) information that can correlate with service agreement specifications and are capable of providing these through specified, access-controlled service portals.

Some of the critical API sets or mechanisms that will be required by the Security Monitoring Usage Model include features that enhance the control, management, reporting and audit of the security environment. The model should span:

- Patch management and version control APIs, with audit/query function
- Identity management services and APIs for consolidation and federation of access control
- Platform Trust APIs (system trust, identity and geographic position/platform location established by the root of trust can be consumed by control, monitor and audit functions)
- API for import/export to **Cloud-Subscriber** log systems from cloud Security Information Event Management (SIEM) systems
- Audit/Query APIs for platform attributes (CPU, memory, chipset security, virtualization features, BIOS revisions)
- Cryptographic Key Management APIs for the deployment, use and escrow of cryptographic keys in cloud and enterprise infrastructures
- Facilities and resource management APIs for dynamic data and access to static and offline data (such as facilities control logs)
- “Peer service” monitor APIs to verify that **Cloud-Subscriber** workload is not on shared resources with specific list of blacklisted peers or being negatively impacted by oversubscribing peer service (e.g., “noisy neighbor”)
- Network traffic and threat analysis services and APIs for controlling and reporting on the infrastructure to mitigate malware and denial-of-service (DoS) attacks

Some of these API sets exist today. Others exist (or are defined within other standards organizations), but may require extensions for the Provider Security Assurance Usage Model. Still others will need to be developed by the industry to support specified uses. Most of these enhancements will fall under the “further actions” statements below, and subsequent revisions of this document will identify the specific API and mechanisms needed to assure that the industry is aligned to specific common methods.

USAGE MODEL DIAGRAM



USAGE MODEL DETAIL

Goals:

To provide a standardized monitoring framework, format and syntax for monitoring the standards defined in the Provider Security Assurance Usage Model, plus provide a view of the actual status of assets that exist in the cloud.

Assumptions:

Open Data Center Alliance Provider Security Assurance Usage Model is actively used as a basis for this Security Monitoring Usage Model.

Success Scenario 1 (full):

Cloud-Providers provide a secure web-based interface, which allows the **Cloud-Subscriber** to get a report of the actual status of the cloud services that they purchase. For example, the web interface would allow the **Cloud-Subscriber** to get anti-virus definition status, IPS events and firewall logs. Note: this Usage Model is for information gathering only. Active actions such as remediation and performing more vulnerabilities scans will not be performed using this tool.

Failure Conditions 1:

- Inconsistent, incomplete or tampered reporting (e.g., gaps in heartbeats or health checks, out-of-band values without documented remediation action, integrity check does not match).
- Unacceptable delays in gathering and preparing the reporting data, or having out-of-date data, without sufficient notification to the **Cloud-Subscriber**.

Success Scenario 2 (partial):

Cloud-Providers provide a standard interface (such as CloudAudit A6 API) that permits the **Cloud-Subscriber** to query security status of the purchased assets in order to get a real-time security status. **Cloud-Providers** should present this interface through a web-based monitoring facility to **Cloud-Subscribers** and to the **Cloud-Compliance-Agency**. **Cloud-Subscribers** should implement their own cloud monitoring infrastructure.

Failure Conditions 2:

- **Cloud-Providers** supply the service, but fail to allow real-time access to the data (e.g., authorization issues or other access problems).
- A **Cloud-Provider's** web-monitoring application does not comply with the monitoring standard as defined by the **Cloud-Standards-Body**.
- The **Cloud-Provider's** data is falsified and so incorrectly represents the status of the service.
- Delays or Failure to respond to queries due to the **Cloud-Provider** having insufficient service capacity to handle volume of real-time monitoring.

Failure Handling:

Security issues and other failure scenarios would be addressed by the contractual agreements between the **Cloud-Subscriber** and **Cloud-Provider**. It is envisioned that, depending on the nature of the failure, there would be progressively increasing penalties.

SUMMARY OF INDUSTRY ACTIONS REQUIRED

In the interest of giving guidance on how to create and deploy solutions that are open, multi-vendor and interoperable, we have identified specific areas where the Alliance believes there should open specifications, formal or de facto standards, or common IP-free implementations. Where the Alliance has a specific recommendation on the specification, standard or open implementation, it is called out in this Usage Model. In other cases, we will be working with the industry to evaluate and recommend specifications in future releases of this document.

The following are industry actions required to refine this usage model:

1. Collaboration between the Open Data Center Alliance, CSA and NIST on security monitoring. Particular focus areas shall be to align to or document support for:
 - Inclusion in current and emerging industry specifications (such as PCI-DSS, ISO, COBIT, FedRAMP and others) addressed by CSA and NIST—including emphasis on continuous monitoring and schedulable recurring capabilities with granular reporting capabilities (e.g., FedRAMP), workload boundary control and monitoring (e.g., NIST FISMA SP800-53), and services provisioning/de-provisioning (e.g., PCI-DSS 2.2.2)
 - New or unique Provider Security Assurance Usage Model capabilities that are not in current or in-process NIST and CSA standards
 - Useful access methods or API sets that are not included in current or in-process A6 API suites
 - NIST SCAP controls and standard formats for monitoring and reporting on security attributes, features and events across spectrum of Provider Security Assurance Usage Model requirements
 - Support for granular capabilities that may be required in tiered service level offerings (e.g., different access levels or functional basis for “bronze” versus “gold” service levels of the Provider Security Assurance Usage Model)
 - Encouragement and cultivation of development of ISACA expertise set, best known methods (BKMs), and standards for Alliance Provider Security Assurance Usage Model audit
 - Encouragement of market adoption of recommendations in the Provider Security Assurance Usage Model and for documentation of success/failure criteria as part of boilerplate Service Level Agreement (SLA) documents

APPENDIX

Relevant/Related Standard Groups and Bodies

- Security Content Automation Protocol (SCAP): <http://scap.nist.gov/>
- CloudAudit: <http://cloudataudit.org/>