



OPEN DATA CENTER ALLIANCESM USAGE: PROVIDER SECURITY ASSURANCE

LEGAL NOTICE

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

This “Open Data Center AllianceSM Usage: Provider Security Assurance” 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: PROVIDER SECURITY ASSURANCE

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 unclear and inadequate security assurances 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. This Usage Model provides standard definitions of security for cloud services, details mechanisms for service providers to demonstrate compliance, and gives organizations the ability to validate adherence to security standards within cloud services.

PURPOSE

This Usage Model seeks to define requirements for standardized definitions of security levels within the cloud. Used with the companion Alliance Usage Model on Security Monitoring, it will enable **Cloud-Subscribers** to:

- Ensure that a **Cloud-Provider** meets certain standards and common levels of security
- Compare security levels between different providers of cloud services and between internally and externally hosted clouds
- Enable organizations that subscribe to cloud services to make more informed choices on the levels of security they may want to adopt, based on the confidentiality, integrity and availability requirements of their hosted solutions

The intent for this Usage Model is to define the security requirements for cloud computing and implement a framework to assure against them. To do this, the Usage Model seeks to define minimum levels for cloud security within tiers. These tiers will provide offerings with increasing levels of security to meet the requirements of organizations that subscribe to cloud services. These levels are:

Assurance Levels	Level Description
Bronze	Basic Security
Silver	Enterprise Security equivalent
Gold	Financial Organization Security equivalent
Platinum	Military Organization Security equivalent

Through the use of these assurance standards (i.e., delivering accredited Platinum, Gold, Silver or Bronze services), the **Cloud-Provider** will be able to show demonstrable evidence of its security posture. This will then allow the provider to issue templated responses to answer potential customer security concerns. This also will allow a level of trust to be maintained with the customer through the continued accreditation to these standards. It is anticipated that provider of cloud services may be able to self-certify to bronze levels; however, it will be required to undertake third-party certification to assure to the higher levels.

The base level requirements defined in the Provider Assurance Model aim to give the provider of cloud services the ability to differentiate their services by offering more than the standard, while giving customers confidence that systems are securely maintained. It is also envisioned that while a provider of cloud services may be certified to “Gold” levels of security, that provider may also choose to offer lower levels (such as Silver or Bronze) by providing solutions that meet the security requirements for those levels.

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 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 National Institute of Standards and Technology (NIST) Usage Cases. Actors shown in italics are created specifically for the Alliance Usage Model detailed below. The descriptions provided for the NIST actors is taken directly from NIST (and has 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.

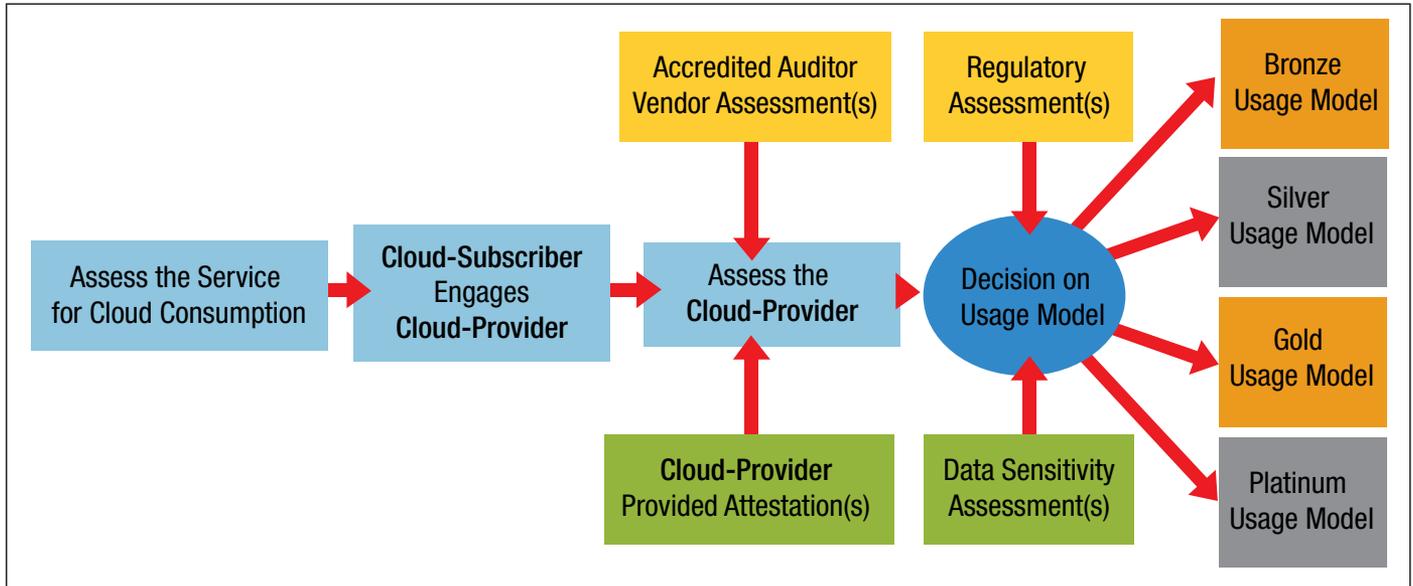
DEPLOYMENT CONSIDERATIONS

Managing risks in interacting with **Cloud-Providers** requires a process to provide an appropriate assurance level. While a **Cloud-Provider** may support many levels of assurance, it is the **Cloud-Subscriber's** responsibility to evaluate its risk appetite and determine the appropriate level of security required. This evaluation may be done by the **Cloud-Subscriber** when choosing a particular **Cloud-Provider** or when selecting a security assurance level. This may also be done as part of the negotiation between the **Cloud-Subscriber** and **Cloud-Provider**.

Some examples of security concerns, which may be addressed by progressing to a higher level of security assurance are shown below:

Deployment Considerations	Level at Which Risks Should Be Diminished			
	Bronze	Silver	Gold	Platinum
Loss of Governance				✓
Lock In (no standardized data)		✓	✓	✓
Isolation Failure			✓	✓
Compliance Risks			✓	✓
Management Interface Compromise		✓	✓	✓
Data Protection			✓	✓
Insecure or Incomplete Data Deletion			✓	✓
Malicious Insider				✓
Intercepting Data in Transit	✓	✓	✓	✓
Distributed Denial of Service		✓	✓	✓
Loss of Encryption Keys			✓	✓
Network Breaks			✓	✓

PROVIDER SECURITY ASSURANCE



USAGE MODEL DETAIL

Goals:

1. To provide standardized definitions of security for cloud-based services so **Cloud-Subscribers** can better compare and understand different cloud offerings. This will, in turn, increase the efficiencies of managing multiple **Cloud-Providers**.
2. To give **Cloud-Providers** the ability to demonstrate compliance to an agreed standard through certification processes maintained by a Cloud-Compliance-Agency.
3. To give **Cloud-Subscribers** the ability to validate adherence to cloud security standards either by direct assessment or third-party accreditation.

Assumptions:

Cloud-Providers must follow compliance reporting standards as detailed in Open Data Center Alliance Usage: Cloud Security Monitoring.

Success Scenario 1 (full):

The Cloud-Standards-Body defines standards and a number of **Cloud-Providers** gain certification through Cloud-Compliance-Agencies. Cloud-Providers advertise services that demonstrate compliance to standards and consistently meet the standards.

Failure Conditions 1:

1. The **Cloud-Provider** advertises a higher level of security than actually exists and claims certification when none exists. This leads to the situation where the **Cloud-Subscriber** purchases services that do not exist and creates significantly greater risk for the **Cloud-Subscriber**.
2. The **Cloud-Provider** achieves certification, but then does not maintain the required processes. This means that the **Cloud-Subscriber** faces a varying level of risk dependent on the level of deviation from the standards.

Success Scenario 2 (partial):

1. The Cloud-Standards-Body ratifies a number of standards, but no certification processes are established.
2. **Cloud-Provider** accepts responsibility to operate to the standards and regularly achieve the required levels.

Failure Conditions 2:

1. The **Cloud-Provider** advertises a higher level of security than actually exists and claims to adhere to the standards without achieving it. This leads to a situation where the **Cloud-Subscriber** purchases services that do not meet the required security level, resulting in significantly greater risk for the **Cloud-Subscriber**.
2. The **Cloud-Provider** achieves the required standard when the contract is initiated, but then does not maintain the required processes. This means that the **Cloud-Subscriber** faces a varying level of risk dependent on the level of deviation from the standards.

Failure Handling:

For all failure scenarios, the monitoring prescribed by the Security Monitoring Usage Model would identify deviations from the standard, thereby allowing the **Cloud-Subscriber** to take necessary actions to reduce risk.

SECURITY REQUIREMENTS

Proposal for Initial Security Requirements

Note: This is not yet an exhaustive list, and it is envisioned that the list will be expanded as the Usage Model matures. Further details to a number of sections are provided below the summary table.

Security Requirement	Level at Each Capability is Offered			
	Bronze	Silver	Gold	Platinum
Antivirus and malware protection (with definition updates within 24 hours)	✓	✓	✓	✓
Vulnerability management process exists and is fully tested to ensure no impact to target or application (further details below)	✓	✓	✓	✓
Network and firewall isolation of Cloud-Subscriber systems with management as described below	✓	✓	✓	✓
Physical access control into cloud data center	✓	✓	✓	✓
Secure protocols used for remote administration (e.g., SSL,SSH, RDP, etc.)	✓	✓	✓	✓
All default passwords and guest access removed	✓	✓	✓	✓
Mandatory use of non-disclosure agreements (NDAs) for Cloud-Provider staff	✓	✓	✓	✓

Security Requirement	Level at Each Capability is Offered			
	Bronze	Silver	Gold	Platinum
Mandatory use of Information Technology Infrastructure Library (ITIL) processes for change, incident and configuration management	✓	✓	✓	✓
Identity management for subscriber assets as described below	✓	✓	✓	✓
Data retention and deletion managed as described below	✓	✓	✓	✓
Security incident and event monitoring as described below	✓	✓	✓	✓
Network intrusion prevention; updates applied within 48 hours		✓	✓	✓
Event logging for all administration-level events (requires controlled access to logs)		✓	✓	✓
Four-eye principle for key administrator changes		✓	✓	✓
Cloud-Provider has an implemented and tested technical continuity plan		✓	✓	✓
Fully documented and controlled network		✓	✓	✓
Systems must be developed using Secure Software Development Lifecycle Coding Standards		✓	✓	✓
Option to perform penetration testing on hosted systems and applications			✓	✓
Physical segmentation of hardware (server, storage, network, etc.) to ensure isolation from all other systems			✓	✓
Encrypted communication between Cloud-Provider and Cloud-Subscriber			✓	✓
Multi-factor authentication			✓	✓
Ability for Cloud-Subscriber to define geographic limits for hosting			✓	✓
Storage encryption at logical unit number (LUN) level			✓	✓
No administrative access for Cloud-Provider staff				✓
Strong encryption mandatory for all data in-flight and at rest				✓

DETAILED SECURITY REQUIREMENTS FOR ASSURANCE LEVELS

Vulnerability Management

A vulnerability management process that ensures installation of system and software patches within the targets is identified below. The test process must ensure proper function of the patch and compatibility to the actual target systems with no negative impact on resource utilization (i.e., memory and CPU consumption).

Bronze	Vulnerabilities with a basic Common Vulnerability Scoring System (CVSS) score of greater than 9 (or those rated as High by Microsoft or other vendors) must be patched within 96 hours, and all others within 1 month.
Silver	Vulnerabilities with a basic CVSS score of greater than 5 (or those rated as Medium or High by Microsoft or other vendors) must be patched within 96 hours; all others within 1 month.
Gold	Vulnerabilities with a basic CVSS score of greater than 2 (or those rated as Low, Medium, or High by Microsoft or other vendors) must be patched within 96 hours; all others within 1 month.
Platinum	All vulnerabilities must be patched within 24 hours of their release by the vendor.

Network and Firewall Isolation

Network segregation and firewalls are required to protect all assets managed in the cloud. The level of involvement of the **Cloud-Provider** in the management of firewall rule sets will vary depending on the level of service offered.

Bronze	The firewall rule sets are managed by the Cloud-Provider with no direct involvement of the Cloud-Subscriber .
Silver	The firewall rule sets are managed by the Cloud-Provider with changes advised to the Cloud-Subscriber before implementation. The Cloud-Provider should offer network segmentation between logical tiers.
Gold	The firewall rule sets are managed by the Cloud-Subscriber . Cloud-Provider retains access to the firewall at administrator level in order to provide system maintenance. The Cloud-Provider must offer network segmentation between logical tiers and should offer Layer-7 protection to prevent application level attacks.
Platinum	Cloud-Provider has no access to firewalls. All admin tasks including rule updates are managed by the Cloud-Subscriber . The Cloud-Provider must offer network segregation between logical tiers and Layer-7 protection to prevent application level attacks.

Identity Management

All services in the cloud must be secured by authentication management systems.

Bronze	Basic username and password systems will exist. Passwords may be basic (but must exist) and no requirement for password aging or reuse exists.
Silver	Basic username and password systems will exist. Strong passwords must be used (e.g., minimum character length of 8 characters, multiple types of characters) and an agreed password aging and reuse policy exists. Service access should support Single Sign-On (SSO) integration using standards-based assertions.
Gold	System and privileged access must be secured using identity federation or strong authentication (i.e., two-factor authentication). In addition to normal passwords, a second secret must be used: a one-time password or a physical token. Service access must support SSO integration using standards-based assertions.
Platinum	System and privileged access must be secured using identity federation or strong authentication (i.e., two-factor authentication). In addition to normal passwords, a unique “biometric” password system must be used. Service access must support SSO integration using standards-based assertions.

Security Incident and Event Monitoring (SIEM)

The **Cloud-Provider** must ensure that any security-related events are advised to the **Cloud-Subscriber**. The minimum requirements for each level are listed below.

Bronze	A SIEM process exists and is operated during normal working hours. Responsibility is assigned within the Cloud-Provider organization. Notification of security-related events is forwarded to the Cloud-Provider within 48 hours of the event.
Silver	A SIEM process exists and is operated 24x7x365. Responsibility is assigned within the Cloud-Provider organization. Notification of security-related events is forwarded to the Cloud-Provider within 24 hours of the event. Security event forwarding to Cloud-Subscriber system is possible.
Gold	A SIEM process exists and is operated 24x7x365. A dedicated team exists and is known to the Cloud-Subscriber . Notification of security-related events is forwarded to the Cloud-Provider within 2 hours of the event. Security event forwarding to Cloud-Subscriber system is mandatory (where such a system exists).
Platinum	SIEM is managed by the Cloud-Subscriber . Security events from the Cloud-Provider’s environment must also be forwarded.

Data Retention and Deletion

The **Cloud-Provider** must ensure that there are adequate controls to support the **Cloud-Subscriber's** requirements for Information Handling and Data Retention/Deletion. In particular, all data whether transient or fixed remains the property of the **Cloud-Subscriber** at all times. The minimum requirements for each level are listed below.

Bronze	Data stored on the Cloud-Provider systems must be deleted when instructed by the Cloud-Subscriber (whether through software or any other means).
Silver	Data stored on the Cloud-Provider systems must be deleted when instructed by the Cloud-Subscriber (whether through software or any other means) and all transient Cloud-Subscriber data tied to a particular user session should be deleted at termination of that session.
Gold	Cloud-Subscriber can define retention policies that can be honored by Cloud-Provider process and automation; full and guaranteed disposal of all data/information from systems that are no longer used by Cloud-Subscriber (session-based for dynamically allocated resources and at end of contract for dedicated systems).
Platinum	Cloud-Subscriber can manage retention policies directly as per their processes (highly automated environment with “self-help” capabilities provided by Cloud-Provider).

Confidentiality

The **Cloud-Provider** must ensure the services offered provide levels of confidentiality dependant on the **Cloud-Subscriber's** requirements. The minimum requirements for each level are listed below:

Bronze	Public website, no requirement for confidential information (e.g., marketing website).
Silver	Suitable controls in place for protecting public and private information (e.g., company website including content management portal).
Gold	Suitable controls in place for protecting public, private or confidential information (e.g., customer relationship management platform).
Platinum	Suitable controls in place for protecting public, private, confidential or highly confidential information (e.g., financial risk modeling product).

Integrity and Trust

The **Cloud-Provider** must ensure that adequate and appropriate trust models be established to determine the integrity of assets. Such models must provide immutable verification mechanisms for key systems and software and enable attestable infrastructure for reporting of such configuration information (see supporting Security Monitoring Usage Model). The minimum requirements for each level are listed below.

Bronze	Trusted Root Certificate Authority (CA) may be provisioned by Cloud-Provider or trusted third party; basic integrity verifications by Cloud-Subscriber .
Silver	Trusted Root CA provisioned by Cloud-Subscriber or trusted third party; could be hosted outside the cloud. If hosted within cloud, it should be hosted on high integrity platform/environment that is verifiable by Cloud-Subscriber , such as a hardware security module (HSM). Reliable integrity checks of static assets.
Gold	Reliable integrity checks of dynamic assets (configurations, files, etc.).
Platinum	Reliable integrity checks of dynamic assets (configurations, files, etc.).

Availability

The **Cloud-Provider** must ensure the services offered provide levels of resiliency dependent on the level requested by the **Cloud-Subscriber**. The minimum requirements for each level are listed below.

Bronze	Best effort.
Silver	Cloud-Provider implemented and tested Technical Continuity Plan.
Gold	Cloud-Provider implemented and tested Technical Continuity Plan. Distributed denial-of-service (DDoS) protection capability available to protect the Cloud-Subscriber's service.
Platinum	Cloud-Provider implemented and tested Technical Continuity Plan. DDoS protection capability available to protect the Cloud-Subscriber's service.

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 defacto standards or common intellectual property-free (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. **Cloud-Providers** and other interested parties requested to submit input on proposed criteria at each level (Bronze, Silver, Gold, Platinum).
2. Cloud-Providers requested to submit early implementations of this framework for consideration.

GLOSSARY

Alliance	Open Data Center Alliance
BCP	Business Continuity Plan
CA	Certificate Authority
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
IP-free	Intellectually Property free
ITIL	Information Technology Infrastructure Library
LUN	Logical Unit Number (with reference to storage solutions)
NDA	Non-Disclosure Agreement
RDP	Remote Desktop Protocol (Microsoft)
SIEM	Security Incident and Event Management
SIEM	Security Incident and Event Monitoring
SSH	Secure Shell
SSO	Single Sign-On
TLS/SSL	Transport Layer Security (Secure Socket Layer) minimum version TLS 1.2