OPEN DATA CENTER ALLIANCE℠ USAGE:
CLOUD BASED IDENTITY GOVERNANCE AND AUDITING REV. 1.0
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Notice</td>
<td>3</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Purpose</td>
<td>5</td>
</tr>
<tr>
<td>Reference Framework</td>
<td>5</td>
</tr>
<tr>
<td>Context</td>
<td>6</td>
</tr>
<tr>
<td>Applicability</td>
<td>7</td>
</tr>
<tr>
<td>Related Usage Models</td>
<td>7</td>
</tr>
<tr>
<td>Taxonomy</td>
<td>7</td>
</tr>
<tr>
<td>Usage Scenarios</td>
<td>8</td>
</tr>
<tr>
<td>Identity Governance</td>
<td>8</td>
</tr>
<tr>
<td>Real-Time User Access Revalidation</td>
<td>8</td>
</tr>
<tr>
<td>Batch or Event-Driven User Access Revalidation</td>
<td>9</td>
</tr>
<tr>
<td>Auditing and Monitoring</td>
<td>11</td>
</tr>
<tr>
<td>Identity Management Audit Logging and Monitoring</td>
<td>11</td>
</tr>
<tr>
<td>Related Usage Models</td>
<td>12</td>
</tr>
<tr>
<td>Industry Call to Action</td>
<td>12</td>
</tr>
</tbody>
</table>
LEGAL NOTICE

© 2012 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.

This “Open Data Center AllianceSM Usage Model: Cloud-Based Identity Governance and Auditing” 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, ODCASTM, 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.

Published April, 2012
EXECUTIVE SUMMARY

Many organizations today have requirements that drive the need to have strong identity governance and auditing on systems that support core business processes or store sensitive information.

These requirements are largely driven by regulatory bodies, compliance requirements, internal security policies/standards, and internal and external audit. Identity governance and auditing are seen as strong forms of monitoring controls, the effectiveness of which can easily be independently tested. Where core services have been moved into the cloud, these systems naturally fall under the same security requirements as internally hosted systems.

These usage scenarios promote the review of access rights and account status that have been provisioned by the cloud subscriber’s identity management system, as well as account and access monitoring in regards to identity management specific concerns.

This document serves a variety of audiences. Solution providers and technology vendors will benefit from its content to better understand customer needs and tailor service and product offerings. Standards organizations will find the information helpful in defining end-user relevant and open standards.
PURPOSE

The ODCA Cloud-Based Identity Governance and Auditing Usage Model was written to promote a consistent approach for the reconciliation of access rights and account status processes required by a cloud subscriber to perform identity governance. It also promote a consistent approach to support identity auditing requirements for cloud-based resources. Additionally, it provides cloud providers and subscribers with clear guidelines for the development of identity management systems and interfaces for cloud-based resources.

REFERENCE FRAMEWORK

The following diagram shows a framework of the functional areas of identity management. This framework provides a reference model for the usage models described below.

The usage model will deal with the identity governance and auditing and monitoring function as shown.
The following diagram shows a summary for the usage models described below regarding identity governance and auditing. This diagram should be used for indicative purposes only and is not intended to be definitive. The identity management (idM) system and the security incident and event monitoring (SIEM) system can be hosted either at the cloud provider or cloud subscriber depending on the assurance level.
**APPLICABILITY**

This usage model is applicable to all levels of cloud services including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

The usage model should be applied in the model of Bronze, Silver, Gold, and Platinum levels of security, as defined in the cloud provider ODCA Provider Assurance Usage Model¹, being required.

Correlation of applicability to other use models can be found in the ODCA Identity Management Interoperability Guide².

**RELATED USAGE MODELS**

This usage model is referenced from the ODCA Identity Management Interoperability Guide. This guide demonstrates the relationships between the different elements of identity management. The ODCA Identity Governance and Auditing Usage Model³ should be read in conjunction with the Interoperability Guide.

General requirements for the levels of security required in cloud solutions can be found in the ODCA Provider Assurance Usage Model.

**TAXONOMY**

<table>
<thead>
<tr>
<th>Actor Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Subscriber</td>
<td>A person or organization that has been authenticated to a cloud and maintains a business relationship with a cloud.</td>
</tr>
<tr>
<td>Cloud Subscriber User</td>
<td>A user of a cloud subscriber organization who consumes the cloud service provided by the cloud provider as an end user. For example, an organization’s email user who is using a SaaS email service the organization subscribes to would be a cloud subscriber’s user.</td>
</tr>
<tr>
<td>Cloud Subscriber Administrator</td>
<td>An administrator type user of a cloud subscriber organization that performs (cloud) system related administration tasks for the cloud subscriber organization.</td>
</tr>
<tr>
<td>Cloud Administrator</td>
<td>An administrator type user that performs administration tasks on a system providing services to a cloud subscriber organization. This is independent of whether the administrator is part of the cloud subscriber organization or whether he/she is part of a cloud provider organization working on resources supplied to the cloud subscriber.</td>
</tr>
<tr>
<td>Cloud Provider</td>
<td>An organization providing network services and charging cloud subscribers. A (public) cloud provider provides services over the Internet.</td>
</tr>
<tr>
<td>Cloud Provider Administrator</td>
<td>An administrator type user of a cloud provider organization that performs (cloud) system related administration tasks for the cloud provider organization as part of a service offering.</td>
</tr>
</tbody>
</table>

¹ [www.opendatacenteralliance.org/docs/ODCA_ProviderAssurance_Rev.1.1_Final.pdf](http://www.opendatacenteralliance.org/docs/ODCA_ProviderAssurance_Rev.1.1_Final.pdf)
² [www.opendatacenteralliance.org/docs/ODCA_IdM_InteropGuide_Rev1.0_final.pdf](http://www.opendatacenteralliance.org/docs/ODCA_IdM_InteropGuide_Rev1.0_final.pdf)
³ [www.opendatacenteralliance.org/docs/ODCA_Identity_Gov_Auditing_Rev1.0_final.pdf](http://www.opendatacenteralliance.org/docs/ODCA_Identity_Gov_Auditing_Rev1.0_final.pdf)
**USAGE SCENARIOS**

**IDENTITY GOVERNANCE**

**USAGE SCENARIO 1: REALTIME-TIME USER ACCESS REVALIDATION**

**Actors:**
cloud subscriber, cloud subscriber administrator, cloud provider

**Goal:**
The cloud subscriber requires a review process to be initiated in real time to pull back provisioned account status and associated access rights. This is to account for cloud subscriber users and cloud administrators that have access to resources managed by the cloud provider. The cloud subscriber has the ability to select one user or multiple users as part of the process.

**Assumption 1:** The cloud subscriber has a role-based identity management system that can differentiate the types of resources required for a cloud subscriber user.

**Assumption 2:** The interface provided by the cloud provider will be through a single standards-based application programming interface (API).

**Assumption 3:** There is a predefined, secure, and trusted communication channel (SSL, VPN (IPSEC/SSL)) between parties.

**Assumption 4:** There is a predefined, secure, trusted, and time-stamped mechanism to ensure message integrity and authenticity of the payload.

**Assumption 5:** The cloud subscriber can apply policies to determine where a cloud subscriber’s access does not conform to roles or if the access is different from what was originally provisioned. Consequently, a course of action can be performed such as automatic removal of access or initiation of a review cycle process.

**Assumption 6:** Modification of access of cloud provider managed resources is performed using Service Provisioning Markup Language (SPML).

**Assumption 7:** The interactions defined below are to be carried out in a timely manner. The maximum delay in transaction time should be defined in the contract.

**Success Scenario 1:**
A reconciliation process is initiated that pulls back all the current cloud subscriber users and cloud administrators from the cloud provider managed resources. That information is stored in the cloud subscriber identity management system to facilitate the review processes.

**Steps:**
1. The cloud subscriber administrator logs into the identity management system and initiates a real time request to reconcile the account status and/or access rights managed by the cloud provider.
2. The cloud provider completes the necessary steps to send back the account status and/or access rights for the relevant resource.
3. The cloud provider returns a “Completed” message indicating the successful completion of the reconciliation request.
4. Within the cloud subscriber’s identity management system, the policies associated with the review process are applied to the reconciled account status and/or access rights.
   a. Where a policy and workflow have been implemented to include automated remediation activities the cloud subscriber’s identity management system may initiate the identity provisioning service to suspend or remove access automatically.
   b. Where there is a secondary process required for remediation such as a manual review cycle the information is sent to the identity management system’s user access rights (UAR) reporting service.
5. The identity management system of the cloud subscriber registers the successful operation. The results can be reviewed by the cloud subscriber administrator.

**Failure Condition 1:**
A failure message is received from the cloud provider system as a response that the reconciliation request has failed.

**Failure Handling 1:**
The identity management system of the cloud subscriber should identify the error and escalate as appropriate.

**Failure Condition 2:**
Following the reconciliation request no response is received from the cloud provider in a timely manner. In this case, the status of the request is unclear.

**Failure Handling 2:**
The request should be identified within the identity management system of the cloud subscriber as a potential risk and should be flagged to the cloud subscriber administrator as requiring further investigation.

**Failure Condition 3:**
A failure message is received from the cloud subscriber’s system regarding the integrity of the message payload that is a result of a failed integrity check or time synchronization issue.

**Failure Handling 3:**
Event message should be flagged to the cloud subscriber administrator as requiring further investigation.

**Failure Condition 4:**
A failure message is received from the cloud provider’s system as a response that it is unable to initiate automatic remediation activities.

**Failure Handling 4:**
Event message should be flagged to the cloud subscriber administrator as requiring further investigation.

**USAGE SCENARIO 2: BATCH OR EVENT-DRIVEN USER ACCESS REVALIDATION**

**Actors:**
cloud subscriber, cloud subscriber administrator, cloud provider

**Goal:**
The cloud subscriber requires a review process to be initiated by a batch process to pull back provisioned account status and associated access rights. This is to account for cloud subscriber users and cloud administrators that have access to resources managed by the cloud provider. The batch process is triggered by a predefined event, such as time for a monthly review cycle.

**Assumption 1:** The cloud subscriber has a role-based identity management system that can differentiate the types of resources required for a cloud subscriber user.

**Assumption 2:** The interface provided by the cloud provider will be made through a single standards based API.

**Assumption 3:** There is a predefined, secure, and trusted communication channel (SSL, VPN/IPSEC/SSL) between parties.

**Assumption 4:** There is a predefined, secure, trusted, and time-stamped mechanism to ensure message integrity and authenticity of the payload.
Assumption 5: The cloud subscriber can apply policies to determine where a cloud subscriber’s access does not conform to roles or if access is different from what was originally provisioned. Consequently, a course of action can be performed, such as automatic removal of access or going through a review cycle process.

Assumption 6: Modification of access as part of remediation of the cloud provider managed resources is performed using an SPML interface.

Assumption 7: The cloud subscriber will configure a batch schedule, based on the subscriber’s requirements, which needs to be agreed on with the cloud provider (e.g., don’t want to perform a batch process at a critical time of the day that may affect performance of the service).

Assumption 8: The interactions defined below are to be carried out in a timely manner. The maximum delay in transaction time should be defined in the contract.

Success Scenario 1:
A reconciliation process is initiated that pulls back all the current cloud subscriber users from the cloud provider managed resources. That information is stored in the cloud subscriber identity management system to facilitate the cloud subscriber’s review processes.

Steps:
1. The cloud subscriber’s identity management system initiates a configured batch schedule to reconcile all, or a subset of, the account status and/or access rights managed by the cloud provider.
2. The cloud provider completes the necessary steps to send back the account status and/or access rights for the relevant resource.
3. The cloud provider returns a “Completed” message indicating the successful completion of the reconciliation request.
4. Within the cloud subscriber’s identity management system, the policies associated with the review process are applied to the reconciled accounts and entitlements.
   a. Where a policy and workflow have been implemented to include automated remediation activities, the cloud subscriber’s identity management system may initiate the identity provisioning service to remove access automatically.
   b. Where there is a secondary process required for remediation, such as a review cycle, the information is sent to the identity management system’s UAR reporting service.
5. The identity management system of the cloud subscriber registers the successful operation. The results can be reviewed by the cloud subscriber administrator.

Failure Condition 1:
A failure message is received from the cloud provider’s system as a response that the reconciliation request has failed.

Failure Handling 1:
The identity management system of the cloud subscriber should identify the error and escalate as appropriate.

Failure Condition 2:
Following the reconciliation request, no response is received from the cloud provider in a timely manner. In this model, the status of the request is unclear.

Failure Handling 2:
The request should be identified within the cloud subscriber’s identity management system as a potential risk and should be flagged to the cloud subscriber administrator as requiring further investigation.

Failure Condition 3:
A failure message is received from the cloud subscriber’s system regarding the integrity of the message payload which is a result of a failed integrity check or a time synchronization issue.
Failure Handling 3:
Event message should be flagged to the cloud subscriber administrator as requiring further investigation.

Failure Condition 4:
A failure message is received from the cloud provider system as a response that it is unable to initiate automatic remediation activities.

Failure Handling 4:
Event message should be flagged to the cloud subscriber administrator as requiring further investigation.

AUDITING AND MONITORING

USAGE SCENARIO 1: IDENTITY MANAGEMENT AUDIT LOGGING AND MONITORING

Actors:
cloud subscriber, cloud subscriber administrator, cloud provider, cloud provider administrator

Goal:
The cloud subscriber requires that identity management-related auditing of cloud subscriber user or cloud administrator activity on resources that are managed by the cloud provider are logged and sent back to the SIEM system. This includes cloud provider staff.

Assumption 1: The audit logs maintained by the cloud provider are at a level which meets the cloud subscriber’s integrity and confidentiality requirements. For example, gold could be forensic level, tamper proof, etc.

Assumption 2: At a minimum, the audit logs will contain the following fields: a time-stamp of the event, the type of event, error code if applicable, user’s identity, resource being accessed, IP address of the client, and hostname.

Assumption 3: The following identity management events will, where technically possible, be captured — authentication logs, access and authorization logs, user login and logoff events (both permit and deny type events based on assurance level).

Assumption 4: All human and non human interaction (e.g. monitoring tools, system accounts) identity management events are logged, unless specifically excluded within the contract.

Assumption 5: The storage of logs, modification of minimum fields and retention of the logs at the cloud provider must be agreed upon to meet any cloud subscriber and cloud provider regulatory and legal requirements. All such agreements will form part of the contract.

Assumption 6: There is a predefined, secure, and trusted communication channel (SSL, VPN (IPSEC/SSL)) between parties.

Assumption 7: There is a predefined, secure, trusted, and time-stamped mechanism to ensure message integrity and authenticity of the payload.

Assumption 8: The interactions defined below are to be carried out in a timely manner. The maximum delay in transaction time should be defined in the contract.

Success Scenario 1:
As a cloud subscriber user accesses and uses a cloud provider managed resource, security events relating to identity management are logged.

Steps:
1. The cloud subscriber user / cloud subscriber administrator accesses the cloud provider managed resource.
2. As the cloud subscriber triggers certain identity management events, the cloud provider logs security events to its central logging service.
3. The cloud provider consolidates the events and forwards them, upon a pre-defined event or upon specific request, to the cloud subscriber’s preferred SIEM system.

4. The SIEM system acknowledges it has received the log update from the cloud provider’s auditing and logging service.

5. The SIEM system performs security correlation on the logs obtained from the cloud provider’s managed resources.

6. The cloud subscriber administrator reviews the logs and generates reports as required.

**Failure Condition 1:**
No logs have been received for a period of time between the cloud provider’s managed resource and the central logging service.

**Failure Handling 1:**
An alert should be raised to the cloud provider administrator as requiring further investigation.

**Failure Condition 2:**
No logs have been received for a period of time between the cloud provider’s central logging service and the SIEM system.

**Failure Handling 2:**
An alert should be raised to the cloud subscriber administrator as requiring further investigation.

**Failure Condition 3:**
A failure message is received from the cloud subscriber’s system regarding the integrity of the message payload which is a result of a failed integrity check or a time synchronization issue.

**Failure Handling 3:**
Event message should be flagged to the cloud subscriber administrator as requiring further investigation.

**RELATED USAGE MODELS**
The following usage models are related to the topic of cloud-based governance and auditing and will provide further detail.

*ODCA Usage Model: Security Monitoring Rev.1.1*  
*ODCA Usage Model: Cloud-Based Identity Provisioning Rev.1.0*

**INDUSTRY CALL TO ACTION**
The following further actions are required:
The ODCA requests providers of identity management systems for the enterprise and cloud providers to produce reference models and proof-of-concept implementations that will show compliance to this requirement.

---


5 [www.opendatacenteralliance.org/docs/ODCA_Identity_Provisioning_Rev1.0_final.pdf](http://www.opendatacenteralliance.org/docs/ODCA_Identity_Provisioning_Rev1.0_final.pdf)