

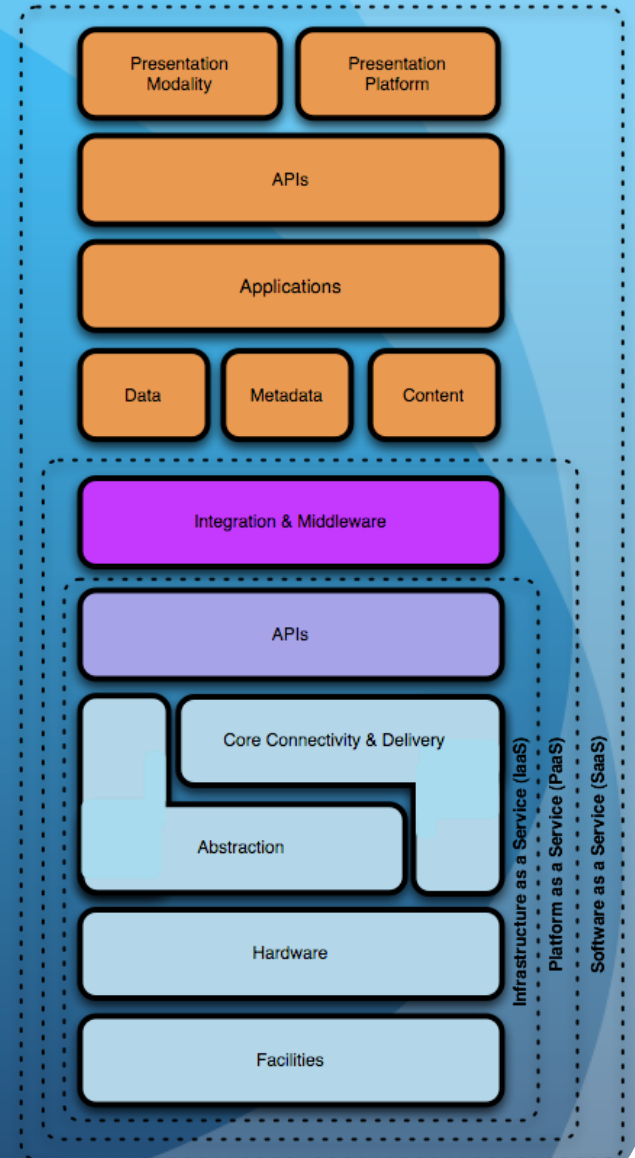


CloudAudit Working Group Update

April 2011

CloudAudit Charter

- Provide a common interface and namespace that allows cloud computing providers to automate collection of Audit, Assertion, Assessment, and Assurance Artifacts (A6) of their operating environments
- Allow authorized consumers of services and concerned parties to do likewise via an open, extensible and secure interface and methodology.



What CloudAudit Does

- Provide a structure for organizing assertions and supporting documentation for specific controls across different compliance frameworks in a way that simplifies discovery by humans and tools.
 - Define a namespace that can support diverse frameworks
 - Express compliance frameworks in that namespace
 - Define the mechanisms for requesting and responding to queries relating to specific controls
 - Integrate with portals and AAA systems

How CloudAudit Works

- Utilize **security automation capabilities** with existing tools/protocols/frameworks via a standard, open and extensible set of interfaces
- Keep it simple, lightweight and easy to implement; offer primitive definitions & language structure using HTTP(S) first at a very basic level
- Allow for extension and elaboration by providers and choice of trusted assertion validation sources, checklist definitions, etc.

Context for CloudAudit

- CloudAudit is not designed to validate or attest “compliance”
- Automates collection and presentation of data supporting queries using a common set of namespaces aligned CSA Cloud Control Matrix
- Artifacts are accessible by a human operating a web browser or a tool capable of utilizing CloudAudit over HTTP(S).
- The consumers of this information are internal & external auditors, compliance teams, risk managers, security teams, etc. & in the longer term, brokers

Aligned to CSA Control Matrix

- Officially folded CloudAudit under the Cloud Security Alliance in October, 2010
- First efforts aligned to compliance frameworks as established by CSA Control Matrix:
 - PCI DSS
 - NIST 800-53
 - HIPAA
 - COBIT
 - ISO 27002
- Incorporate CSA's CAI and additional CompliancePacks
- Expand alignment to “infrastructure” and “operations”-centric views also

What Was Delivered in v1.0

- The first release of CloudAudit provides for the scoped capability for providers to store evidentiary data in well-defined namespaces aligned to the 5 CSA Control Matrix Mappings (PCI, HIPAA, NIST800-53, ISO27002, COBIT)*
- The data in these namespaces is arbitrary and can be named and file-typed as such, so we need a way of dealing with what can be one to hundreds of supporting files, the contents of some of which are actually URIs to other locations

* Update v1.1 packaging available to include CSA CCM Updates

Current Discussions*

- Stack Providers with whom we have discussed CloudAudit:
 - VMware, Citrix, Microsoft, OpenStack
- Cloud Service Providers with whom we have discussed CloudAudit:
 - AWS, Google, Microsoft, Terremark, Savvis, Rackspace
- Tool (GRC) solution providers with whom we are discussing CloudAudit Implementation:
 - Agilance, RSA
- Audit/Standards associations with whom we are discussing CloudAudit:
 - ISACA, ODCA, BITS, ISO, Open Group, DMTF, IETF

* NOTE: Discussions do not imply commitment to proceed or intent to support

What's On The 6 Month Roadmap

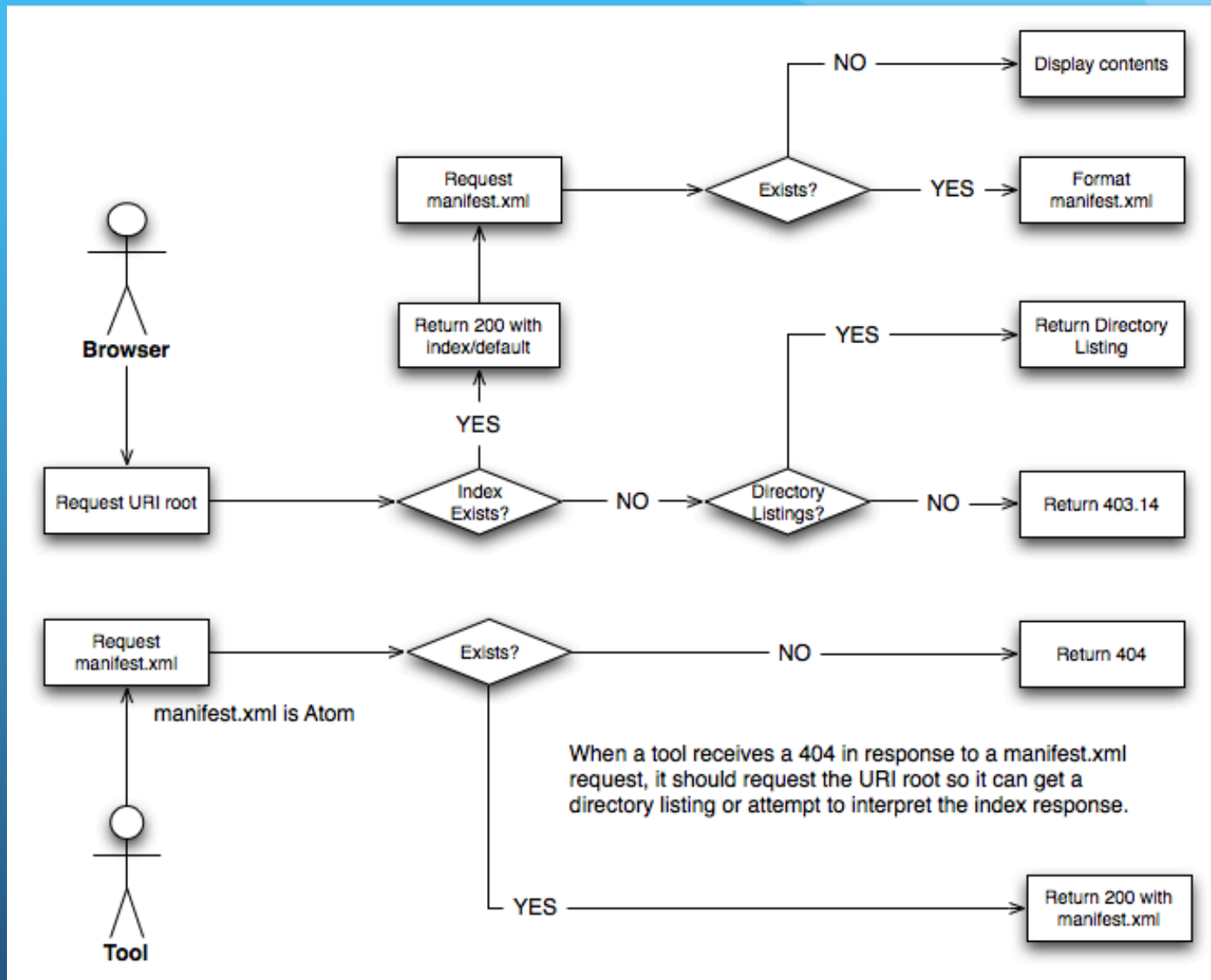
- Extend ATOM in manifest.xml to provide for timestamps, signatures and version control [need XML/ATOM expertise]
- Version control and change notification in conjunction with...
- ...Architecture for registry services [cloudaudit.net] and extensions of such (public and/or private)
- Implementation architecture for “atomic queries” (e.g. “PCI Compliant,” or “SAS-70 Certified”)
- Expand On Specific CloudAudit Use Cases:
 - CloudAudit for Federal Government
 - CloudAudit for Cloud Providers
 - CloudAudit for Auditors/Assessors

How It Works

Atom Specification (RFC4287)

- <http://www.ietf.org/rfc/rfc4287.txt>
- Atom is an XML-based document format that describes lists of related information known as "feeds". Feeds are composed of a number of items, known as "entries", each with an extensible set of attached metadata. For example, each entry has a title.
- The primary use case that Atom addresses is the syndication of Web content such as weblogs and news headlines to Web sites as well as directly to user agents.

Request Flow for Users & Tools



index.html/default.jsp/etc.

- Index.html is for dumb browser consumption
 - Typically, the direct human user use case
- It can be omitted if directory browsing is enabled (not recommended)
- It contains JavaScript to look for the manifest.xml file, parse it, and render it as HTML.
- If no manifest.xml exists, it should list the directory contents relevant to the control in question

Manifest.xml

- Structured listing of control contents
- Can be extended to provide contextual information
- Primarily aimed at tool consumption
- In Atom format

Manifest.xml Example

```
<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">
  <title>ISO 27002 v2005 15.3.1</title>
  <link href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v2005/15/3/1/" rel="self"/>
  <id>http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v2005/15/3/1/</id>
  <subtitle>Information systems audit controls</subtitle>
  <updated>2010-01-13T18:30:02Z</updated>
  <generator uri="http://cloudaudit.org/development/bootstrap.tgz" version="1.0">Cloud Audit Manual Bootstrap Package</generator>
  <author>
    <name>Jon James</name>
    <email>jonjames@cloudhosting.com</email>
  </author>
  <rights type="text">Copyright (c) 2009, Cloud Hosting Inc.</rights>
  <category term="/iso/27002/v2005/" label="ISO 27002 v5"/>

  <entry>
    <title>Audit Schedule</title>
    <link href="http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v2005/15/3/1/auditschedule.xls" type="application/msexcel"
    rel="related"></link>
    <id>http://www.cloudhosting.com/.well-known/cloudaudit/org/iso/27002/v2005/15/3/1/auditschedule.xls</id>
    <updated>2009-12-28T12:24:02Z</updated>
    <id></id>
    <summary>the 2010 audit schedule for cloud hosting inc.</summary>
    <author>
      <name>Eric Smith</name>
      <email>ericsmith@cloudhosting.com</email>
    </author>
    <contributor>
      <name>Mary Huxley</name>
      <email>maryhuxley@kpwey.com</email>
      <uri>http://www.kpwey.com</uri>
    </contributor>
  </entry>
```

What This Looks Like (CSA CompliancePack)

The screenshot shows a web browser window with the URL <https://cloud.enstratus.com/.well-known/cloudaudit/>. The browser's address bar also shows "enStratus Networks LLC" and a search bar with "Google". The page header includes the "enSTRATUS" logo and a "CONTACT US 612.746.3091" link. The main content area is titled "Compliance Information" and contains the following text:

Author: George Reese (george.reese@enstratus.com)
Date: 2010-08-17T14:01:58Z

- [CSA Guidance](#)

For more information on CloudAudit, see [the CloudAudit web site](#).

The footer of the page contains the text: "Copyright © 2010 enStratus Networks LLC CONFIDENTIAL – FOR ENSTRATUS CUSTOMER USE ONLY".

...Which Yields:

enStratus Networks LLC

CONTACT US 612.746

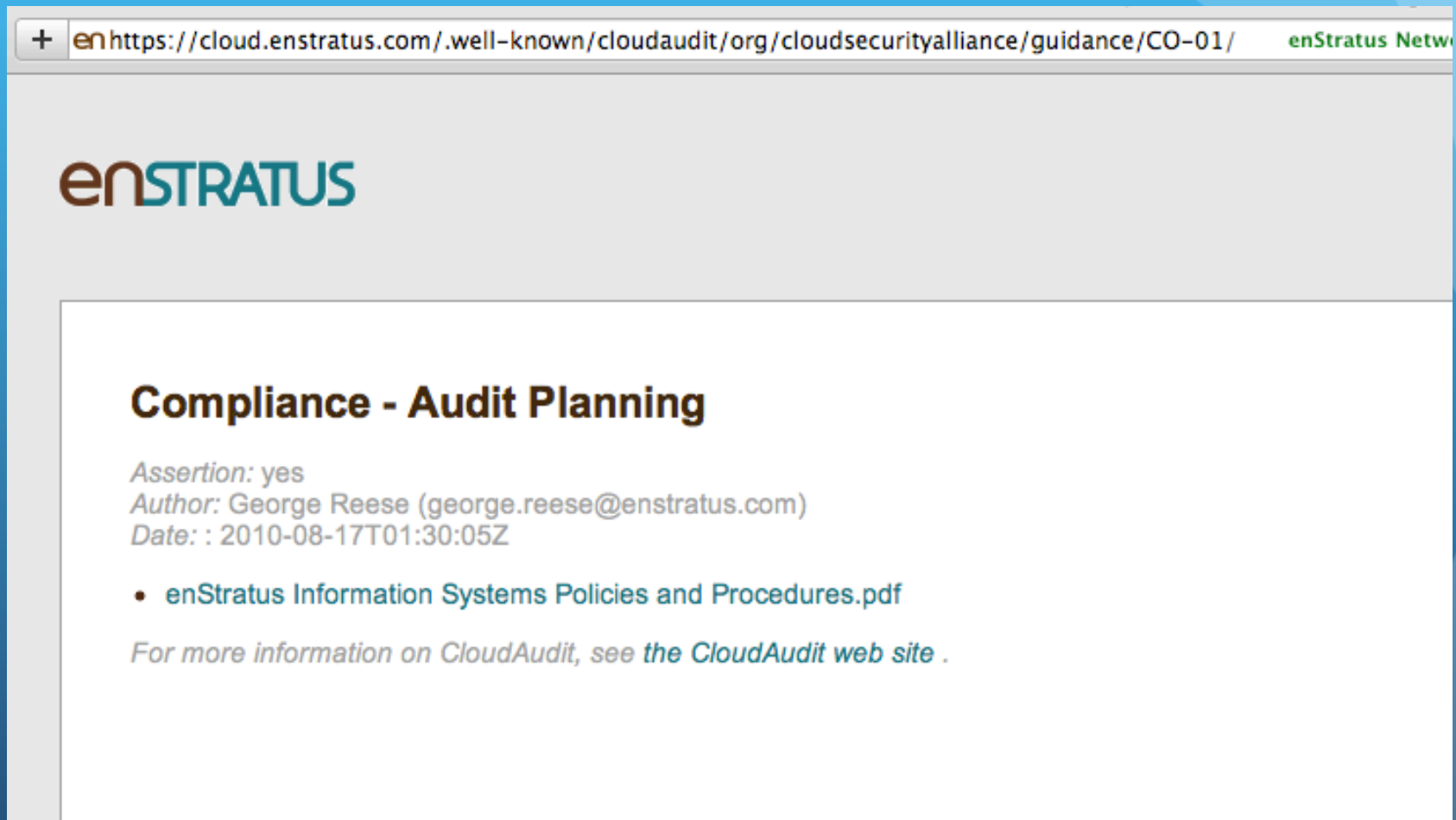
enSTRATUS

CSA Guidance Assertions for enStratus

Author: George Reese (george.reese@enstratus.com)
Date: 2010-08-17T14:01:58Z

Control	Name	Description	Assertion
CO-01	Compliance - Audit Planning	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to, to minimize the risk of disruptions to business processes, focusing on data duplication, access, and data boundary limitations.	yes
CO-02	Compliance - Independent Audits	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing,	no
CO-03	Compliance - Third Party Audits	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the service delivery agreements.	yes

...Further



The screenshot shows a web browser window with the following content:

- Address bar: <https://cloud.enstratus.com/.well-known/cloudaudit/org/cloudsecurityalliance/guidance/CO-01/>
- enSTRATUS logo
- Section header: **Compliance - Audit Planning**
- Metadata:
 - Assertion: yes
 - Author: George Reese (george.reese@enstratus.com)
 - Date: : 2010-08-17T01:30:05Z
- List item:
 - [enStratus Information Systems Policies and Procedures.pdf](#)
- Text: *For more information on CloudAudit, see the CloudAudit web site .*

...Assuming You Are Authorized, Of Course

The screenshot shows a web browser window with the URL <https://cloud.enstratus.com/.well-known/cloudaudit/org/cloudsecurityalliance/guidance/CO-01/enS>. The page features the enSTRATUS logo in the top left and a LOGIN button in the top right. The main content area is a white box with a dark border containing the following text:

Access Denied

We are unable to provide you with access to the requested resource right now. Either you do not have the appropriate access rights or an access error has occurred.

Please use the Support link below if you believe you have received this message in error.

At the bottom of the white box, there is a dark brown bar with a red button labeled "Support".

Project Deliverables

- Initial Release Deliverables:

[http://www.cloudaudit.org/
CloudAudit_Distribution_20100815.zip](http://www.cloudaudit.org/CloudAudit_Distribution_20100815.zip)

- Contains all CompliancePacks, documentation and scripts needed to begin implementation of CloudAudit
- Working with Service Providers and Tool Vendors for Adoption