CloudAudit
A6 Working Group Call

February 26, 2010

Agenda

- Administrivia
- Review Last Call
- Specification & Requirements Discussion
- Deliverables, Timelines, Administrivia Part Deux
  - Team & Leadership
  - Tools
  - Process

Administrivia

Where We Are @ A High Level

- We broke the 215 people mark on the Google Groups membership
- We have an amazing core team from the who's-who of Cloud & an expansive set of extended participants
- We've received some very visible press/media exposure
- We now have hooks/alliances building with other efforts that are related (CSA, ENISA, CAM, and more)
- Time to get to work…

Organization

- I am a SPoF & Sam is a busy sum'bitch (congrats on the new gig @ Google, BTW)
- I'm an idea guy, I need do'ers with practical experience in this sort of thing. I know you're out there
- At the end of this call, I'm going to ask for people to step up and lead with their expertise in areas they have the time and ability to commit to
- I'm going to start by talking a lot (again, surprise) but I want to facilitate discussion and consensus, not be a benevolent curator of flawed, un-implementable ideas.

Motivated Interested Parties* ;)

Name	Affiliation
Chris Hoff	Cisco
Ben Sapiro	Telus
Glenn Brunette	Sun
Lew Tucker	Sun[shine]
Doug Egan	CSC
George Reese	Enstratus
Gunnar Peterson	Arctec
Andy Ellis	Akamai
Craig Nelson	Microsoft
Allwyn Sequeira	VMware
Sam Johnston	Super Awesome Cloud Consultant

Name	Affiliation
Shlomo Swidler	Orchestratus
Scott Sanchez	Unisys
Steve Riley	Amazon Web Services
Ken Owens	Savvis
Chris Drumgoole	Terremark
Bret Piatt	Rackspace Cloud
John Menerick	Netsuite
Randy Bias	CloudScaling
James Urquhart	Cisco
...and more that shall be named soon	

**Does not denote any contractual arrangement or corporate commitment*

Review Of Last Call

CloudAudit Overview (Recap)

- The goal is to **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 (firewall=true or SAS70=false)
- Allow for extension and elaboration by providers and choice of trusted assertion validation sources, checklist definitions, etc.
- Encourage adoption by driving client usage; providers opt-in. Null returns could be considered “non-validated” or “non-asserted”
- Do not require adoption of other platform-specific APIs
- Provide interfaces to Cloud naming and registry services

From Our Last Call (2/12/10)

- We need to build the foundational set of requirements and specifications that define elements of interest for v1.0 of the CloudAudit Protocol
- How will the exposed API be consumed?
- How will the resultant responses be cross-referenced to things like compliance frameworks that have specific requirements?
- What are the A6 requirements for third party trust brokers and should worry about this now?
- We should be able to get to a roughed out work product relatively quickly given the Cloud service consumer-driven requirements

Specifications & Requirements Discussion

Discussing the model and moving forward…

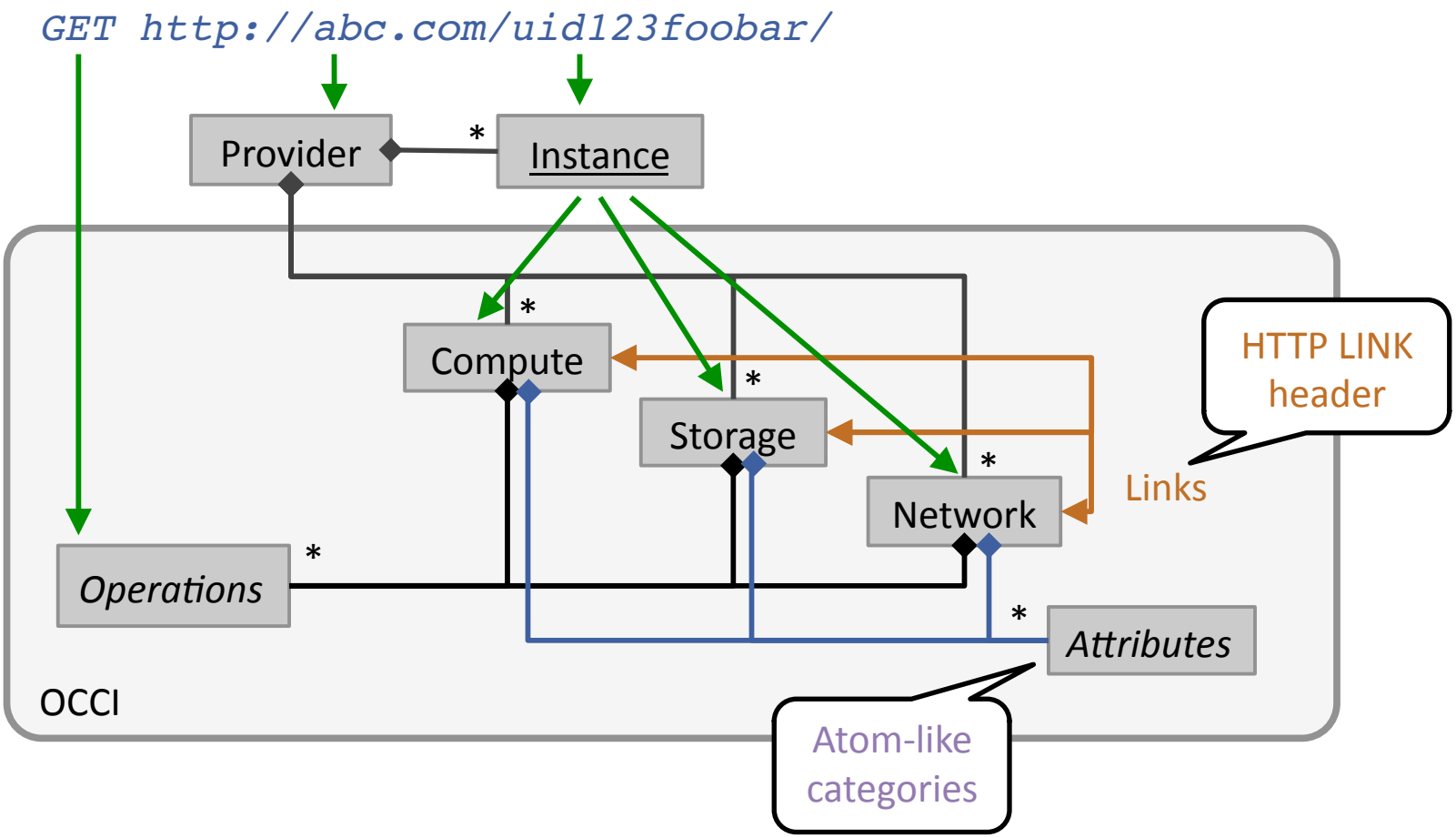
Regret Using the word ‘API’?

- The first deliverable is shaping up to be less about producing a *programmatic* interface and more about a common semantic schema/registry of the sorts of information that ought to be provided across CSP’s
- How that information is extracted from their service is up to the CSP (we have ideas,) how it’s stored and made available for consumption is our first goal
- The mechanisms used to present that information to a “consumer” should, in conjunction with AAA, at a minimum use simple HTTP(s) commands with verbs, nouns and adjectives similar to what we saw in OCCI

What We Do/Don't Want to Prescribe

- We want to be open and provide for modularity associated with supported interface modalities, AAA implementations, data formats, collection mechanisms, tool input/output
- We're more interested in standardizing the data footprint to allow for consistent automation for both the provider and consumer; how you get there is your decision
- No reinventing the wheel; if there's a better mousetrap, let's use it

5,000-foot Look at OCCI



Simple Element Audit/Assurance Such As:

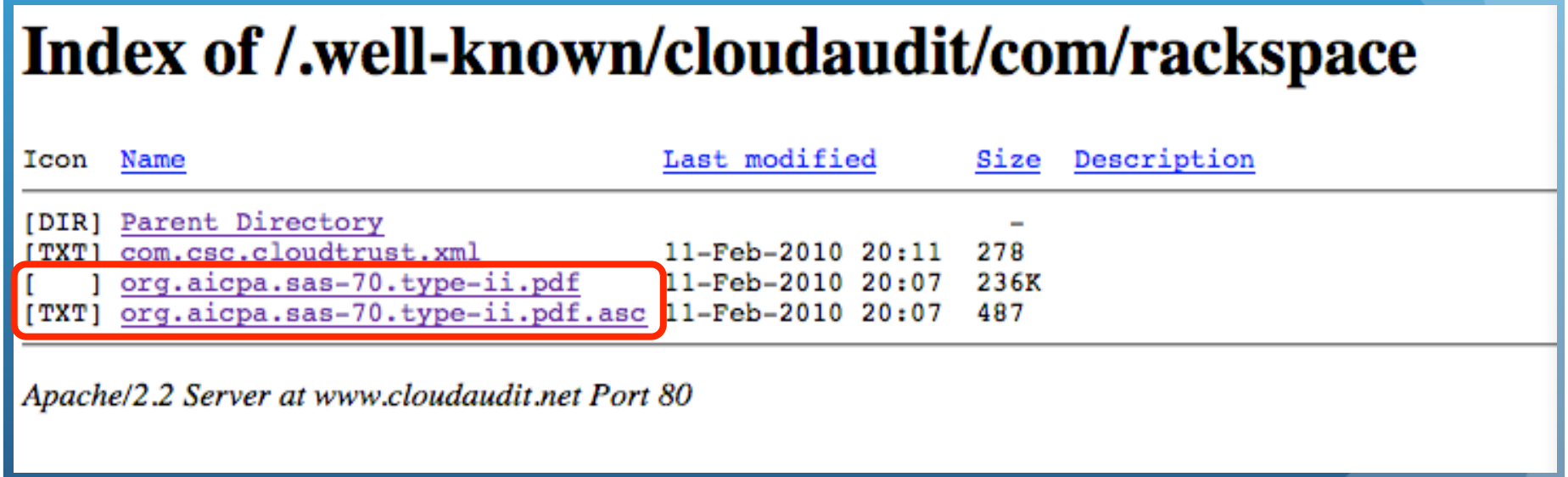
- http://www.cloudaudit.net/.well-known/cloudaudit/com/rackspace/com.csc.cloudtrust.xml

```
- <!--

        CloudTrust Demo
        Created by Sam Johnston on 2010-02-12.
    Example static rendering of CloudTrust standard.
  -->
- <cloudtrust>
  - <assertion id="123">
      <name>tape-backup</name>
      <status>true</status>
    </assertion>
  </cloudtrust>
```

A Simple CloudAudit Example

- http://www.cloudaudit.net/.well-known/cloudaudit/com/rackspace/

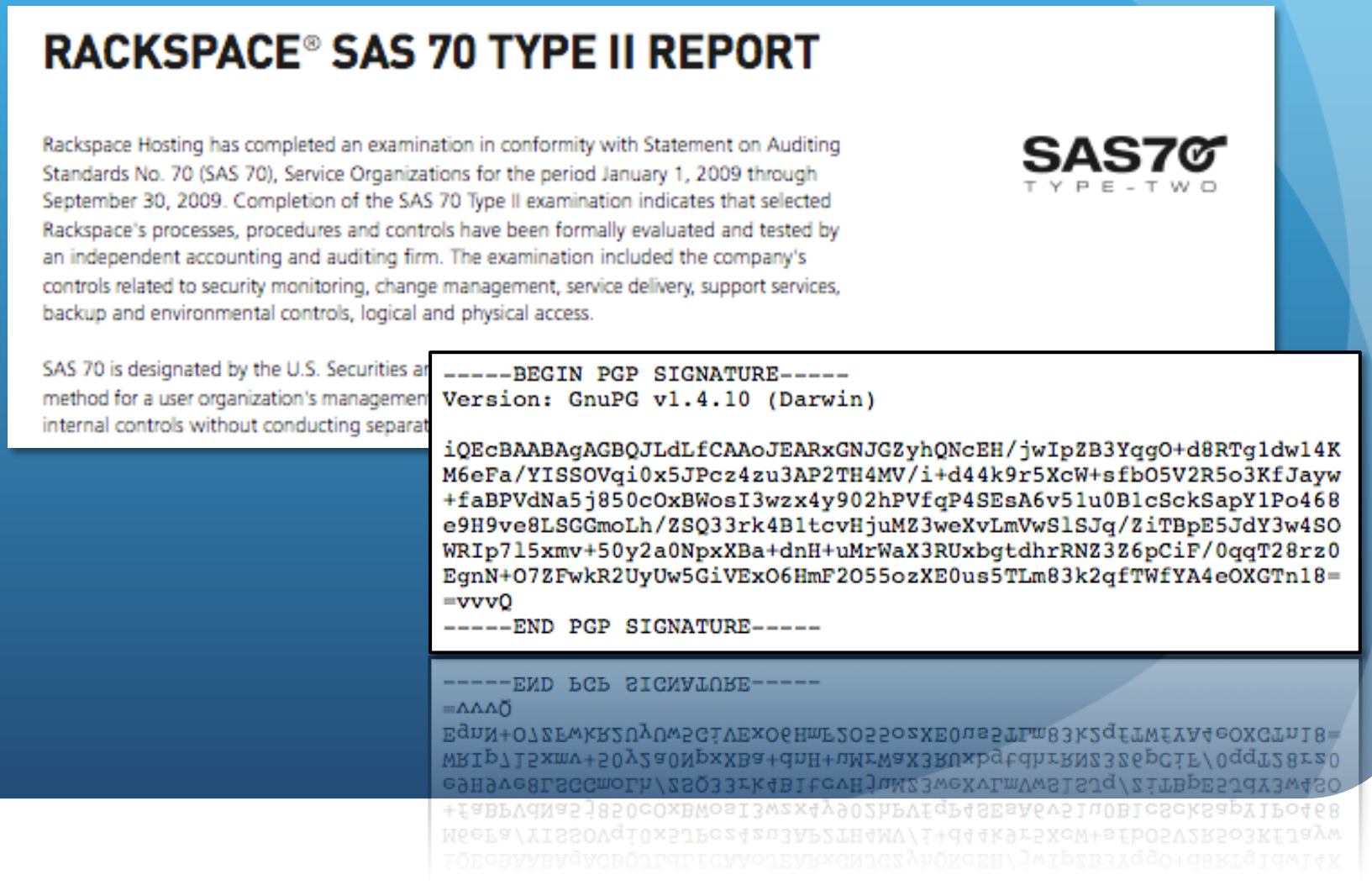


Index of /.well-known/cloudaudit/com/rackspace

Icon	Name	Last modified	Size	Description
[DIR]	Parent Directory		-	
[TXT]	com.csc.cloudtrust.xml	11-Feb-2010 20:11	278	
[ ]	org.aicpa.sas-70.type-ii.pdf	11-Feb-2010 20:07	236K	
[TXT]	org.aicpa.sas-70.type-ii.pdf.asc	11-Feb-2010 20:07	487	

Apache/2.2 Server at www.cloudaudit.net Port 80

Which Can Present Things Like…



RACKSPACE® SAS 70 TYPE II REPORT

Rackspace Hosting has completed an examination in conformity with Statement on Auditing Standards No. 70 (SAS 70), Service Organizations for the period January 1, 2009 through September 30, 2009. Completion of the SAS 70 Type II examination indicates that selected Rackspace's processes, procedures and controls have been formally evaluated and tested by an independent accounting and auditing firm. The examination included the company's controls related to security monitoring, change management, service delivery, support services, backup and environmental controls, logical and physical access.

SAS 70 is designated by the U.S. Securities a
method for a user organization's managemen
internal controls without conducting separat

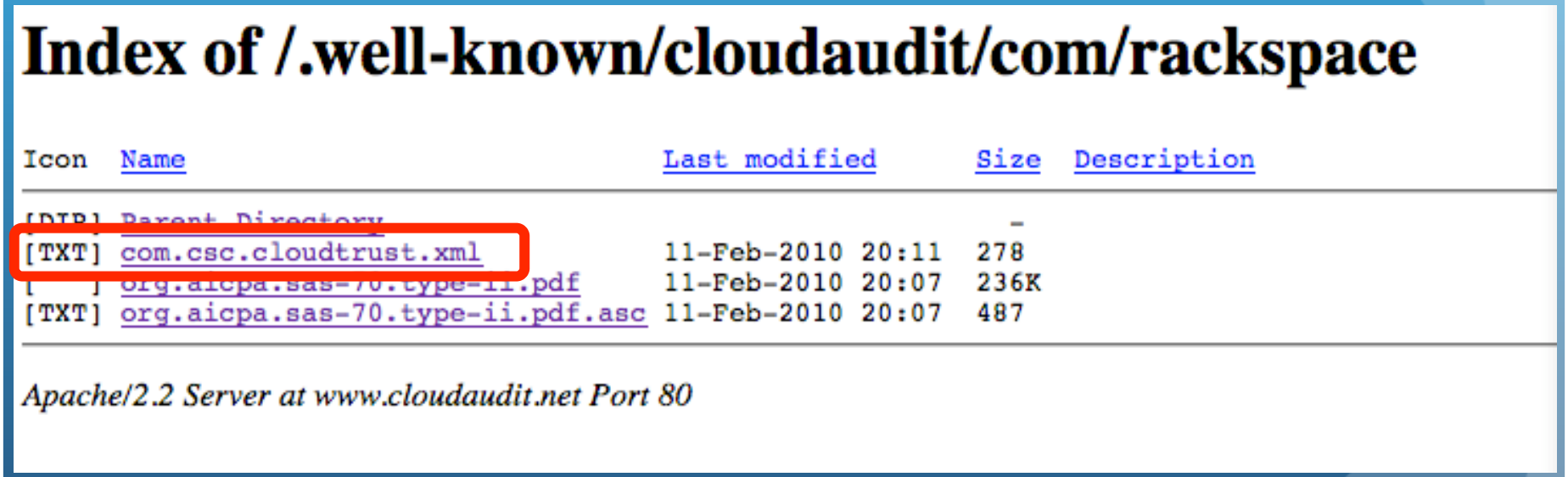
SAS70
TYPE-TWO

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.10 (Darwin)

iQEcBAABAgAGBQJLdLfCAAoJEARxGNJGZyhQNcEH/jwIpZB3YqgO+d8RTg1dw14K
M6eFa/YISSOVqi0x5JPcz4zu3AP2TH4MV/i+d44k9r5XcW+sfbO5V2R5o3KfJayw
+faBPVdNa5j850cOxBWosI3wzx4y902hPVfqP4SEsA6v51u0BlcSckSapY1Po468
e9H9ve8LSGGmoLh/ZSQ33rk4B1tcvHjuMZ3weXvLmVwSlSJq/ZiTBpE5JdY3w4SO
WRIp715xmv+50y2a0NpxXBa+dnH+uMrWaX3RUxbgtdhrRNZ3Z6pCiF/0qqT28rz0
EgnN+O7ZFwkR2UyUw5GiVExO6HmF2O55ozXE0us5TLm83k2qfTWfYA4eOXGTn18=
=vvvQ
-----END PGP SIGNATURE-----
```

Or…

- http://www.cloudaudit.net/.well-known/cloudaudit/com/rackspace/



Index of /.well-known/cloudaudit/com/rackspace

Icon	Name	Last modified	Size	Description
[DIR]	Parent Directory		-	
[TXT]	com.csc.cloudtrust.xml	11-Feb-2010 20:11	278	
[ ]	org.aicpa.sas-70.type-ii.pdf	11-Feb-2010 20:07	236K	
[TXT]	org.aicpa.sas-70.type-ii.pdf.asc	11-Feb-2010 20:07	487	

Apache/2.2 Server at www.cloudaudit.net Port 80

Data Formats and Such…

- The thoughts are that we don't really care all that much about trying to envision (or more importantly) define all formats, but we'd like to arrive at an intelligent consensus
- XML, URLs, JSON, PDF's, XLS, RTF, TXT, JPG, etc… depends on what's being asked for…
- We need to determine who's going to use this information and how

How are we going to craft this?

- We need to build the class structures associated with the primitives we expect to require at a minimum
- Compute/Network/Storage? Infrastructure/ Metastructure/Infostructure? Audit/Assertion/ Assessment/Assurance? ← How to organize?
- Map/associate/cross-reference these “hard” primitives and data sets to ”soft” things like “compliance”
- This is the most onerous pieces of the process

Deliverables, Timelines & Administrivia, Part Deux

Deliverables & Timelines

- The first deliverable ought to be the specifications that will allow a CSP to organize the collective output (or a subset) of our requirements and deliver an interface to this information
- Needs to map to customer-driven governance, assurance and compliance frameworks
- Work with security tool vendors to encourage them to enable their products to consume this information
- I'd like to have the first reasonable draft done in 90 days

What We Need Quickly

- Need small team of folks from the core team to take the lead at sketching out the scope (a good mix from CSP's, ISVs, Integrators, Consultants, Consumers)
- Collect the data points we want to collect
- Prioritize and sort by lens
- Provide to the larger group (outside the core team) to segment by class and start building schema/primitives
- Separate the content/storage from the access to it, but have a small team think about these requirements

Step Up

- Need that previously-mentioned small group of people (5-6) to start sketching out the schema/primitives
- Need 2-3 people from the core team willing to help co-lead this effort:
  - Help run meetings
  - Organize deliverables
  - Project Manage
  - Tools setup
- Need some help with “marketing”
  - FAQ on website
  - Interfacing with media, other groups…
- Organize around Contributors, Reviewers, Consulted roles

Notes:

- Technical/Non-Technical Elements
  - “Namespace” - What
  - “Transport” - How
  - “Language/Protocol” - How
- Split apart “What” from “How”
- Define stakeholders, consumers and lenses
- “Read Only” namespace (initially)
- Production/Collection by providers
- Registry/Dictionary

Who's Doing What…

- "Who" Leads
  - "**Transport**" – Ravi, Ken Owens, Edward Haletky, Sam Johnston
  - "**Language/Protocol**" – John Menerick, Doug Egan, Lynn Terwoerds, Sam Johnston
- "What" Leads
  - "**Namespace**" – Scott Sanchez, Glenn Brunette, James (which?), Craig Balding, Ben Sapiro, Anton Chuvakin
- FAQ/Mktg – James Urquhart, Mike Versace

Contact Info

- Chris Hoff
  - hoffc@cisco.com | choff@packetfilter.com
  - +1.978.631.0302
  - @beaker
  - Skype: infosecenigma
- Google Group
  - http://groups.google.com/group/A6WG
- Website
  - http://www.CloudAudit.org