

# Continuous Auditing in Cloud

37 WCARS

14 – 15 September 2016 – Gold Coast, Australia

# **Continuous Auditing in Cloud**



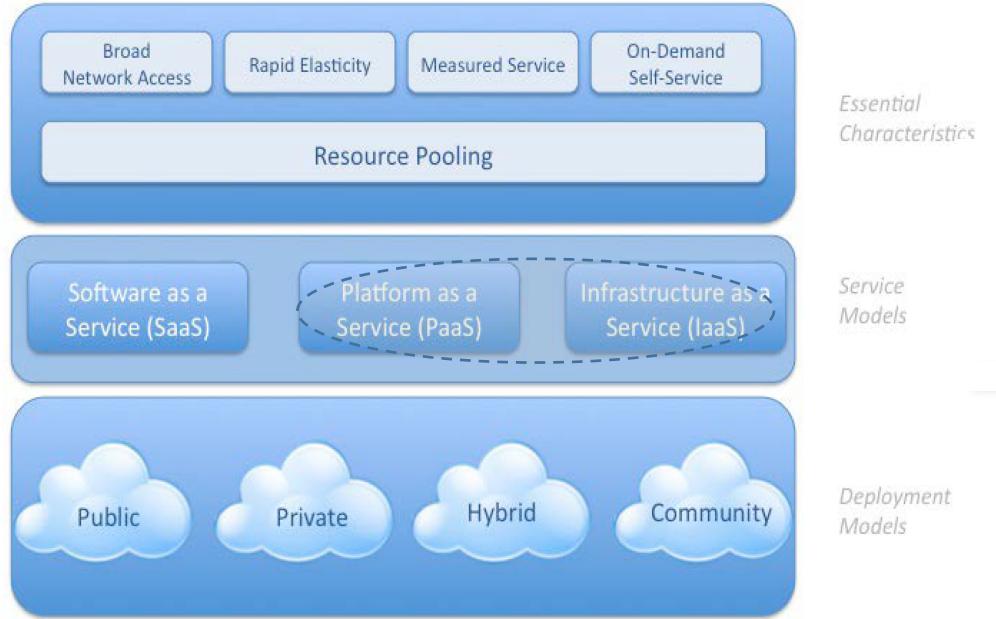


Figure 1—NIST Visual Model of Cloud Computing Definition<sup>2</sup>

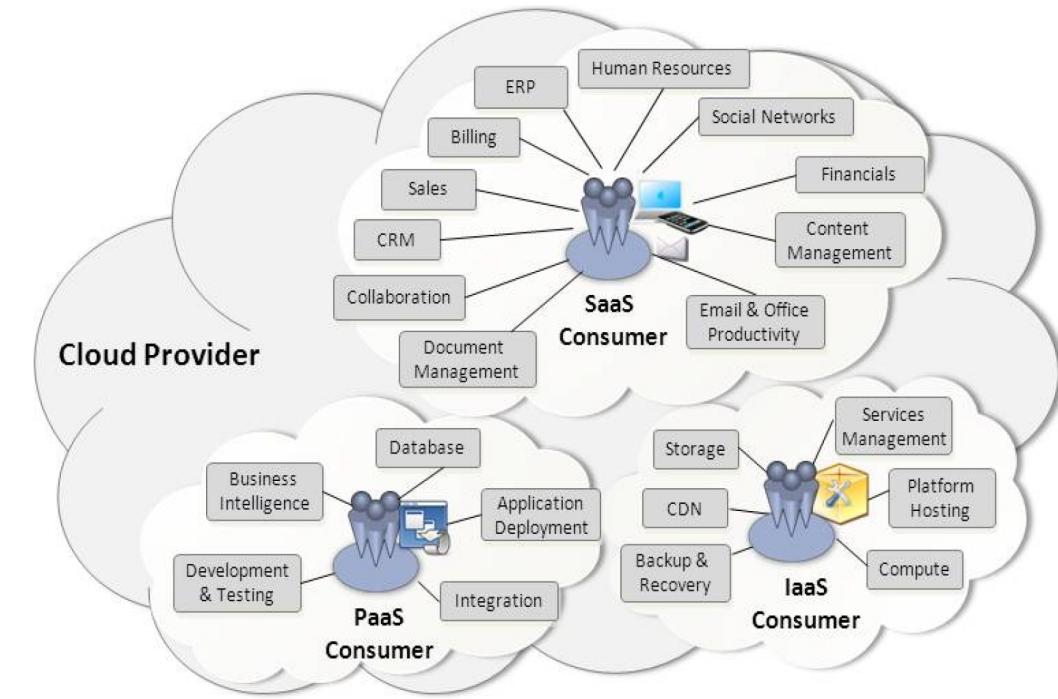


Figure 4: Example of Services Available to a Cloud Consumer (NIST SP 500-292)

**Cloud computing**, is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

National Institute of Standards and Technology (NIST)

## **Cloud Characteristic**

On Demand  
Self Service

Broad Network  
Access

Resource  
Pooling

Rapid Elasticity

Measured  
Service

## **Potential Audit concern**

- User driven versus IT driven
  - Shadow IT
  - Cloud Services discovery

- Enhanced threat profile, attack surface
  - Perimeter definition

- Multi-tenancy
  - Co-mingling of data and assets

- VM Sprawl- uncontrolled scale up
  - Data Remanence

- Proliferation of cloud services due to initial low opex

# Cloud Risks

Policy &  
Organisational Risk

Technical Risks

Virtualisation Risks

Legal Risks

Non Cloud Specific  
Risks

# Cloud Risks

## Policy & Organisational Risk

- Provider Lock in
- Loss of Governance
- Compliance Risk
- Provider Exit

## Technical Risks

- Consolidation of IT Infrastructure – single point of failure
- Control over technical risk shifting to provider
- Insecure or incomplete data deletion
- Lack of Portability

## Virtualisation Risks

- Guest Escape – Break out of OS – Access by Hypervisor or other guests
- Sprawl – Loss of control over image store
- Multitenancy

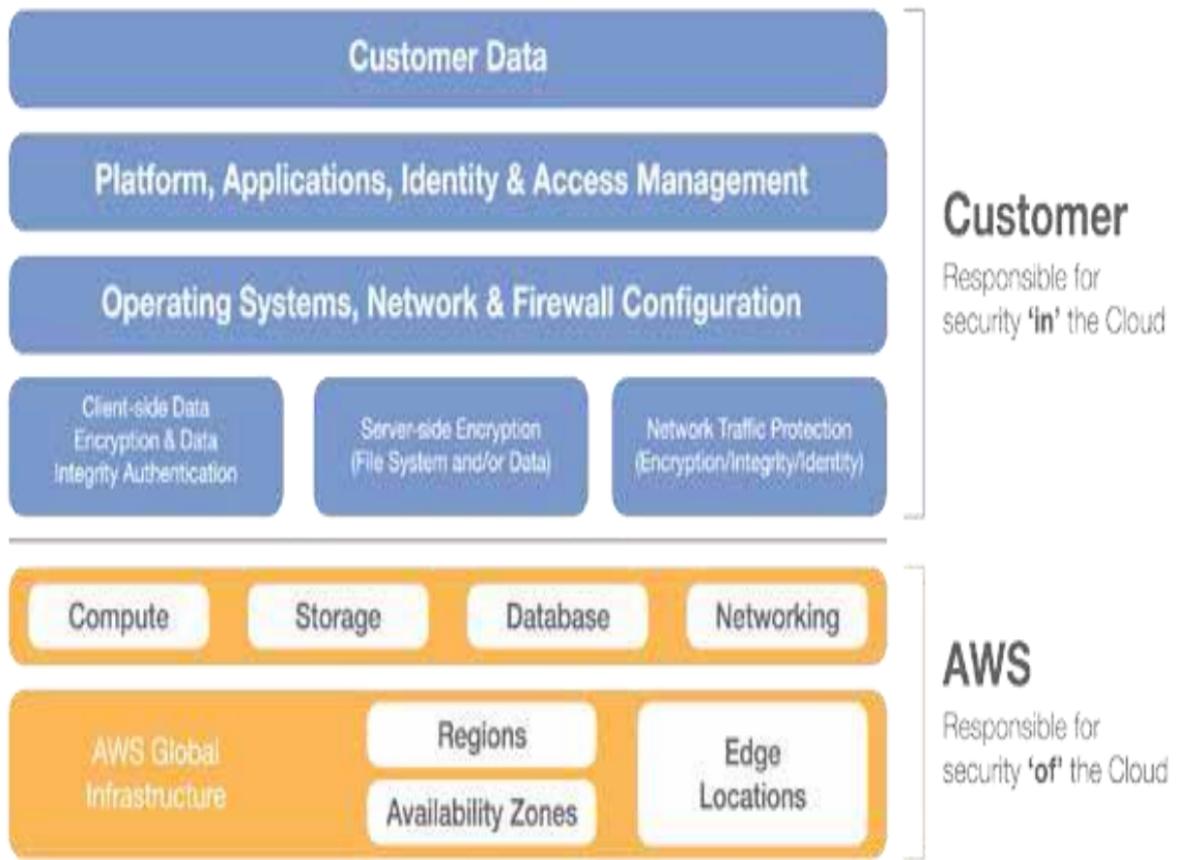
## Legal Risks

- Data Protection

## Non Cloud Specific Risks

- Natural disasters
- Unauthorised facility access

# Shared Responsibility model in cloud



SERVICE OWNER	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

© - Cloud Security Alliance

Figure 1: The AWS Shared Responsibility Model



# Complexities in Security Controls

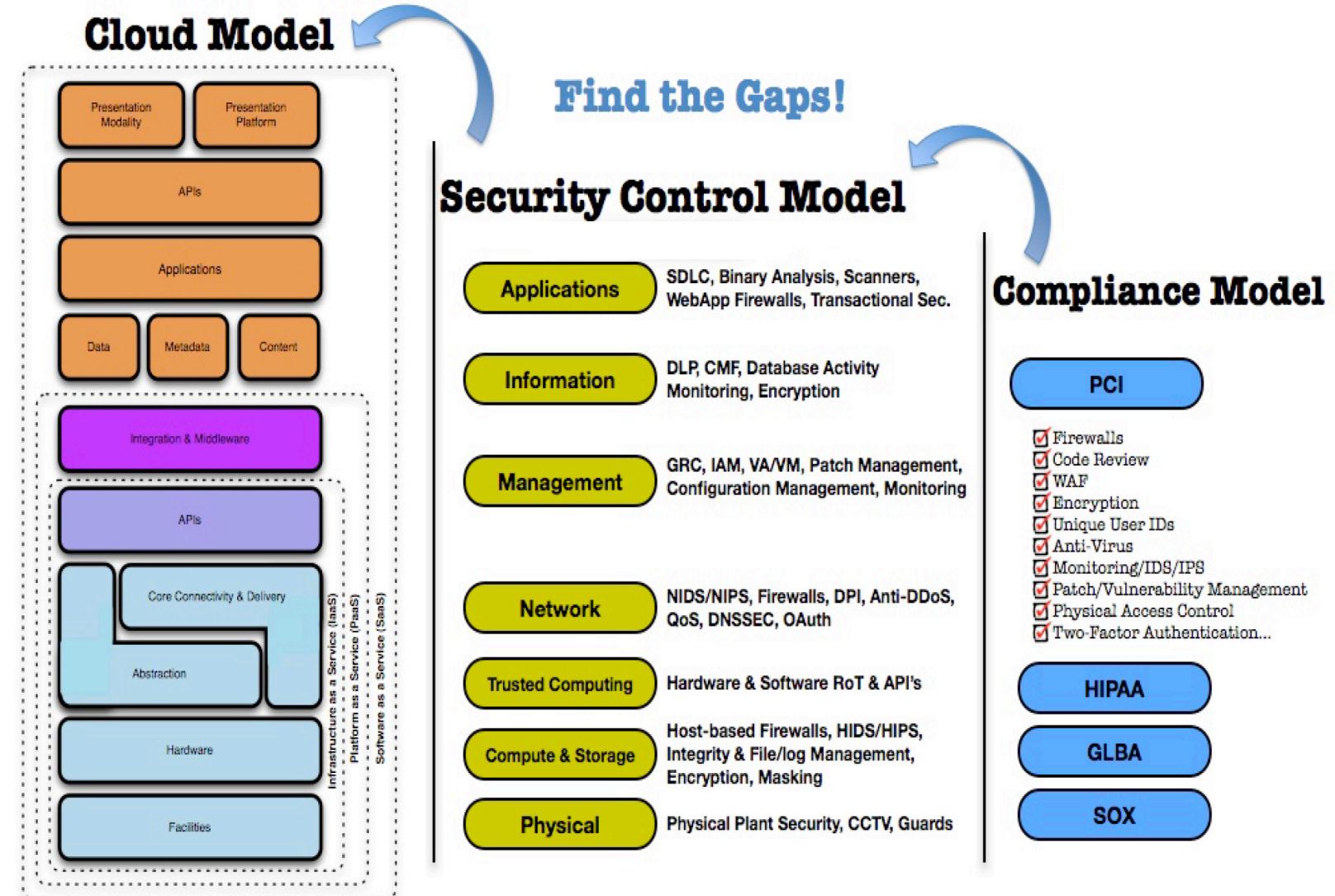
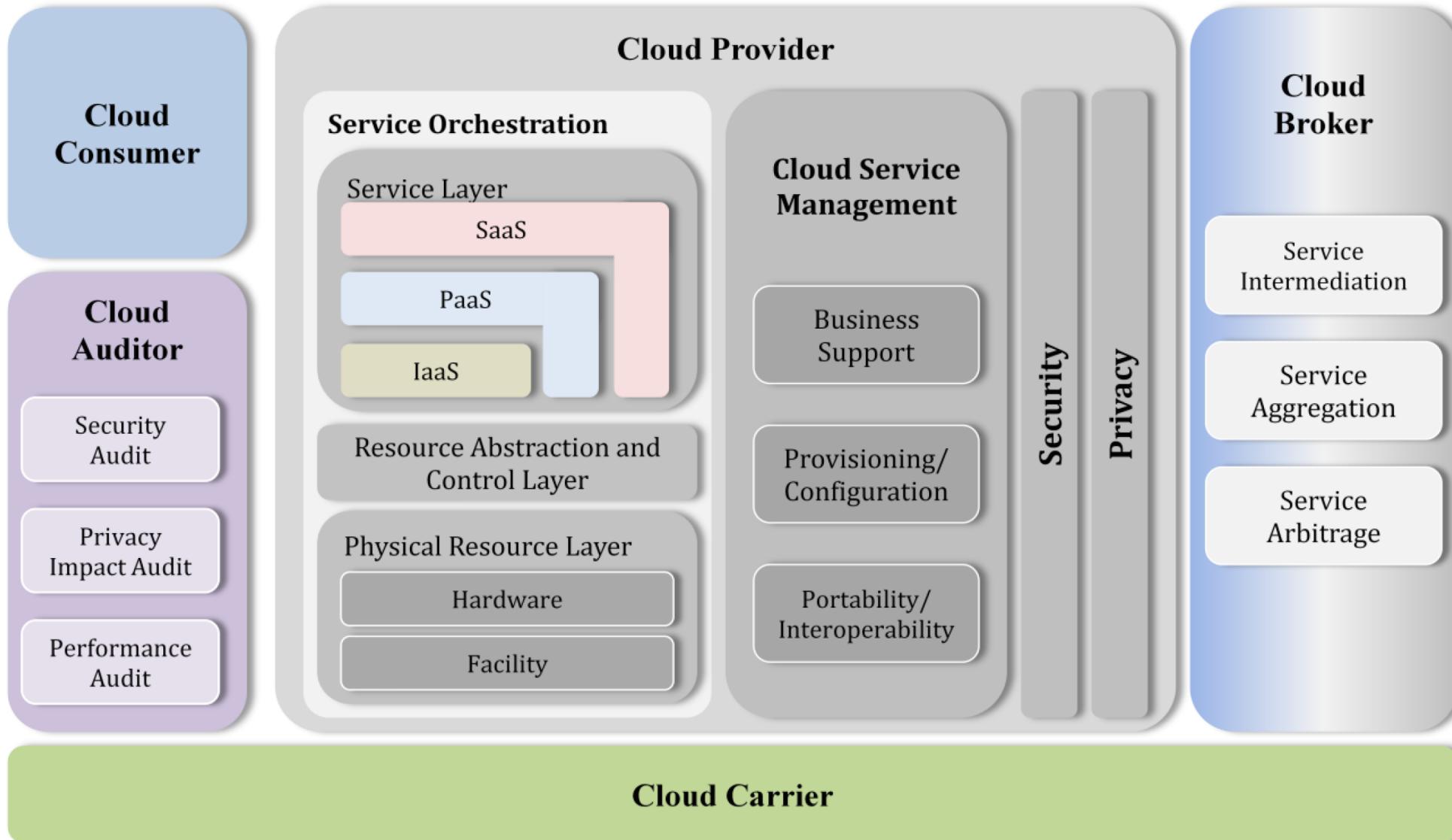


Figure 5—Mapping the Cloud Model to the Security Control & Compliance



**Figure 1: The Conceptual Reference Model**

# Assurance

ISACA defines an assurance initiative as an “objective *examination of evidence* for the purpose of providing an assessment on risk management, control or governance processes for the organization.”<sup>2</sup>

With shared resourcing, multitenancy and geolocation in mind, cloud computing requires an *entirely new approach to providing assurance*.

*Assurance needs to become more real-time, continuous and process-oriented* vs. transactional in focus, while CSPs need to provide greater transparency to their clients regarding the movement of the clients’ data.

Cloud computing requires *continuous monitoring of compliance*

# Assurance Frameworks

- **Technology Neutral** widely accepted frameworks customizable for the cloud (i.e., COBIT, ISO 2700x)
- **Cloud Specific** (i.e., CSA Cloud Control Matrix, Jericho Forum™ Self-Assessment Scheme, NIST)

Existing Std. &  
Framework Adequate

Supplement existing  
Std.

New Standards and  
Framework



For Service  
Organizations

Provides information to service  
organizations on building trust and  
confidence in their systems.



[Jungwoo Ryoo, Syed Rizvi, William Aiken, John Kissell](#)

- Auditing has made great strides in the past decade, but it has not seemingly kept pace with the real-time economy. ***Some auditing approaches and techniques that were valuable in the past now appear outdated.*** Also, the auditing evolution has reached a critical juncture whereby auditors may either lead in promoting and adopting the future audit or continue to adhere to the more traditional paradigm in some manner. Future audit approaches would likely require auditors, regulators, and standards setters to make significant adjustments.

## Auditor Skills

According to Ryoo et al. (2015), “An audit’s quality depends heavily on the auditor’s cloud computing experience and knowledge” (para. 41). This audit experience could cause a major problem if an auditor is more familiar with in-house systems as opposed to constantly evolving cloud systems.

These secure services needs create greater demand for more quality auditors, and as systems grow with the advent of multi-vendor systems, there will be a need for audit standardization of cloud-computing services.

*Cloud Security framework and audit methods 36922 - SANS 2015*

More than half of CAEs (57 percent) are not convinced that their teams have the skills and expertise needed to deliver on stakeholders’ current expectations—let alone future demands. If Internal Audit can’t fulfill stakeholder expectations, how can it exert influence and have an impact on the organization?

*deloitte-audit-executive-survey-2016*

## **Continuous Audit**

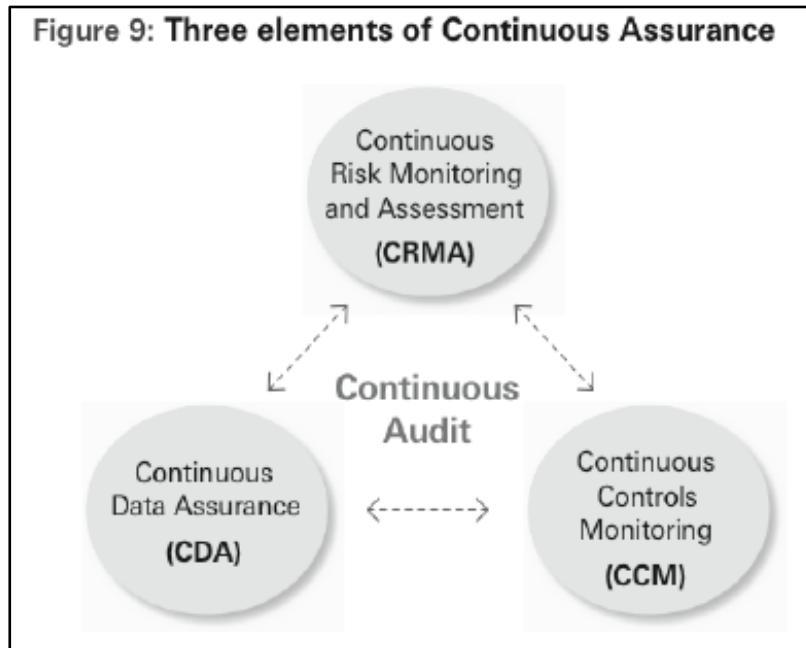
A continuous audit is a methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter (CICA/AICPA, 1999).

## Continuous Assurance Components

**Continuous controls monitoring (CCM)** - consists of a set of procedures used for monitoring the functionality of internal controls

**Continuous data assurance (CDA)** - verifies the integrity of data flowing through the information systems

**Continuous Risk Monitoring and Assessment (CRMA)** - used to dynamically measure risk and provide input for audit planning.

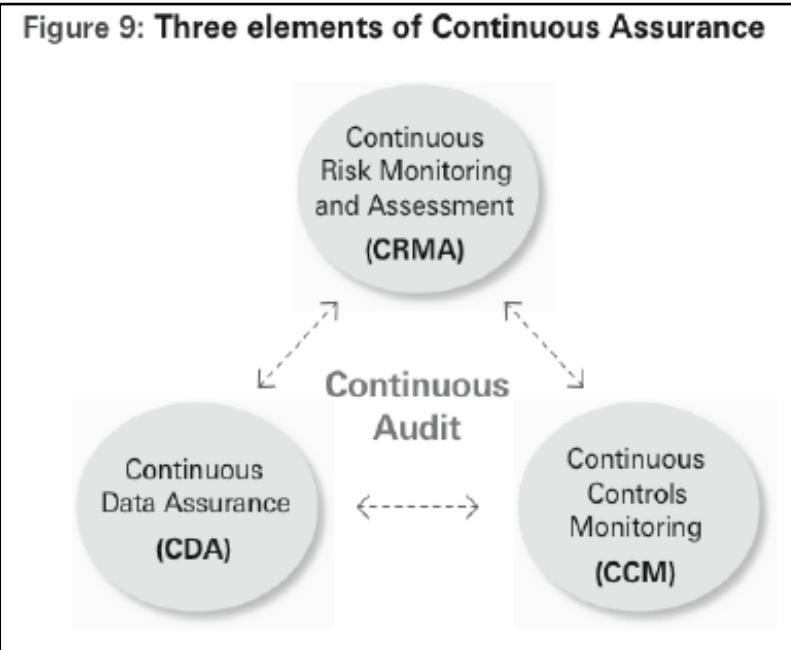


**Examples of CCM include procedures for monitoring**  
Access control and authorisations  
System configuration  
Business process settings.

**Examples of CDA include procedures for verifying**  
Master data  
Transactions  
Key process metrics using analytics (including continuity equations [CEs]).

**CRMA includes processes that**  
Measure risk factors on a continuing basis  
Integrate different risk scenarios into some quantitative framework  
Provide inputs for audit planning.

## Continuous Assurance opportunities



- Transaction verification
- Data analytics
- E-discovery – data dispersion

## CSA Cloud Control Matrix

Provides fundamental security principles to guide cloud vendors and to assist cloud customers in assessing the overall security risk of a cloud provider

### Cloud Controls Matrix v3.0.1 Quick Stats

FOR MORE INFORMATION:  
<https://cloudsecurityalliance.org/research/ccm>  
<https://blog.cloudsecurityalliance.org/ccm/>  
[ccm-leadership@cloudsecurityalliance.org](mailto:ccm-leadership@cloudsecurityalliance.org)



- What controls can be automated ?

## What we are auditing

Operations  
Compliance  
ICFR

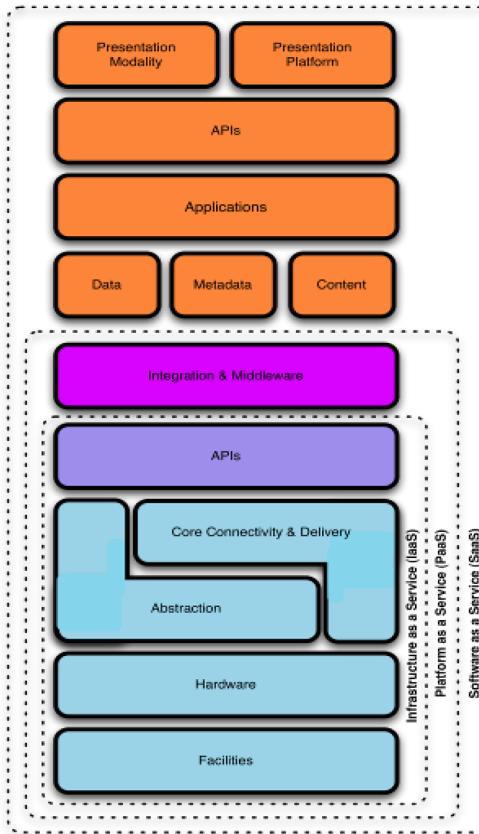
Information  
Systems

SaaS

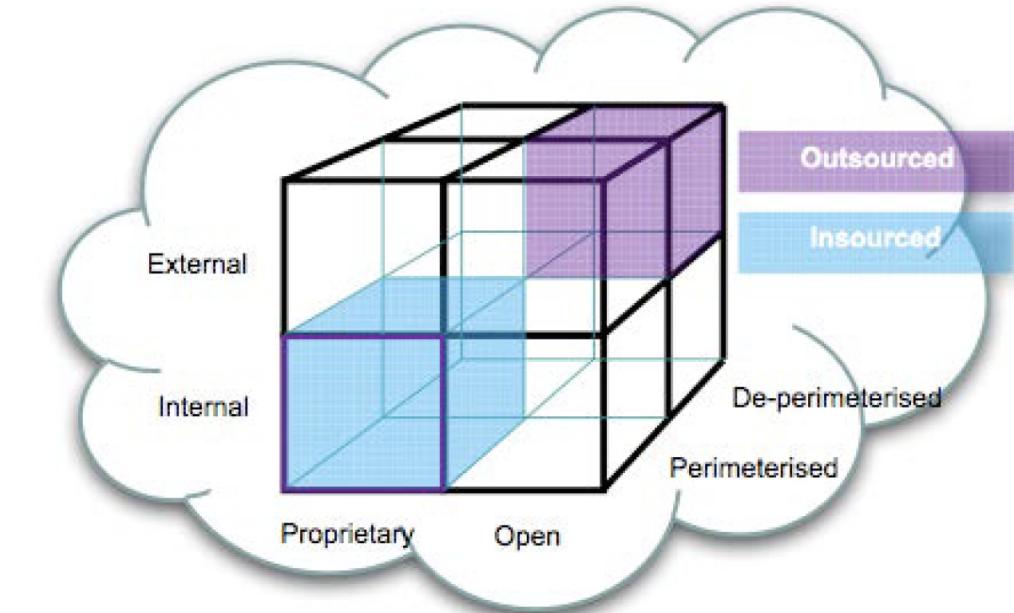
PaaS

IaaS

## Which service model



## Which deployment model



**The Cloud Cube Model**

*Figure 4—Jericho Cloud Cube Model*

Public

Private

Hybrid

Community

# Auditing SaaS

- Customisable reports
  - Application Functionality Configuration options
  - Application Security configuration options  
*(aka ERP configurable controls)*
  - User driven data export /interface capabilities
  - Limited or nil involvement in application development life cycle
  - CAAT development is challenging

Home » Developer Documentation »

## Sample CRM Dashboards

v37.0 EN [Download PDF](#)

Search in document 

Contents

- Sample CRM Dashboards
- Sales & Marketing Dashboards
  - Marketing Executive Dashboard
  - Sales Executive Dashboard
  - Sales Manager Dashboard
  - Salesperson Dashboard
- Customer Service Dashboards

### Marketing Executive Dashboard

Marketing executives, such as directors and VPs, can use this dashboard to find out if they are creating efficient campaigns and generating and converting leads.

#### Campaigns by ROI This Quarter



Campaign Type	Sum of ROI	Sum of Total Value Opportunities
Email Blast...	-100	-100
Email Market...	-100	-100
Search Engine...	-100	-100
Technology...	-100	-100

Campaigns by ROI This Quarter

#### Lead Trending Report



Create Date	Open	Qualified - Convert	Draft	Working	Archived	Approved	Total
December 20, 2010	85	10	5	0	0	0	100
January 20, 2011	15	5	5	0	0	0	25
February 20, 2011	10	5	5	0	0	0	20
March 20, 2011	5	5	5	0	0	0	15
April 20, 2011	2	2	2	0	0	0	6
May 20, 2011	1	1	1	0	0	0	3

Lead Trending Report Last 13 Month

#### Lead Conversion Summary (MTD)

Category	Value
# of Leads Created:	290
# of Leads Converted:	32
Opportunity Amount Converted:	\$356K
Opportunity Amount Converted & Closed:	\$151K

# of Leads by Campaign This Quarter

Campaign Name	Record Count
Email Blast - Services Promotions	3

Top 5 Campaigns by # of Leads

#### Actual ROI by Campaign Type

Campaign Type	Largest ROI
Internet Search	-100
Email	-100
Telemarketing	-100

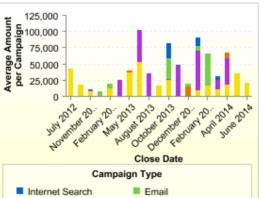
Campaigns by ROI & Campaign Type This Quarter

#### Top Marketing Channels by Campaign

Campaign Name	Record Count
Email Blast - Services Promotions	3

Top 5 Industries by # of Leads

#### Average Oppy Amount per Campaign



Close Date	Internet Search	Telemarketing	Seminar/Conference	Email	Online Ads & Banners	Web Direct
July 2012	100,000	0	0	0	0	0
November 2012	0	0	0	0	0	0
February 2013	0	0	0	0	0	0
May 2013	0	0	0	0	0	0
August 2013	0	0	0	0	0	0
October 2013	0	0	0	0	0	0
December 2013	0	0	0	0	0	0
February 2014	0	0	0	0	0	0
April 2014	0	0	0	0	0	0
June 2014	0	0	0	0	0	0

Average Opportunity Amount per Campaign Last 13 Month

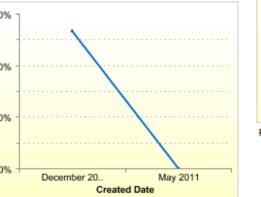
#### Converted Leads by Month



Converted Date	Record Count
12/16/2010	5.5
12/22/2010	2.5
3/27/2011	2.5
6/6/2011	1.5
9/2/2011	4.5
5/2/2012	5.5

Number of Converted Leads Last 13 Month

#### Lead Conversion Rate



Created Date	Conversion Rate
12/1/2010	28%
5/1/2011	10%

Lead Conversion Rate Last 13 Month

#### Leads by Source



Created Month	Direct Mail	Google Adwords	Email	Web Direct	Deal Registration	Referral	Organic	Jigsaw	Total
12/1/2010	0	0	0	0	0	0	0	0	0
5/1/2011	0	0	0	0	0	0	0	0	0

# of Leads by Source Last 13 month

# Auditing SaaS – Application Security

## Monitor Setup Changes

The setup audit trail history tracks the recent setup changes that you and other administrators have made to your org. Audit history can be especially useful in orgs with multiple administrators.

Available in: both Salesforce Classic and Lightning Experience

Available in: Contact Manager, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com Editions

### User Permissions Needed

To view audit trail history:	"View Setup and Configuration"
------------------------------	--------------------------------

To view the setup audit trail history, from Setup, enter **View Setup Audit Trail** in the Quick Find box, then select **View Setup Audit Trail**. To download your org's full setup history for the past 180 days, click the **Download** link.

The setup audit trail history shows you the 20 most recent setup changes made to your org. It lists the date of the change, who made it, and what the change was. Additionally, if a delegate (such as an administrator or customer support representative) makes a setup change on behalf of an end-user, the Delegate User column shows the delegate's username. For example, if a user grants login access to an administrator and the administrator makes a setup change, the administrator's username is listed.

The setup audit trail history tracks the following types of changes:

Setup	Changes Tracked
Administration	<ul style="list-style-type: none"><li>Company information, default settings such as language or locale, and company message changes</li><li>Multiple currency setup changes</li><li>User, portal user, role, permission set, and profile changes</li></ul>

# Auditing SaaS – Application Security

- Logs for access controls, Transaction activity, Change management etc.
- Existence of myriad of logs
- Need automation to map controls to Key Risk Indicators - KRIs
- Opportunities to leverage cloud infrastructure - it is more cost effective and efficient to develop on demand , elastic audit databases, implement audit automation

The screenshot shows the Salesforce Security Guide page. At the top, there's a navigation bar with links for PRODUCTS, RESOURCES, COMMUNITY, BLOG, and TRAILHEAD, along with a search bar and login/signup options. Below the header, the page title is "Salesforce Security Guide". On the left, there's a sidebar with navigation links for various security topics, and a main content area titled "Auditing". The "Auditing" section contains several paragraphs of text and links to further reading.

**Auditing**

Auditing provides information about use of the system, which can be critical in diagnosing potential or real security issues. The Salesforce auditing features don't secure your organization by themselves; someone in your organization should do regular audits to detect potential abuse.

To verify that your system is actually secure, you should perform audits to monitor for unexpected changes or usage trends.

**Record Modification Fields**

All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.

**Login History**

You can review a list of successful and failed login attempts to your organization for the past six months. See [Monitor Login History](#).

**Field History Tracking**

You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. See [Field History Tracking](#).

**Setup Audit Trail**

Administrators can also view a Setup Audit Trail, which logs when modifications are made to your organization's configuration. See [Monitor Setup Changes](#).

◀ Previous

Next ▶

# Auditing IaaS & PaaS

## Example : Continuous Monitoring services in AWS

### AWS CloudTrail

AWS CloudTrail is a service that logs API activity within an AWS account and delivers these logs to an Amazon Simple Storage Service (Amazon S3) bucket.

### Amazon CloudWatch

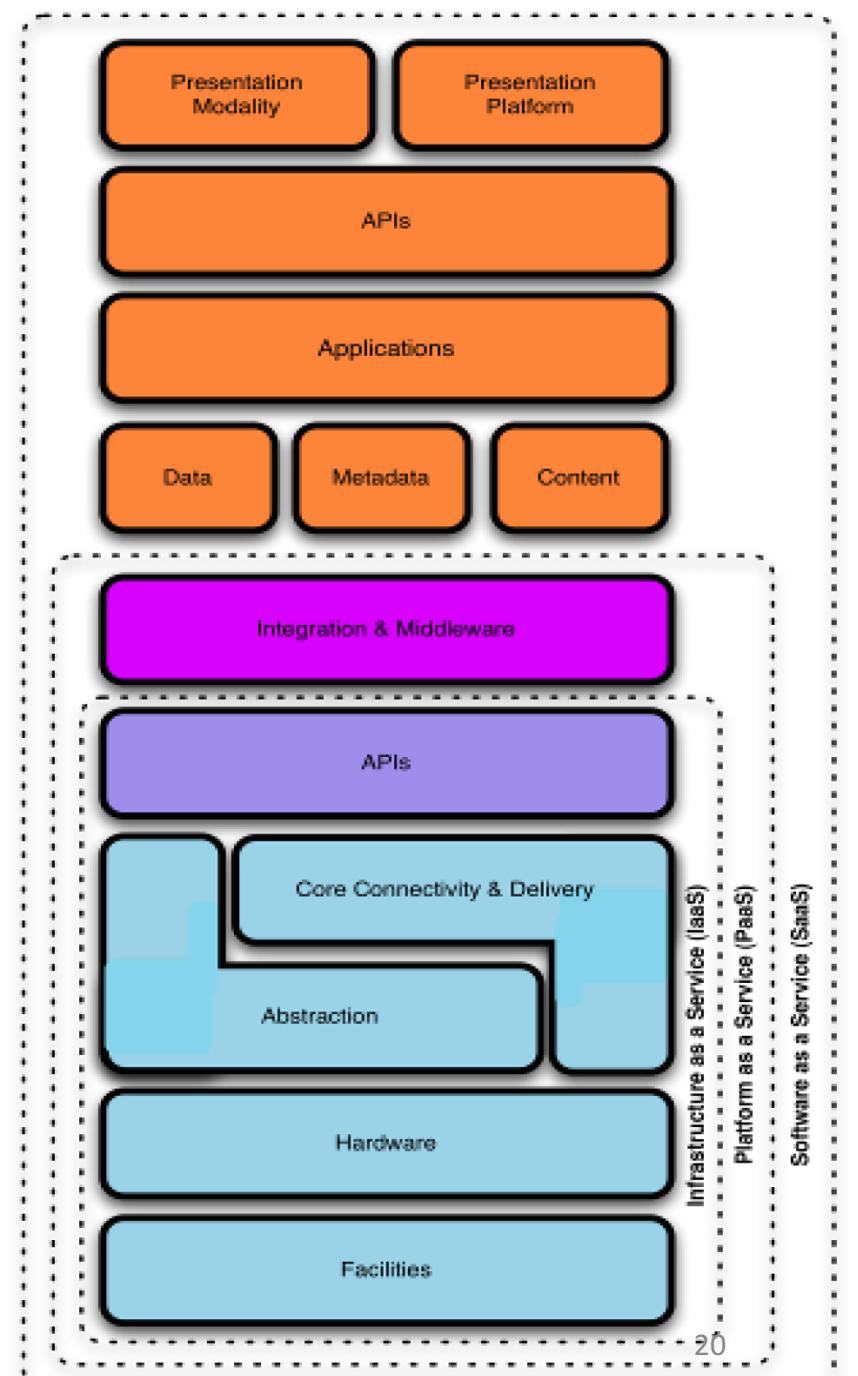
Alarms Amazon CloudWatch alarms notify users and applications when events related to AWS resources occur.

### AWS Config

AWS Config allows detailed tracking and notification whenever a resource in an AWS account is created, modified, or deleted.

### Audit concerns

- Ensure PaaS Portability (open standard APIs)
- New approaches to auditing DevOps (DevOps Control Objectives)
- Audit Automation challenges
- Third party attestation SOC 1/ SOC2
- No physical access to data centre

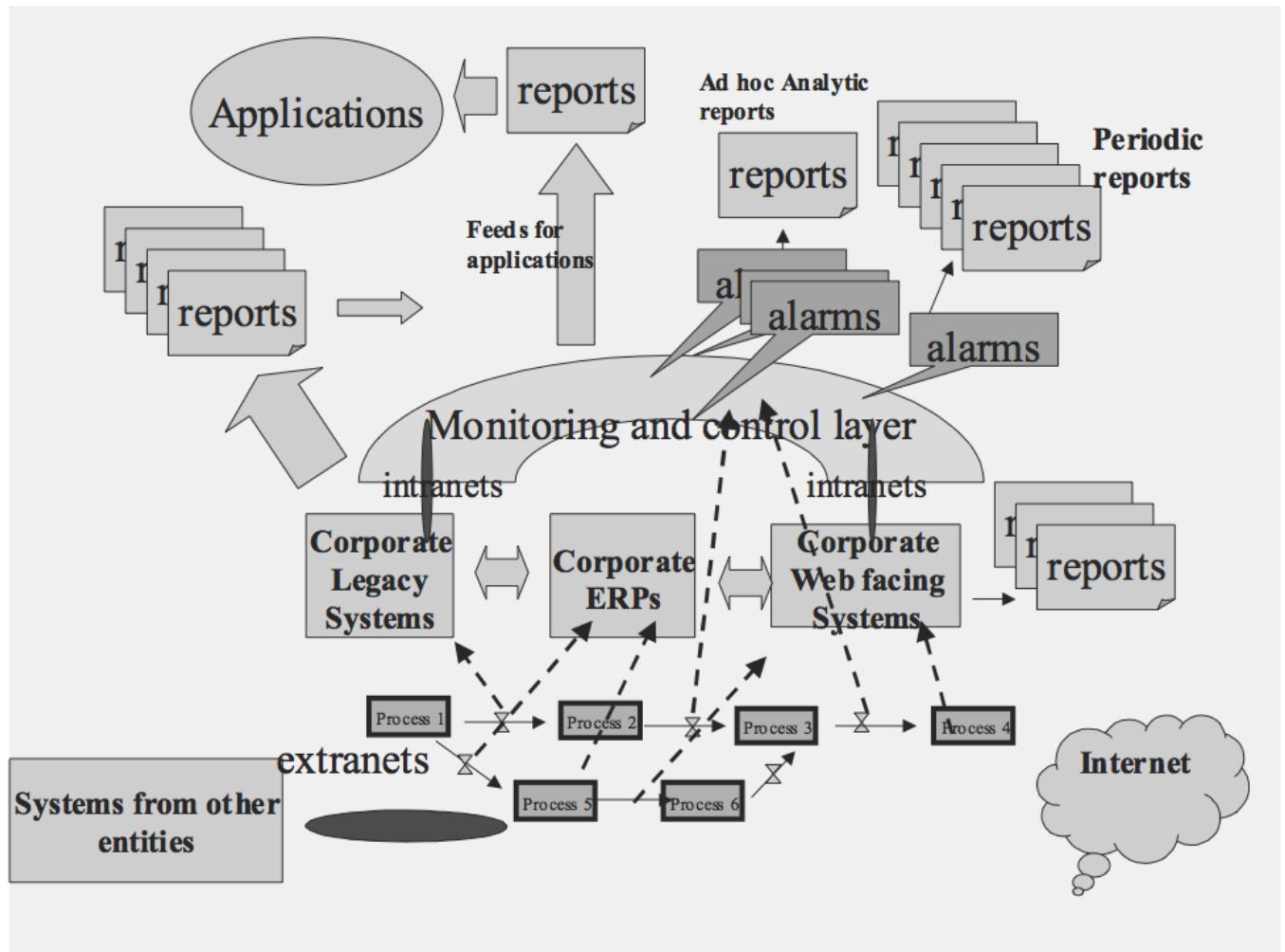


# How can we leverage cloud platform to implement audit automation

Cloud provides unique opportunities for audit automation and audit analytics

- Ability to create VM instances on demand for analytics
- Measured service, low opex
- Rapid elasticity to address audit universe
- Ability to scale down
- Avoid slow data downloads
- Potential for “in memory” analysis
- Big Data - Hadoop/MapReduce

**EXHIBIT 2**  
The Monitoring and Control (MC) Layer in Corporate System Architecture

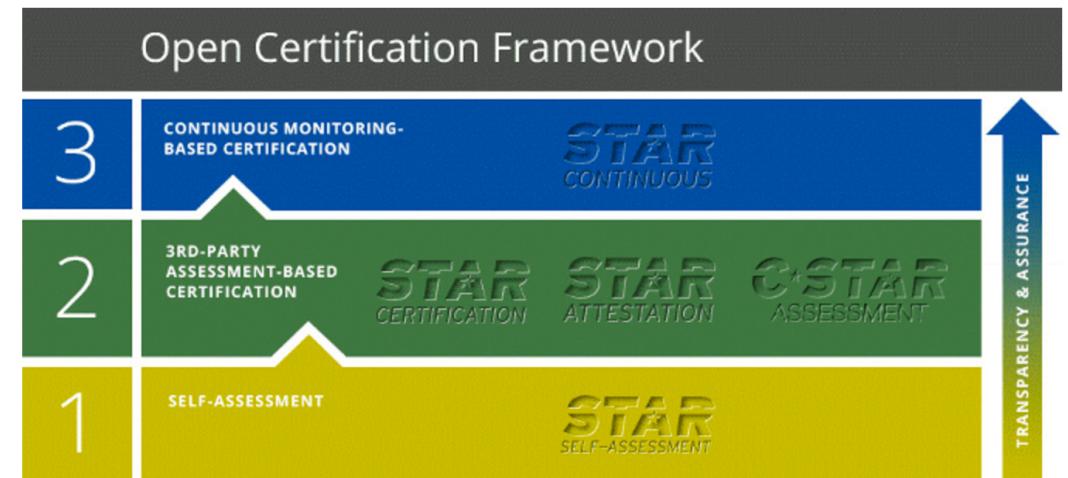


## Cloud Security Alliance – Continuous Audit Initiative

CSA STAR Continuous will be based on a continuous auditing/assessment of relevant security properties.

It will built on the following CSA best practices/standards:

- Cloud Controls Matrix (CCM)
- Cloud Trust Protocol (CTP)
- CloudAudit (A6)



***The CloudTrust Protocol (CTP)*** is the mechanism by which cloud service consumers (also known as “cloud users” or “cloud service owners”) ask for and receive information about the elements of transparency as applied to cloud service providers. The primary purpose of the CTP and the elements of transparency is to generate evidence-based confidence that everything that is claimed to be happening in the cloud is indeed happening as described, ..., and nothing else.

***The goal of CloudAudit*** is to provide a common interface and namespace that allows enterprises who are interested in ***streamlining their audit processes*** (cloud or otherwise) as well as ***cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments*** and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology

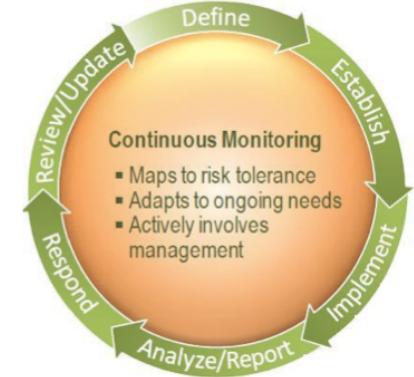


Continuous monitoring is part of the risk management process of FedRAMP, and is a requirement for all CSPs to maintain an ATO. FedRAMP has chosen to implement continuous monitoring because it enables greater transparency into the CSP system and allows for timely risk-management decisions.

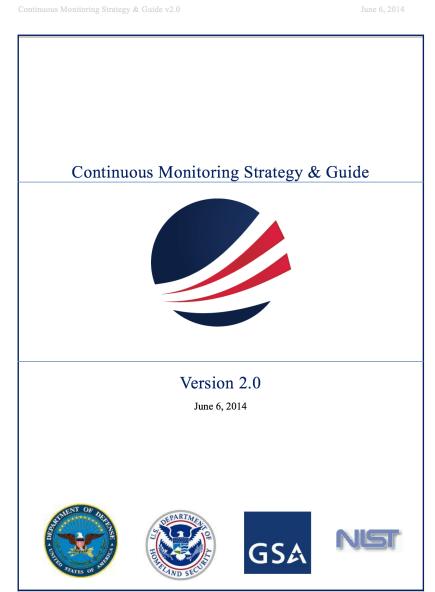
© FedRAMP

Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

© NIST 800-- 137



Continuous Monitoring Strategy Guide



## Summary

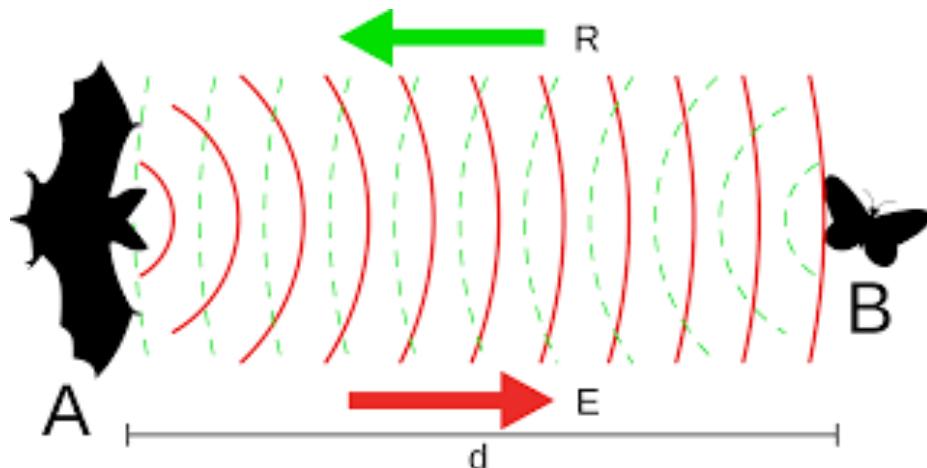
- Cloud Computing has transformed business models, IT infrastructure ownership and operations models
- There is a growing awareness that assurance approach needs to change to address new risks and cloud models
- Cloud Security Alliance and cloud service providers have commenced initiatives / services in continuous auditing and monitoring of Cloud Security
- Cloud platform provides new opportunities to leverage cloud technology to automate Operational, Compliance and Financial auditing and use advanced audit analytics
- Auditor knowledge and experience in cloud computing are critical to quality of cloud audits

**"There are known knowns"** (*Donald Rumsfeld*)

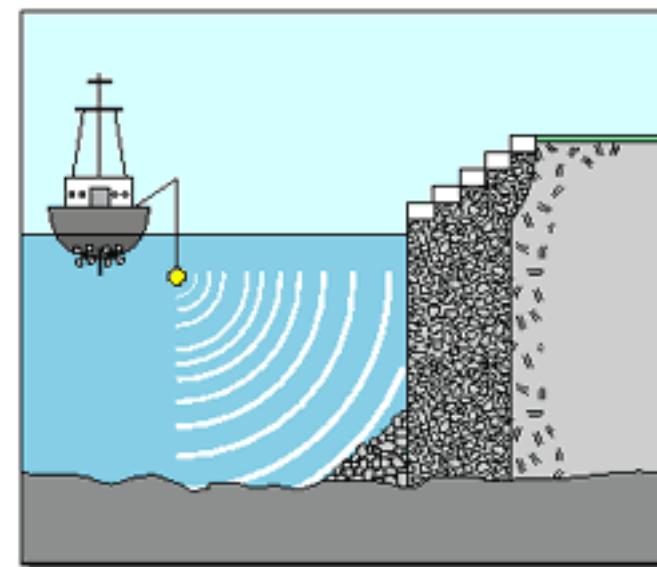
**"True wisdom is knowing what you don't know"** (*Confucious*)



© Wikipedia

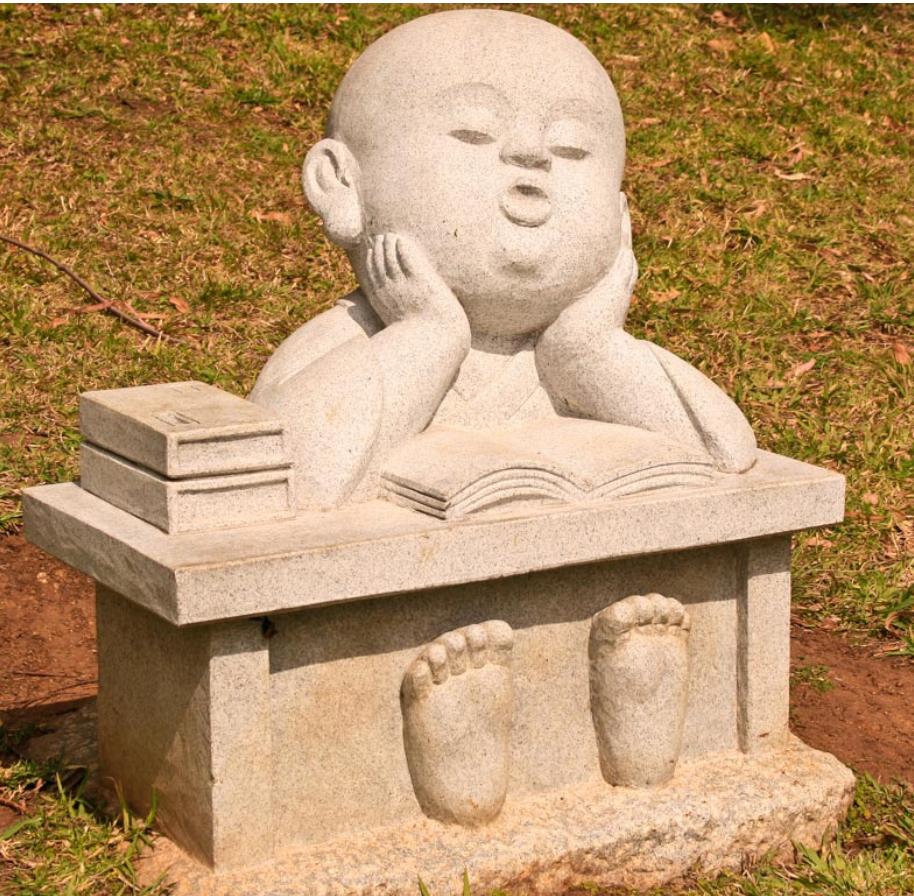


© commons.wikimedia.org



In 1960, Lewis Nixon invented the very first sonar listening device to detect icebergs.

© tech-fact-blogspot.com



# Thank You

Shrikant Deshpande  
*CCSP, CISSP, CISA, CRISC, CGEIT, CIA*

[emailshrikant@icloud.com](mailto:emailshrikant@icloud.com)  
+61 457 560 814