

Security, Compliance & Risk Management for Cloud Relationships

Adnan Dakhwe, MS, CISA, CRISC, CRMA
Safeway Inc.

In-Depth Seminars – D32



Introductions & Poll

-  Organization is leveraging the Cloud?
-  Organization is considering leveraging the Cloud?
-  Have done review/assessment of Cloud Service Providers?
-  Will be doing a review/assessment of Cloud Service Providers?

Agenda

Cloud 101/Overview

Current Trends in Cloud Computing

Benefits of Cloud Computing

Risks and Challenges Companies Need to Consider

Corporate Cloud Strategy and Governance – COSO ERM for Cloud Computing

Key Considerations for Security, Compliance and Risk Management for Cloud Relationships

Resources/Best Practices from ISACA and CSA

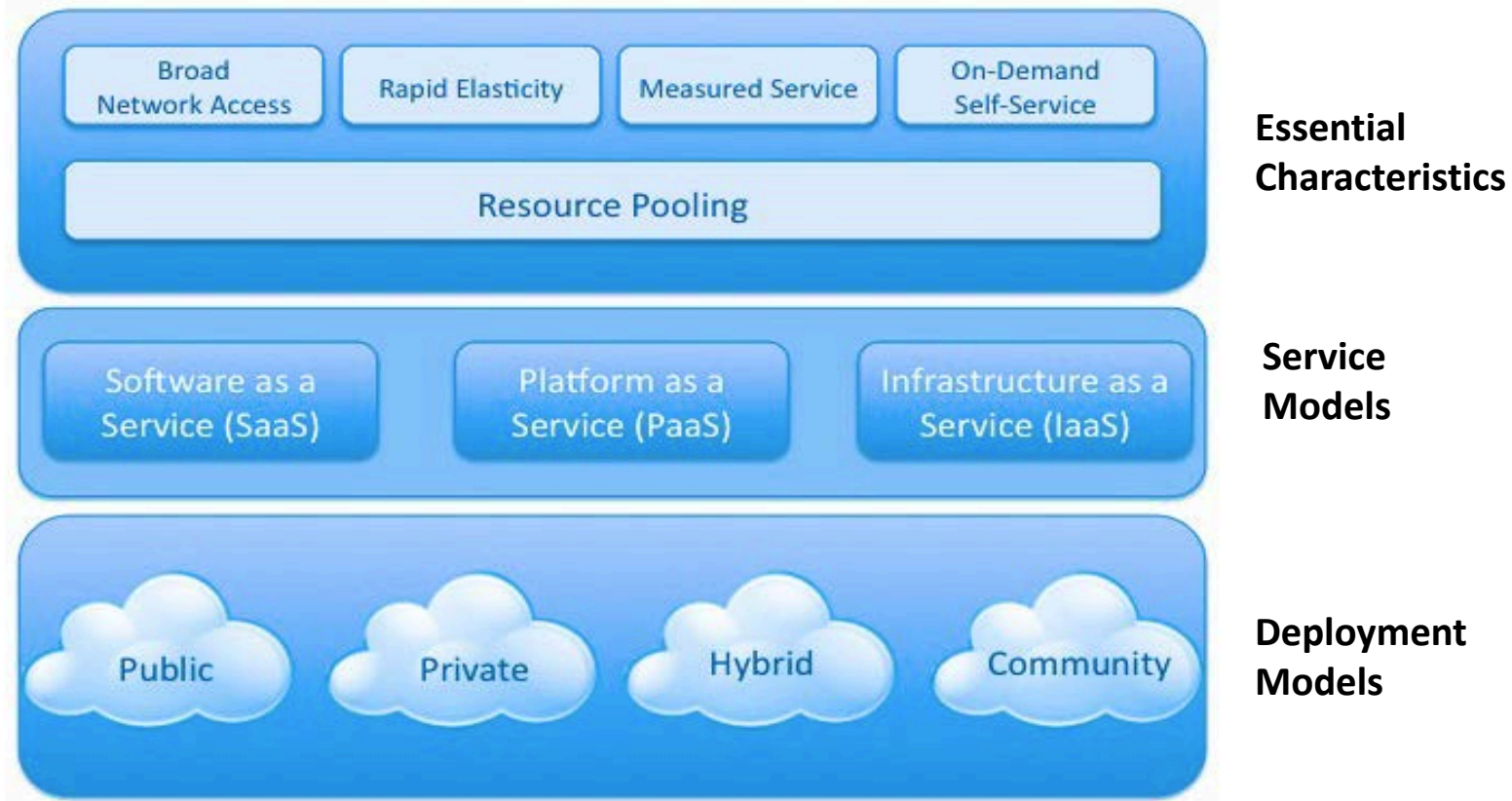
Cloud 101/Overview

What is Cloud Computing?

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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.¹

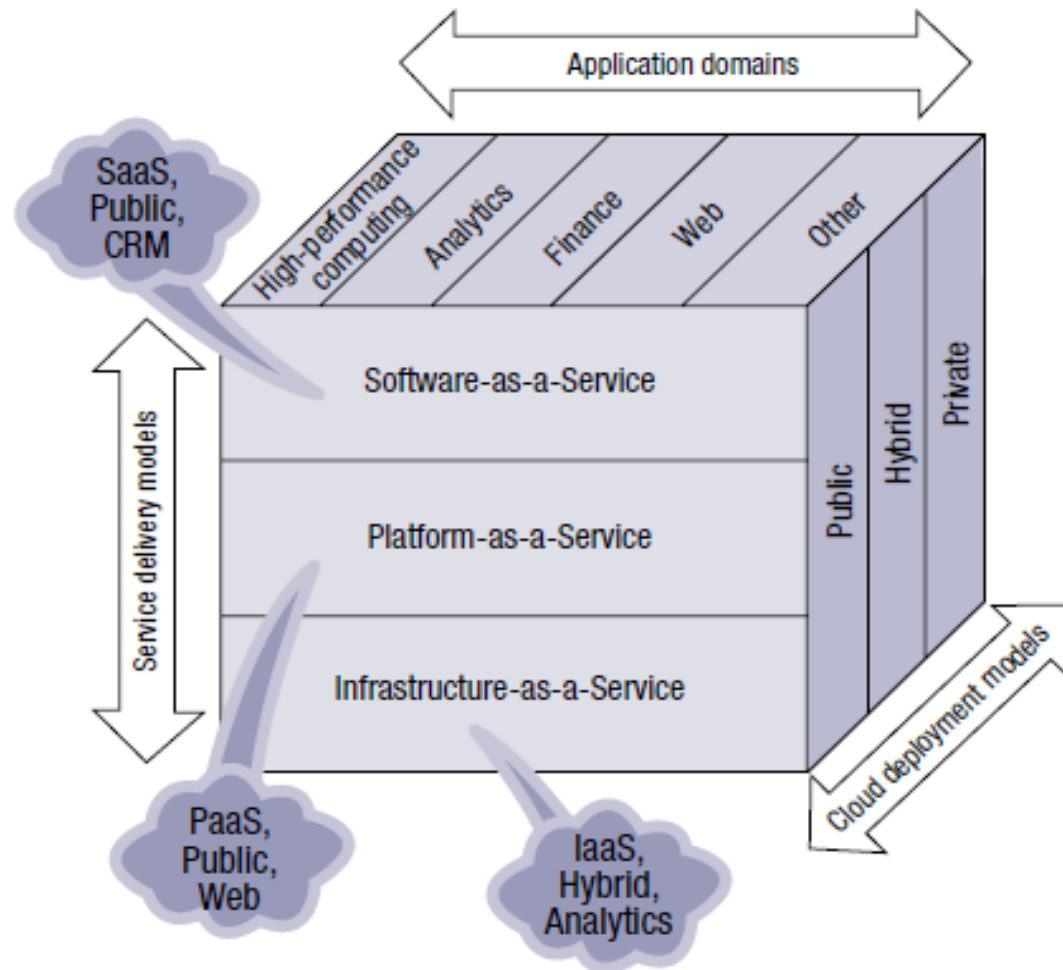
1 – SP 800-145 - The NIST Definition of Cloud Computing

NIST Visual Model of Cloud Computing



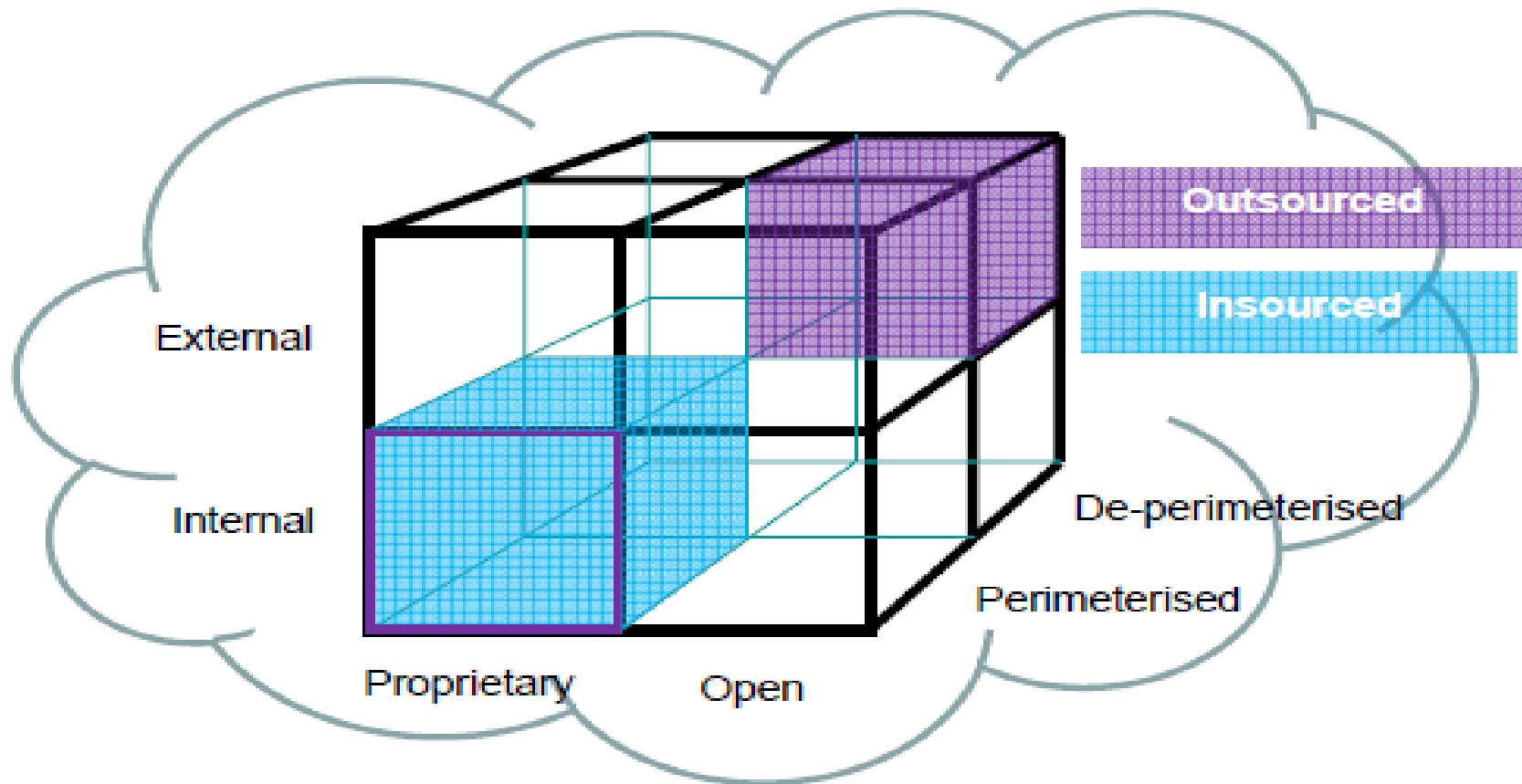
Source – NIST and CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

Cloud Computing Service and Deployment Models



Source – ISACA – IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

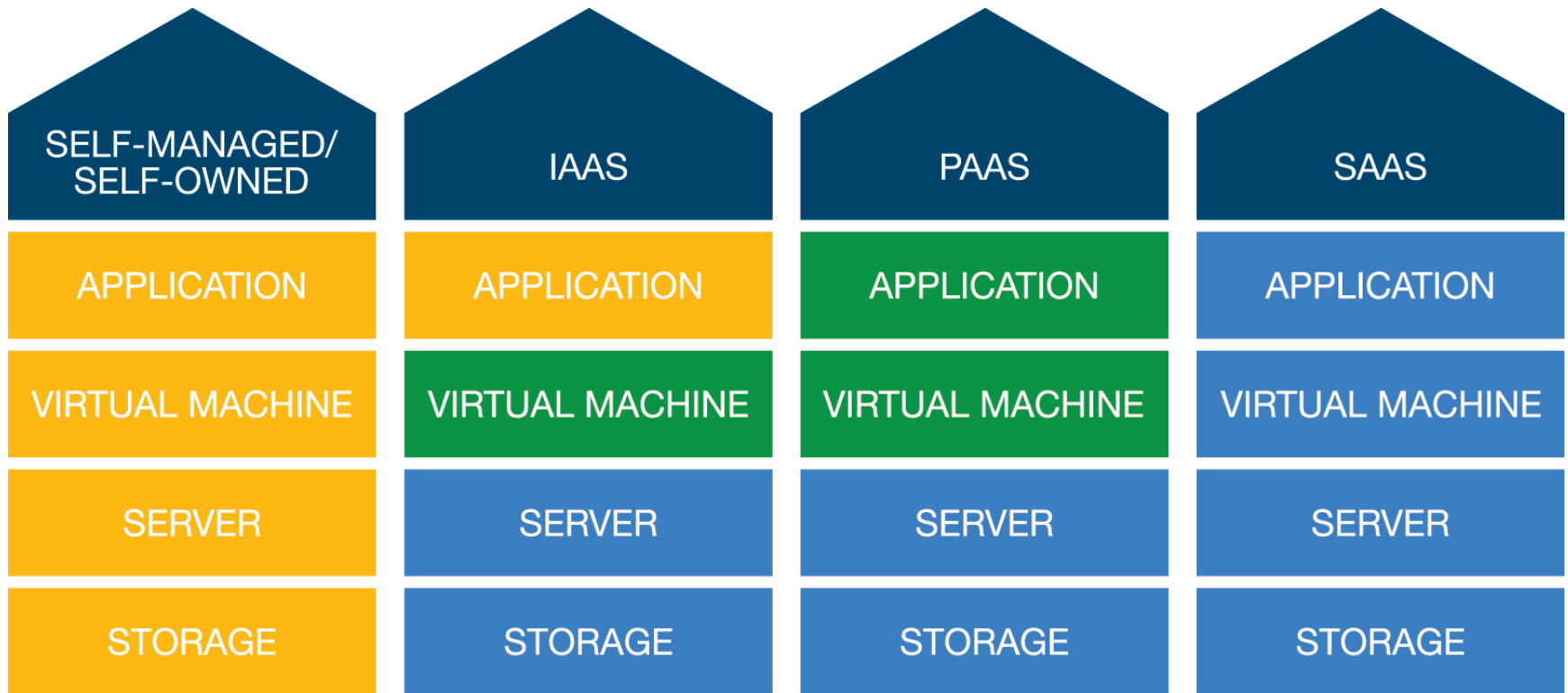
Jericho Forum – Cloud Cube Model



The Cloud Cube Model

Source – https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Levels of Control by Cloud Service Model



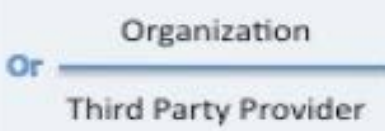

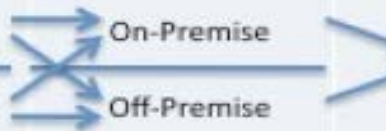
Organization
has control

Organization shares
control with vendor

Vendor
has control

Source – COSO – ERM for Cloud Computing

Cloud Deployment Models

	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization Third Party Provider	 Organization Third Party Provider	 On-Premise Off-Premise	 Trusted
Hybrid	<u>Both</u> Organization & Third Party Provider	<u>Both</u> Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

¹ Management includes: governance, operations, security, compliance, etc...

² Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

³ Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control

⁴ Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Source – CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

Current Trends in Cloud Computing

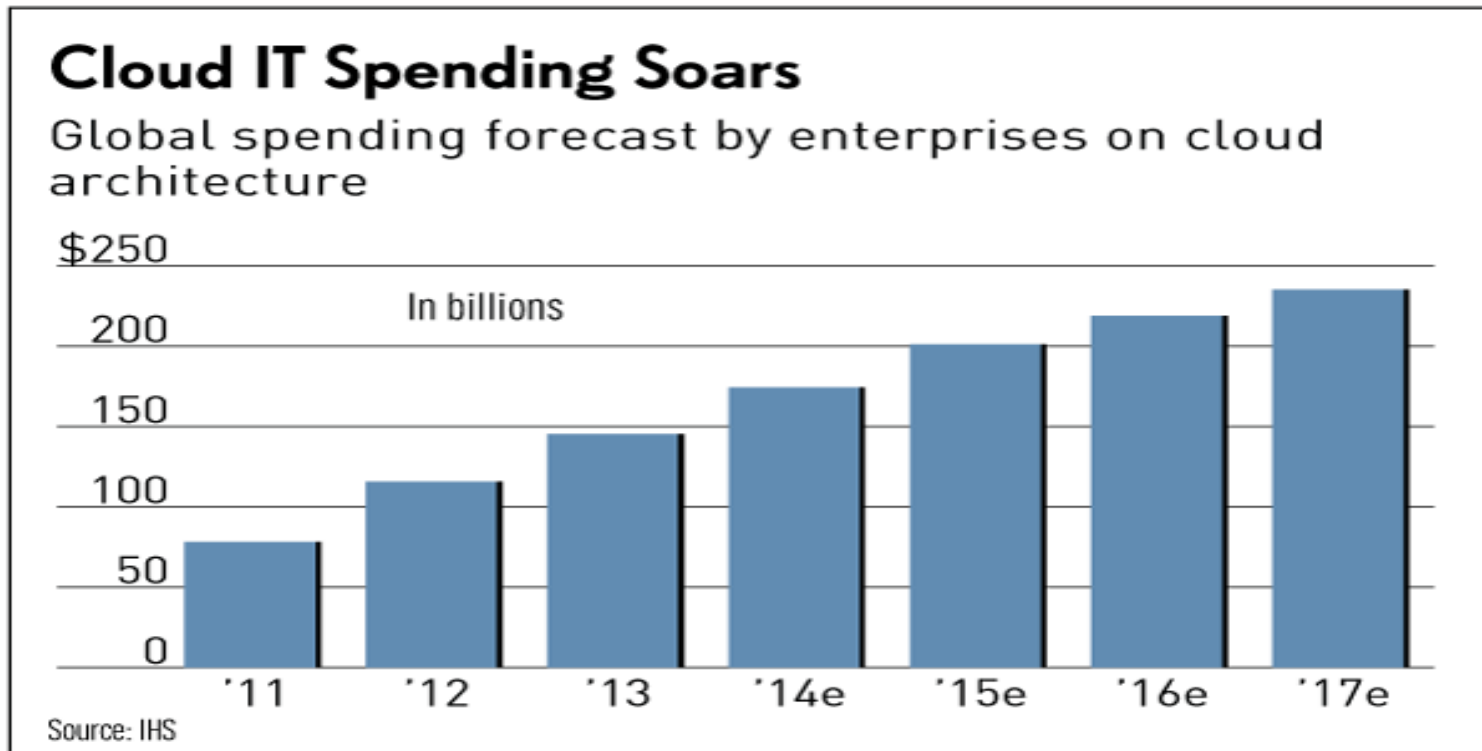


CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Trends in Cloud Computing

Corporate spending on cloud infrastructure and services is forecast to triple from 2011 to 2017 to a projected \$235.1 billion.¹



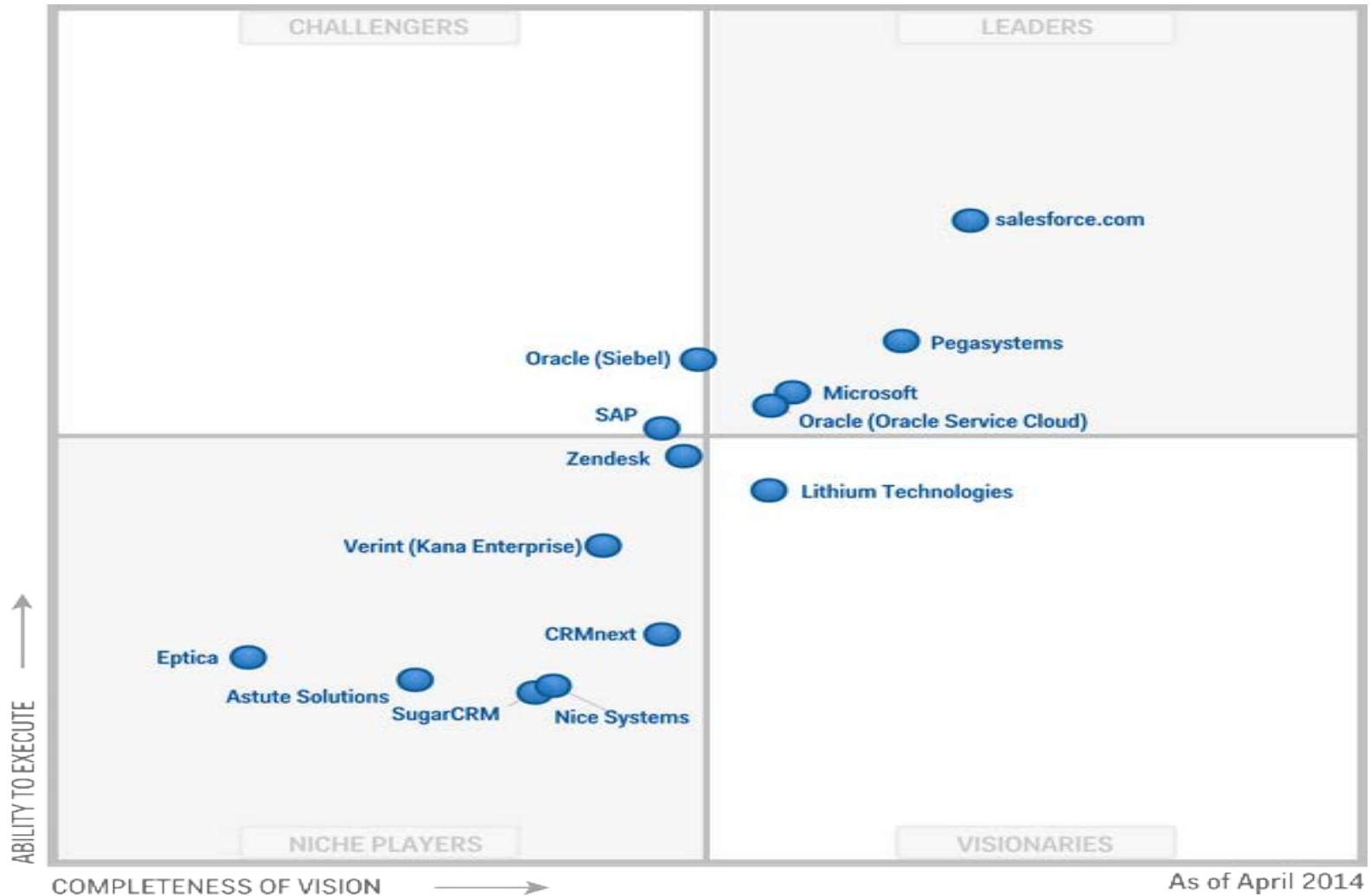
1 – IHS Technology Study

Trends in Cloud Computing

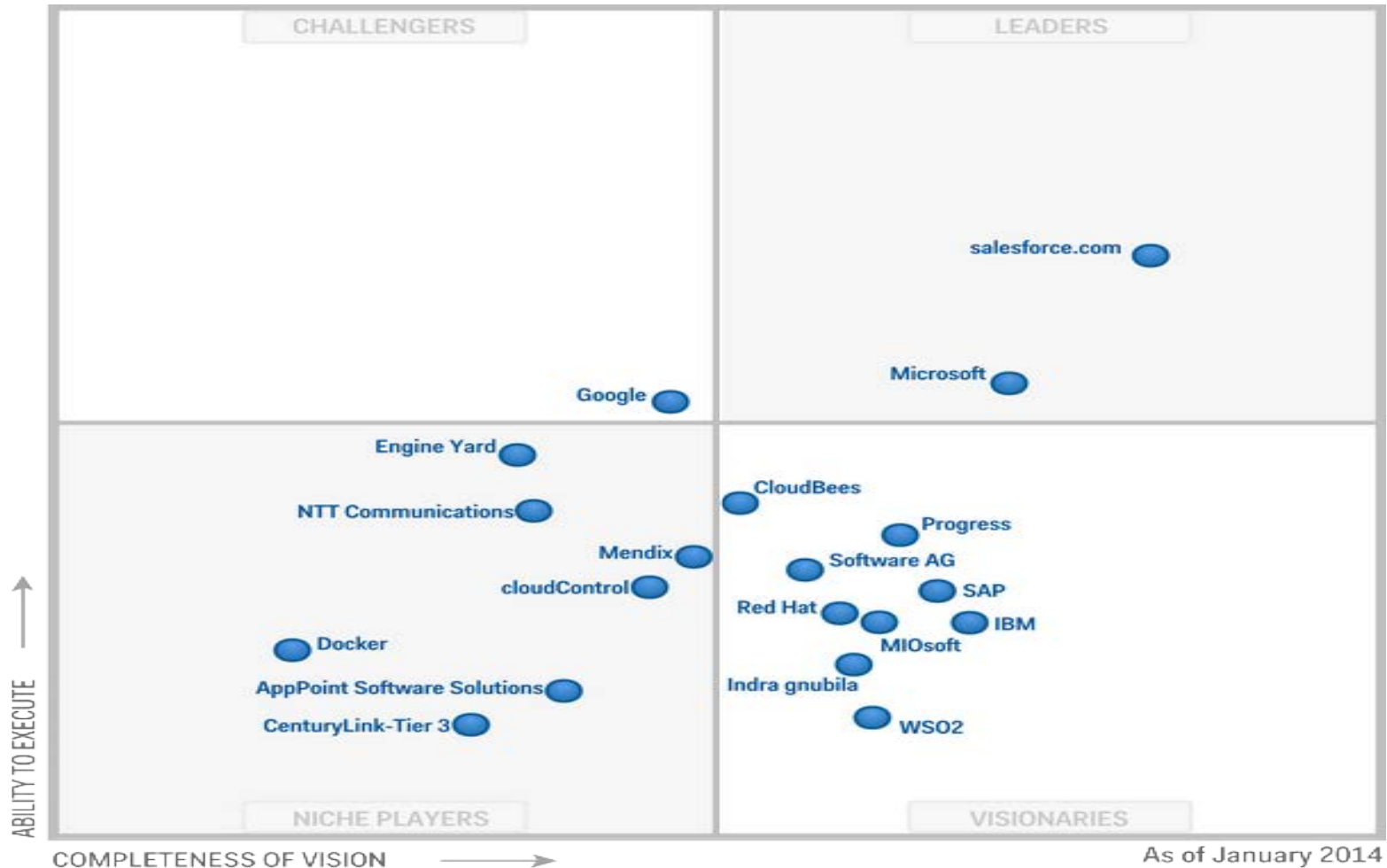
The global cloud computing market is expected to grow at a 30% compound annual growth rate (CAGR) reaching \$270 billion in 2020.¹

1 – www.marketresearchmedia.com - Global Cloud Computing Market Forecast 2015-2020

Gartner Magic Quadrant for SaaS - CRM Customer Engagement Center



Gartner Magic Quadrant for Enterprise Application PaaS



Gartner Magic Quadrant for IaaS



New Service Offerings

- Disaster Recovery as a Service - DRaaS
- Security as a Service – SecaaS
- Identity as a Service – IDaaS
- Data Analytics as a Service – DAaaS
- Data Storage as a Service - DSaaS
- Information as a Service (InfoaaS)
- Integration Platform as a Service (IPaaS)
- Forensics as a Service (FRaaS)

Source – ISACA – Controls and Assurance in the Cloud Using COBIT 5

Benefits of Cloud Computing



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Benefits of Cloud for User Organizations (Customers)

- Cost savings/reduction/management – lower entry costs, pay as you go, CAPEX to OPEX, reduced hardware infrastructure costs, reduced IT staffing and administration costs, etc.
- Scalability
- Flexibility/agility and speed of deployment
- Environmental benefits – power reduction for the user company, enhancement of user company's "green" credentials
- Optimized server utilization
- Access to capabilities/skills which are not in-house
- Faster cycle of innovation

Risks and Challenges Companies Need to Consider



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Risks and Challenges

- Vendor Management - inadequate contracts (right to audit clause, etc.), service provider viability, financial stability, etc.
- Regulatory Compliance – PCI, HIPAA, SOX, GLBA, etc.
- Data Security and Privacy – data location, co-mingled data/data segregation, loss of control over data, consolidation of multiple organizations presents a more attractive target for attacks, physical security, etc.
- Reliability, Availability and Performance – SLAs, etc.
- Termination of Services - vendor lock-in, portability and interoperability, etc.
- Business Continuity, Disaster Recovery and Resilience
- Shadow IT
- Access Control and Identity Management
- Governance
- Integration with existing systems
- Record protection/support for forensic audits
- Incident Management

Recent Cloud Outages

- Microsoft Cloud Service Azure Experienced Global Outage – August 13, 2014 – Lasted around 5 hours¹
- Microsoft Exchange – June 24, 2014 - Almost 9 hours – networking infrastructure issue²
- Microsoft Lync – June 23, 2014 – several hours - network routing infrastructure issues²
- iCloud – June 12, 2014 – few hours²
- Feedly – June 11 – 13, 2014 – on and off for 3 days – DDoS attack²
- Evernote – June 10, 2014 – 10+ hours – DDoS attack²
- Adobe Creative Cloud service – May 16, 2014 – About 28 hours - database maintenance activity caused the outage²
- Samsung's Smart TV platform global outage – April 20, 2014 – 4.5 hours – fire at one of the facilities in South Korea, was sparked by a failure with a power supply.²
- Basecamp goes offline – March 24, 2014 – Around 2 hours – due to DDoS attack²
- Google Apps – March 17, 2014 – About 3.5 hours – maintenance gone wrong²
- Dropbox – March 2, 2014 – Just under an hour²
- Gmail, Google Calendar, Google Docs, and Google+ go offline – January 24, 2014 – About an hour – software bug²
- Dropbox – January 10, 2014 – About 2 days - a scripting glitch caused OS upgrades to be applied on actively running machines during routine maintenance.²

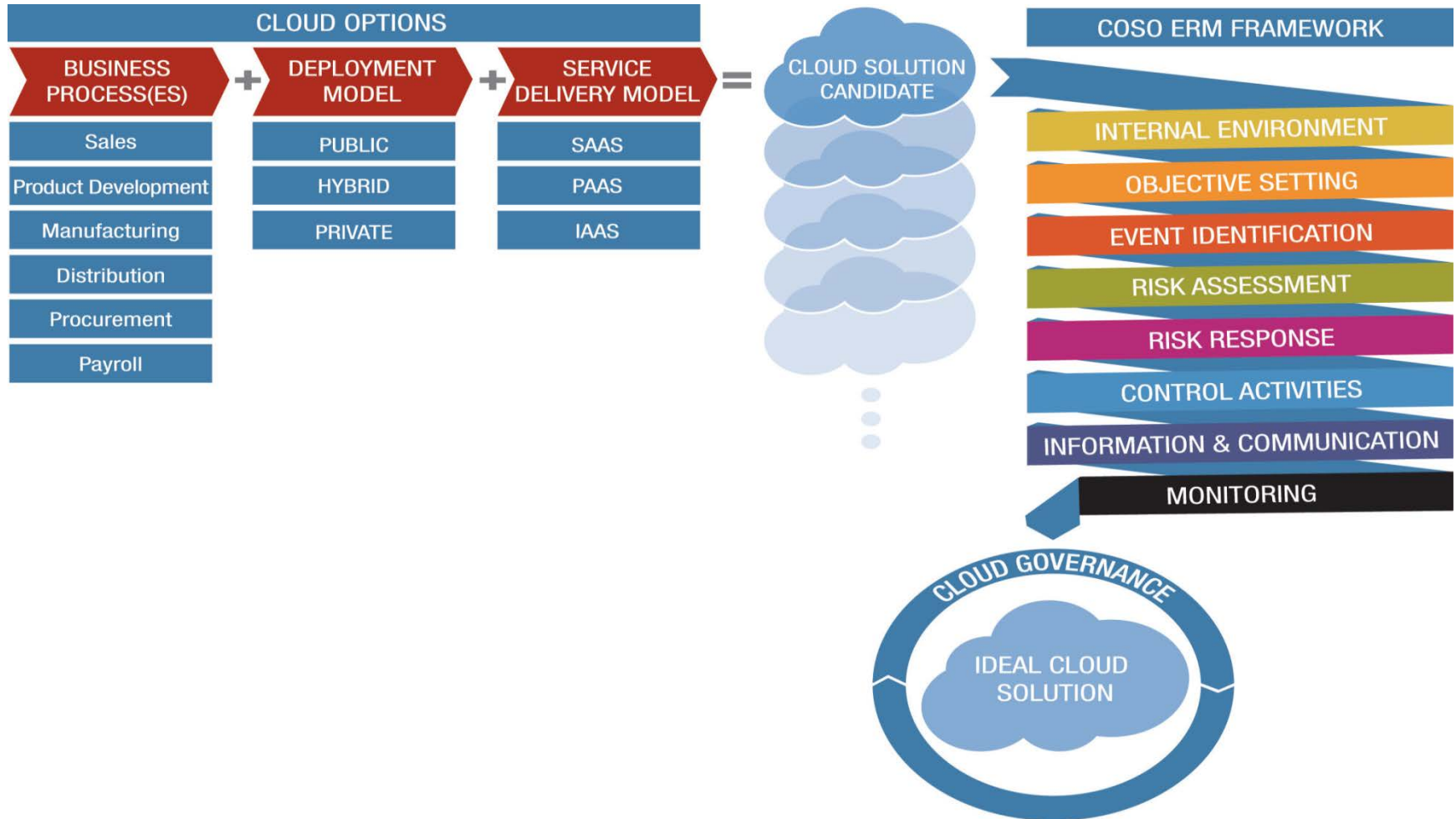
1 - <http://www.bloomberg.com/news/2014-08-18/microsoft-s-cloud-computing-service-azure-experiencing-outage.html>

2 - <http://www.infoworld.com/article/2606209/cloud-computing/162288-The-worst-cloud-outages-of-2014-so-far.html>

Corporate Cloud Strategy and Governance – COSO ERM for Cloud Computing



Corporate Cloud Strategy and Governance: COSO ERM Framework for Cloud Computing



Source – COSO Enterprise Risk Management for Cloud Computing.

Corporate Cloud Strategy and Governance

Some of the governance and monitoring aspects for cloud relationships can be automated using tools; e.g., from Netskope or Skyhigh Networks.

Key Considerations for Security, Compliance and Risk Management for Cloud Relationships

Key Considerations for Security, Compliance and Risk Management

- Strategy - Evaluate if cloud is right for you as an option for IT sourcing?
- Give a deep thought before putting mission critical data in the cloud
- Assess Cloud Service Providers (CSP) – SOC 1/2/3, ISAE 3402, ISO 2700x, STAR Registry, OCF, CAIQ, CCM, etc.
- Contract - Ensure adequate terms, conditions and SLAs
- Support for eDiscovery and forensic audits
- Encrypt any sensitive data or use tokenization
- Ensure compliance requirements are met
- Ensure adequate identity and access management for users including CSP staff
- Secure disposition of data from servers including backups
- Define termination/exit and portability items upfront
- Governance and monitoring
- Business continuity and disaster recovery
- Backups
- Information security
- Physical security

Information Security Considerations

- Policies and procedures
- IPS/IDS, penetration testing and vulnerability management
- Adequate authentication controls
- DLP, antivirus, anti-malware, log management and file integrity management
- Web application security – web application firewall (WAF), encryption (data at rest and in motion) or tokenization, key management, etc.
- Incident response plan
- Configuration, change and patch management
- Security Information Event Management (SIEM)
- Virtualization security and controls
- Make sure your (customer organization) internal security is up to date. Don't let your corporate network become the weakest link in the chain.

Key Points to Consider for Contracts

- Right to audit clause
- Third party assurance of controls – SOC 1/2/3, ISAE 3402, ISO 27001, etc.
- Financial performance monitoring (needs to be negotiated in the contract for private service providers)
- Governance and monitoring
- Regulatory compliance
- Dispute resolution and termination
- Information Security and physical security requirements – IPS/IDS, WAF, penetration testing, vulnerability management, SIEM, etc.
- Service level agreements and reporting procedures
- Recourse and remediation of unsatisfactory performance
- Data breach liability

Key Points to Consider for Contracts

- Incident management
- Confidentiality/Intellectual Property
- Disaster recovery and business continuity
- Sub-contracting – i.e., CSP is leveraging other CSPs
- eDiscovery and forensics
- Handling of sensitive data – encryption
- Disposition of data
- Term of contract
- Billing provisions
- Non-disclosure

Resources/Best Practices from ISACA and CSA



ISACA – Security Considerations for Cloud Computing

Security Considerations for Cloud Computing

- Download (873K; Member Only)
- Purchase the eBook
- Download Tool Kit (267K; Member Only)
- Consideraciones para la Nube Checklist (Spanish, 27K; Member Only)
- Purchase the Book
- Provide feedback on this document
- Visit the Cloud Computing Knowledge Center community

Another publication in the Cloud Computing Vision Series, *Security Considerations for Cloud Computing* presents practical guidance to facilitate the decision process for IT and business professionals concerning the decision to move to the cloud. It helps enable effective analysis and measurement of risk through use of decision trees and checklists outlining the security factors to be considered when evaluating the cloud as a



Security-Considerations-Cloud-Computing-Tool-Kit.zip

Search Sec

Name

- 1 Table of Contents.pdf
- 2. Breakdown of Cloud Service Model Decision Tree.docx
- 3. Breakdown of Cloud Deployment Decision Tree.docx
- 4. Cloud Considerations Checklist.docx
- 5. Risk Factors of Cloud Service and Deployment Models.docx
- 6. Cloud Threats and Mitigating Actions Mapped to COBIT 5 for Information Security.docx

source - <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Considerations-for-Cloud-Computing.aspx>

ISACA Cloud Resources – Security, Compliance and Risk Management



Source - <http://www.isaca.org/Knowledge-Center/Research/Pages/Cloud.aspx>

ISACA Cloud Resources – Security, Compliance and Risk Management



Source - <http://www.isaca.org/Knowledge-Center/Research/Pages/Cloud.aspx>

CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

14 domains:

- Cloud Computing Architectural Framework
- Governance and Enterprise Risk Management
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Audit Management
- Information Management and Data Security
- Interoperability and Portability
- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operations
- Incident Response
- Application Security
- Encryption and Key Management
- Identity, Entitlement and Access Management
- Virtualization
- Security as a Service

Source – https://cloudsecurityalliance.org/research/security-guidance/#_overview

CSA Cloud Controls Matrix (CCM)

- Control framework that gives detailed understanding of security concepts and principles
- Strengthens information security control environments by delineating control guidance by service provider and consumer, and by differentiating according to cloud model type and environment
- Maps to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, COBIT, PCI, NIST, NERC CIP, ENISA, COPPA, HIPAA/HITECH, AICPA 2014 Trust Services Criteria, etc.
- 133 controls

Source – <https://cloudsecurityalliance.org/research/ccm/>

CSA Cloud Controls Matrix (CCM) v3.0.1

AIS Application & Interface Security	HRS Human Resources Security
AAC Audit Assurance & Compliance	IAM Identity & Access Management
BCR Business Continuity Mgmt & Op Resilience	IVS Infrastructure & Virtualization
CCC Change Control & Configuration Management	IPY Interoperability & Portability
DSI Data Security & Information Lifecycle Mgmt	MOS Mobile Security
DSC Datacenter Security	SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
EKM Encryption & Key Management	STA Supply Chain Mgmt, Transparency & Accountability
GRM Governance & Risk Management	TVM Threat & Vulnerability Management


Source – <https://cloudsecurityalliance.org/research/ccm/>

CSA Cloud Controls Matrix (CCM) v3.0.1

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1										
2	Control Domain	CCM V3.0 Control ID	Updated Control Specification	COBIT 5.0	COPPA	CSA Enterprise Architecture (formerly Trusted Cloud Initiative)			CSA Guidance V3.0	ENISA IAF
3										
4										
						Domain > Container > Capability	Public	Private		
5	Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03	312.8 and 312.10	Application Services > Development Process > Software Quality Assurance	shared	x	Domain 10	6.03.01. (c)
6	Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	APO09.01 APO09.02 APO09.03 APO13.01	312.3, 312.8 and 312.10	BOSS > Legal Services > Contracts	shared	x	Domain 10	
7	Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	DSS06.02 DSS06.04	312.8 and 312.10	Application Services > Programming Interfaces > Input Validation	shared	x	Domain 10	
8	Application & Interface Security Data Security / Integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.	APO09.01 APO09.02 APO09.03 APO13.01 DSS05.02 DSS06.06	312.8 and 312.10	BOSS > Data Governance > Rules for Information Leakage Prevention	shared	x	Domain 10	6.02. (b) 6.04.03. (a)
	Audit Assurance & Compliance Audit Planning	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any	APO12.04 APO12.05 APO12.06 MEA02.01 MEA02.02	Title 16 Part 312	BOSS > Compliance > Audit Planning	shared	x	Domain 2, 4	6.01. (d)

Source – <https://cloudsecurityalliance.org/research/ccm/>

CSA Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1

<div>  <div> CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1 </div> </div>								
Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	AICPA TSC 2009	AICPA Trust Service Criteria (SOC 2SM Report)	AICPA TSC 2014	BITS Shared Assessments AUP v5.0
Application & Interface Security <i>Application Security</i>	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	CC7.1	1.4
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?				
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?				
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?				
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?				

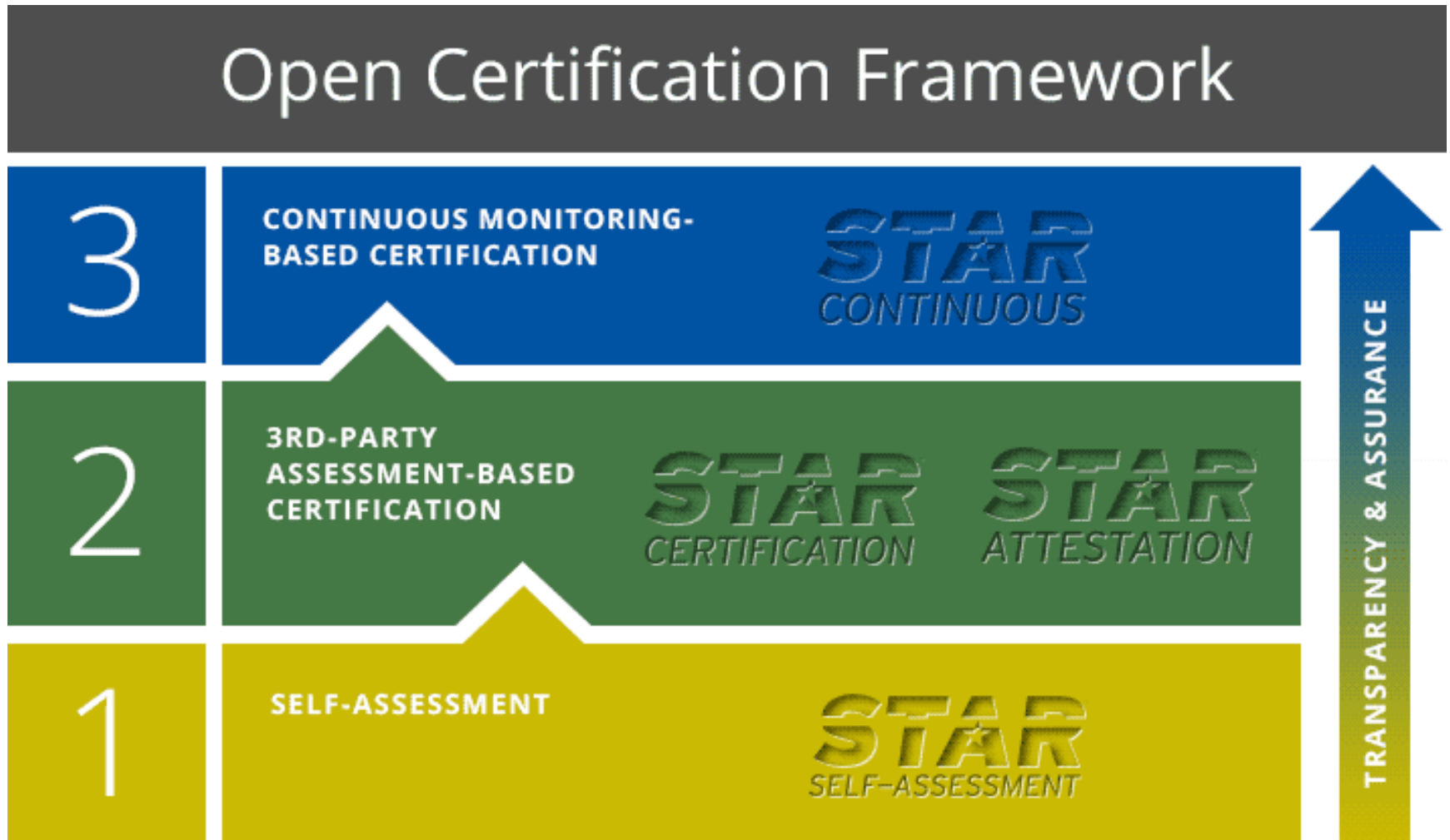
Source – <https://cloudsecurityalliance.org/research/cai/>

CSA Security, Trust and Assurance Registry (STAR)

- **LEVEL ONE: CSA STAR Self-Assessment:** Cloud providers either submit a completed CAIQ, or to submit a report documenting compliance with CCM. Free offering.
- **LEVEL TWO: CSA STAR Attestation:** Collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM.
- **LEVEL TWO: CSA STAR Certification:** A rigorous third party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2005 management system standard together with the CSA CCM.
- **LEVEL THREE: CSA STAR Continuous Monitoring:** Currently under development and scheduled for 2015 release, CSA STAR Continuous Monitoring enables automation of the current security practices of cloud providers. Providers publish their security practices according to CSA formatting and specifications, and customers and tool vendors can retrieve and present this information in a variety of contexts.

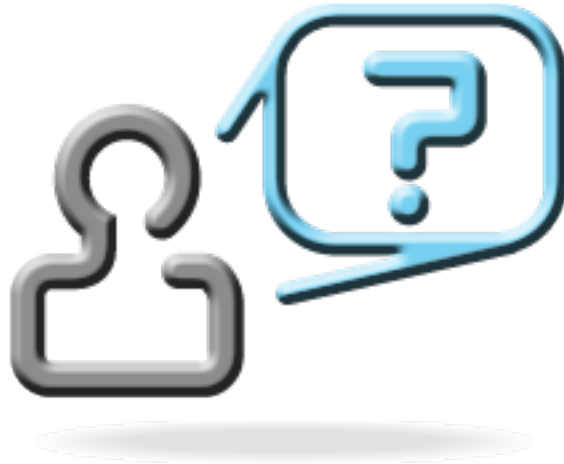
Source – <https://cloudsecurityalliance.org/star/>

CSA Security, Trust and Assurance Registry (STAR)



Source – <https://cloudsecurityalliance.org/star/>

Questions?



Contact Information



Adnan Dakhwe, MS, CISA, CRISC, CRMA

adnan.dakhwe@safeway.com

adnandakhwe@gmail.com

<https://www.linkedin.com/in/adnandakhwe>

Thank you !