

Maintaining Ownership & Control of Your Data, Optimising cloud security, trust and transparency



November 25, Lloyd Hotel, Amsterdam
Round table - Cloud Computing : Legal Tips
Organised by ICT Legal Consulting

Reinier Landsman BSc BBA
Chairman Cloud Security Alliance Netherlands Chapter
Managing Partner at Cert2Connect B.V.

About the Cloud Security Alliance

- Global, not-for-profit organisation
- Over 48,000 individual members, more than 180 corporate members, and 65 chapters
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
 - GRC: Balance compliance with risk management
 - Reference models: build using existing standards
 - Identity: a key foundation of a functioning cloud economy
 - Champion interoperability
 - Enable innovation
 - Advocacy of prudent public policy

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

Cloud BARRIERS

- (Perceived) Loss of control
- Lack of clarity around the definition and attribution of responsibilities and liabilities
- Difficulties achieving accountability across the cloud supply chain
- Incoherent global (and even sometimes regional and national) legal framework and compliance regimes



....and more barriers

- The lack of transparency of some service providers or brokers
- Lack of clarity in Service Level Agreements
- Lack of interoperability.
- Lack of awareness and expertise



In 3 words: **LACK OF TRUST**



“Let’s try it once without the parachute.”

HOW DO WE BUILD TRUST & TRANSPARENCY?

➤ Good Practices for INDIRECT CONTROL

➤ Accountability



➤ Assessment & Certification



➤ Sharing information



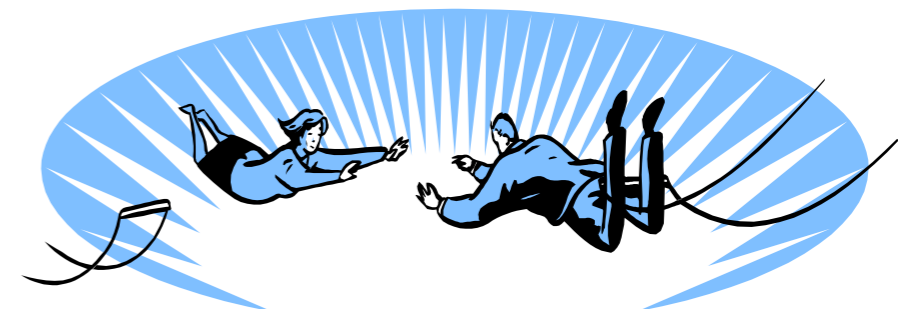
Cloud enforces to think about?

- Separation between data owners and data processors!
- Anonymity of location data center and equipment
- Anonymity of suppliers
- Temporary relationships with suppliers
- Physical checks to be compensated by virtual controls
- Identity management has a key role in the whole!
- Cloud requires a renewed approach to security
- Data residency, laws and regulations
- Maintaining Ownership & Control of Your Data
- Data encryption




What are the trust issues

- Is my cloud provider transparent about the governance and operational issues?
- Am I still viewed as compliant for my environment?
- Do I know where my data is located?
- Is the lack of standardization an accelerated aging issue (accelerated depreciation)?
- Are my cloud service providers really better at security than I can do it myself?
- Am I in the cloud a popular target for hackers?
- Is the existing IT staff still needed?

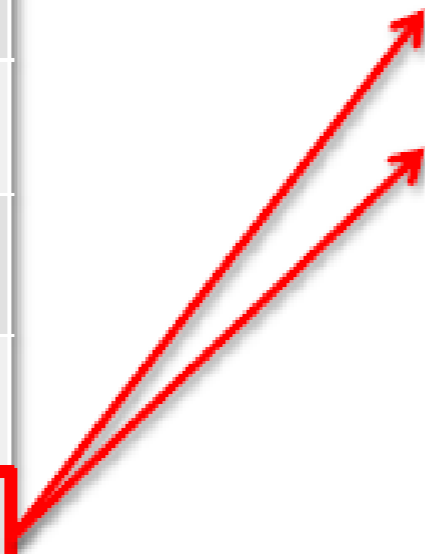


Top threats 2013: CSA

2010 Top Threats	
1	Abuse of Cloud Services
2	Insecure APIs
3	Malicious Insiders
4	Shared Technology Issues
5	Data Breaches & Loss
6	Account Hijacking
7	Insufficient Due Diligence

 cloud security alliance™ Survey of 300 security professionals in 50 countries

2013 Top Threats	
1	Data Breaches
2	Data Loss
3	Account Hijacking
4	Insecure APIs
5	Denial of Service
6	Malicious Insiders
7	Abuse of Cloud Services
8	Insufficient Due Diligence
9	Shared Technology Issues



Most important issues for the future

- Can I keep the same trend with cloud changes?
- Worldwide incompatible legislation and policy?
- No standardized Private and Public clouds
- Lack of continuous Risk Management & Compliance Monitoring
- Incomplete Identity Management implementations
- Haphazard response (unpredictable and incomplete) on security incidents
- Unauthorised data disclosure and leakage.

Maintaining Ownership & Control of Your Data



Unless you know who can do what with your data,
how do you manage risk and maintain control?



-Dave Cullinane

Chairman, Cloud Security Alliance
former Chief Security Officer, eBay

Ownership & Control Requirements

Data Security

- Security Breaches
- Hackers
- Rogue Employees
- Data co-mingling
- Separation of Controls

Data Disclosure

- Court Order/ Subpoena
- Blind Subpoena or Gag Order

Compliance

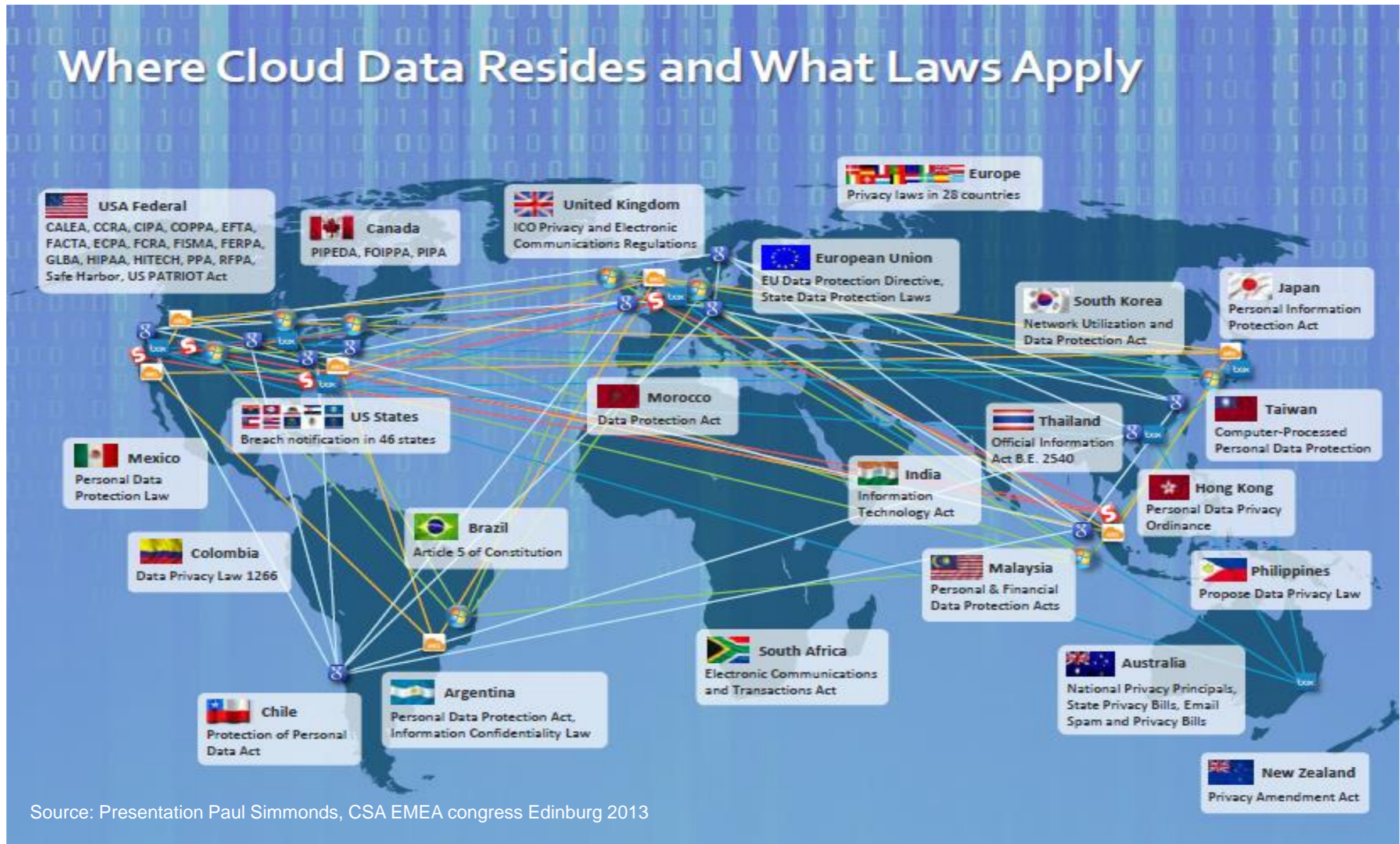
- Encryption is part of:
HIPAA, NEN7510, GLBA, PCI-DSS, WBP
- Independence in managing requests

Data Residency

- EU Safe Harbor vs. Patriot Act
- Foreign jurisdiction and disclosure
- Privacy laws

Source: Vaultive

Legislation and regulations



Compliance: Cannot Be Assigned

- Compliance responsibility stays with end-user
- Encryption for data at rest requirements still apply for cloud data
- Cannot transfer risk to cloud providers
- Cloud Service Providers provide a subset of compliance coverage
- ❖ ***"Customers are responsible for being the steward of their own data."***
(source: Microsoft Dynamics CRM Online Security Response)
- ❖ ***"Customers are responsible for configuring Box in a HIPAA compliant manner and for enforcing policies in their organizations to achieve HIPAA compliance."*** (source: Box HIPAA and HITECH Overview and FAQs)

Source: Vaultive

Compliance: PCI DSS Cloud Guidance

Principles:

- Understand scope in terms of roles and responsibilities
- CSP only responsible for subset of PCI DSS requirements
- Shared responsibility model does not mean no responsibility for end user

End User Ownership and Control Guidance:

- Strong data encryption for cloud data
- Separation of controls for key management
- **Maintain encryption and key management on-premise**



Unauthorized Disclosure

On-Premise Email / Data



Cloud Email / Data



With persistent encryption: Cloud Email / Data



**Cloud Provider's Responsibility:
Securing the cloud platform**

**End-User's Responsibility:
Controlling its data**

Cloud Roles and Responsibilities

Cloud Service Provider

Hosting &
Processing

Security

End-User Organization

Ownership

Control

Practical Steps To Maintain Control



Cloud Control Matrix 3.0, Oct 2013

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

- Select a Cloud Service Provider that adheres to CCM
- Encrypt data **before it leaves** the end-user organization's control
- Encrypt data at rest, data in transit and **data in use**
- Encryption keys should **be retained by the end-user organization**, not the Cloud Service Provider

Encryption & Key Management Storage and Access

EKM-04 Strong encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. **Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.**

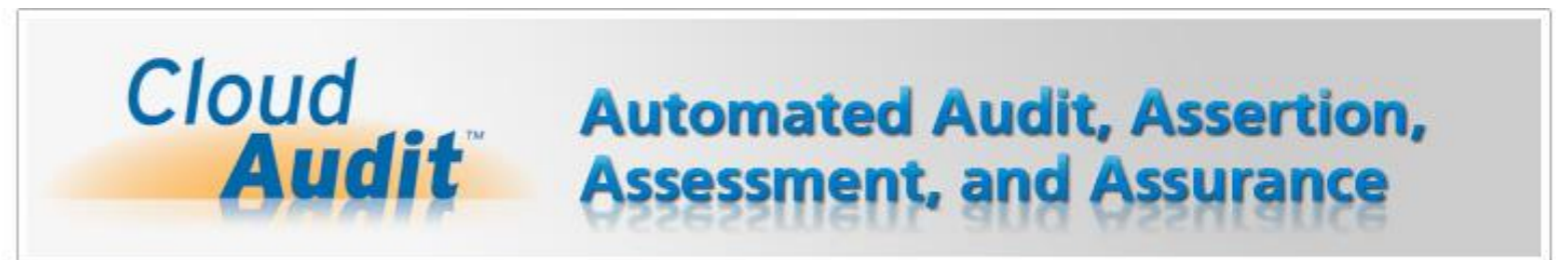


The Answer from Cloud Security Alliance

Cloud Security Alliance and resilience

- Through transparency with regard to the security levels and measures of a Cloud Services Provider a customer can achieve the assurance that it is well arranged, guaranteed and maintained.
- Only through a common framework with control elements that provide clarity it can be clear to a customer.

View by the CSA



Some CSA products...

View by the CSA



CSA Security Guidance for Critical Areas
of Cloud Computing Version 3.0



CCSKTM
Certificate of
Cloud Security Knowledge



CCMTM Security Controls Framework
For Cloud Providers & Consumers
Cloud Controls Matrix



CTPTM Promoting Elements of
Transparency in the Cloud



Cloud AuditTM Automated Audit, Assertion,
Assessment, and Assurance



Cloud CERTTM Computer Emergency
Response Team

Some CSA products...



Security Controls Framework
For Cloud Providers & Consumers



CCM V 3.0: Cloud Control Matrix

Cloud Controls Matrix (v3.0)



- Objectives (controls) derived from guidance
- Mapped against known standards such as ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP
- Apply on (..)aaS
- Suppliers vs client role
- Helps reducing the bridge between IT staff and auditors
- Assists in defining appropriate SLA

Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

1	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability	
				SaaS	PaaS	IaaS	Service Provider	Customer
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X	
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X
62	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X	

CSA Controls Matrix (CM) v2.0 / Compliance Mapping Reference

CCM and other standards

Mapped against:

- COBIT 4.1
- HIPAA/ HITECH Act
- ISO/IEC 27001:2005
- NIST Special publication SP 800-53 (rev 3)
- FedRAMP
- PCI DSS v 2.0
- BITS shared Assessments
- GAPP
- Jericho Forum
- NERC CIP
- AICPA Trust Services Principles & Criteria (TSP)

In next versions more mappings against standards...

CCM v 3.0 – 16 Control domains

Control domains	CCM V3.0
1. Application and Interface Security	9. Human Resource Security (HRS)
2. Audit, Assurance and Compliance	10. Identity and Access Management
3. Business Continuity and Management Resilience	11. Interoperability and Portability
4. Change Control and Configuration Management	12. Infrastructure and Virtualization Security
5. Data Center Security	13. Mobile Security
6. Data Security & Information Lifecycle Management	14. Security Incident Management – e-Discovery Cloud Forensics
7. Encryption and Key Management	15. Supply Chain management, Transparency and Accountability
8. Governance and Risk Management	16. Threat and Vulnerability management

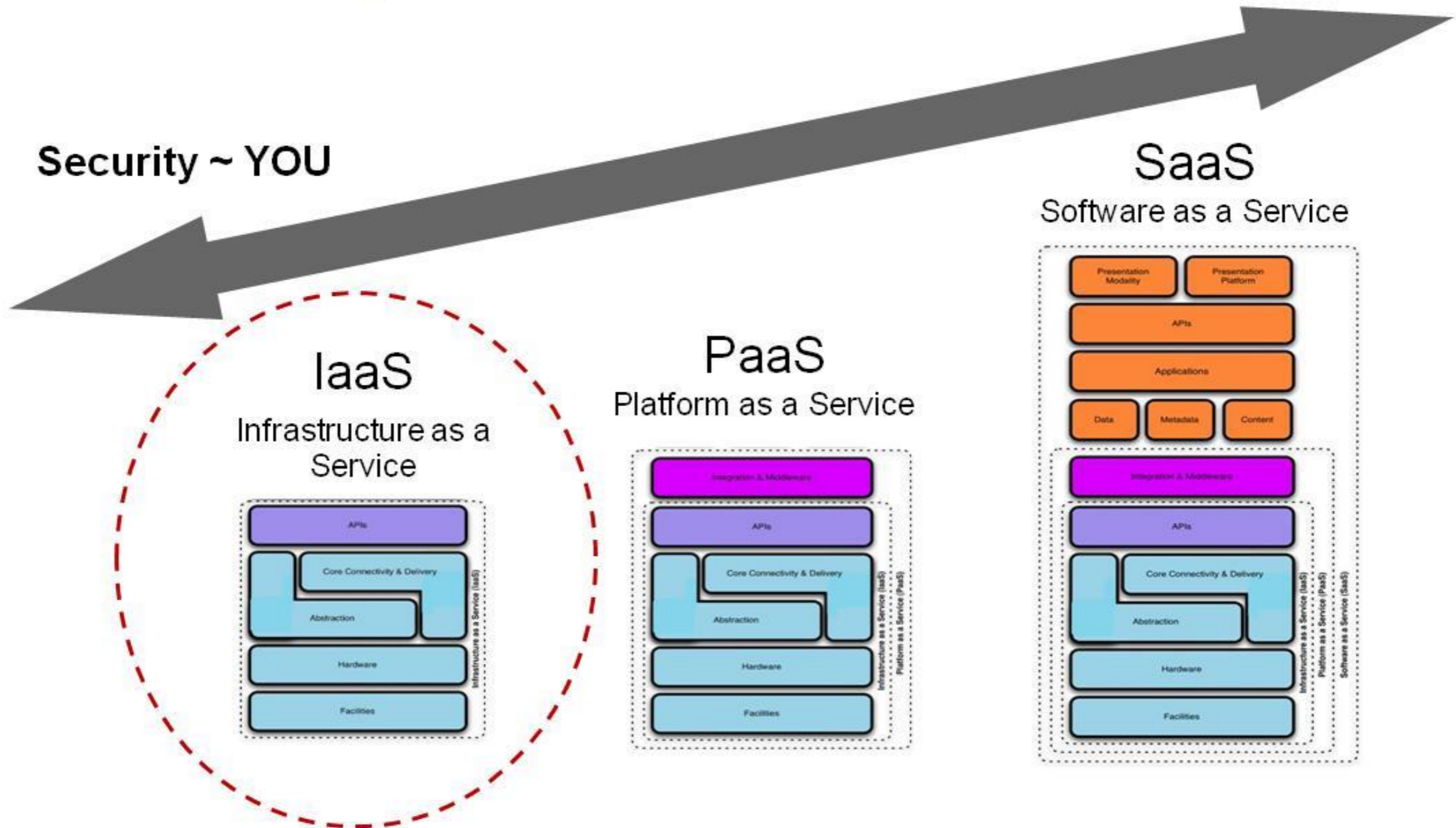
CCM V3: 45 additional new controls on top of ISO27001:2005

Who arranges security?

Role Clarity

Security ~ THEM

Security ~ YOU



CSA CCM Control ownership

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

CCM role supplier and client [1]



CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship	
			Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer
Application & Interface Security <i>Application Security</i>	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.		X	X	X	X	X		X	X	X	X	
Application & Interface Security <i>Customer Access Requirements</i>	AIS-02	Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.	X	X	X	X	X	X	X	X	X	X	X	X
Application & Interface Security <i>Data Integrity</i>	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.		X	X	X	X	X		X	X	X	X	X
Application & Interface Security <i>Data Security / Integrity</i>	AIS-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure, alteration, or destruction. These policies, procedures, processes, and measures shall be in accordance with known legal, statutory and regulatory compliance obligations.		X	X	X	X	X	X	X	X	X	X	X
Audit Assurance & Compliance <i>Audit Planning</i>	AAC-01	Audit plans, activities, and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	X	X	X	X	X	X	X	X	X	X	X	X
Audit Assurance & Compliance	AAC-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to	X	X	X	X	X	X	X	X	X	X	X	X

CCM role supplier and client [2]

Control Domain	CCM V3.0 Control ID	Control Specification	Supplier Relationship	
			Service Provider	Tenant / Consumer
Application & Interface Security <i>Application Security</i>	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	X	
Application & Interface Security <i>Customer Access Requirements</i>	AIS-02	Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.	X	X
Application & Interface Security <i>Data Integrity</i>	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.	X	X

Certification for cloud services

- In the Agenda of the EC
- Requested from Art29 WP as a measure for privacy compliance
- Already part of the cloud strategy in countries such USA, Singapore, Thailand, China, Honk Kong, Taiwan,
- In Europe various Member States are looking at a certification/accreditation schema for cloud service (especially in Public Procurement)
- The UK G-Cloud is based on a logic of companies accredited to offer service in the App Store

Principles

- **Comparability** - results should be repeatable, quantifiable and comparable across different certification targets.
- **Scalability** - the scheme can be applied to large and small organisations.
- **Proportionality (risk based)** - evaluation takes into account risk of occurrence of threats for which controls are implemented.
- **Composability/modularity** - addresses the issue of composition of cloud services including dependencies and inheritance/reusability of certifications.
- **Technology neutrality:** allows innovative or alternative security measures.
- **Transparency** of the overall auditing process.

Requirements

- Provide a globally relevant certification to reduce duplication of efforts
- Address localized, national-state and regional compliance needs
- Address industry specific requirements
- Address different assurance requirements
- Address “certification staleness” – assure provider is still secure after “point in time” certification
- User-centric
- Voluntary, business driven
- Leverage global standards/schemes
- Do all of the above while recognizing the dynamic and fast-changing world that is cloud

Objectives

- To improve customer trust in cloud services
- To improve security of cloud services
- To increase the efficiency of cloud service procurement
- To make it easier for cloud providers and customers to achieve compliance
- To provide greater transparency to customers about provider security practices
- To achieve all the above objectives as cost-effectively as possible

The Answer from Cloud Security Alliance

CSA STAR:

Security, Trust & Assurance Registry

➤ Launched in 2011, the CSA STAR is the first step in **improving transparency and assurance** in the cloud.



➤ The STAR is a **publicly accessible** registry that documents the security controls provided by cloud computing offerings

➤ Helps users to assess the security of cloud providers

➤ Searchable registry to allow cloud customers to review the security practices of providers, accelerating their due diligence and leading to **higher quality procurement experiences.**

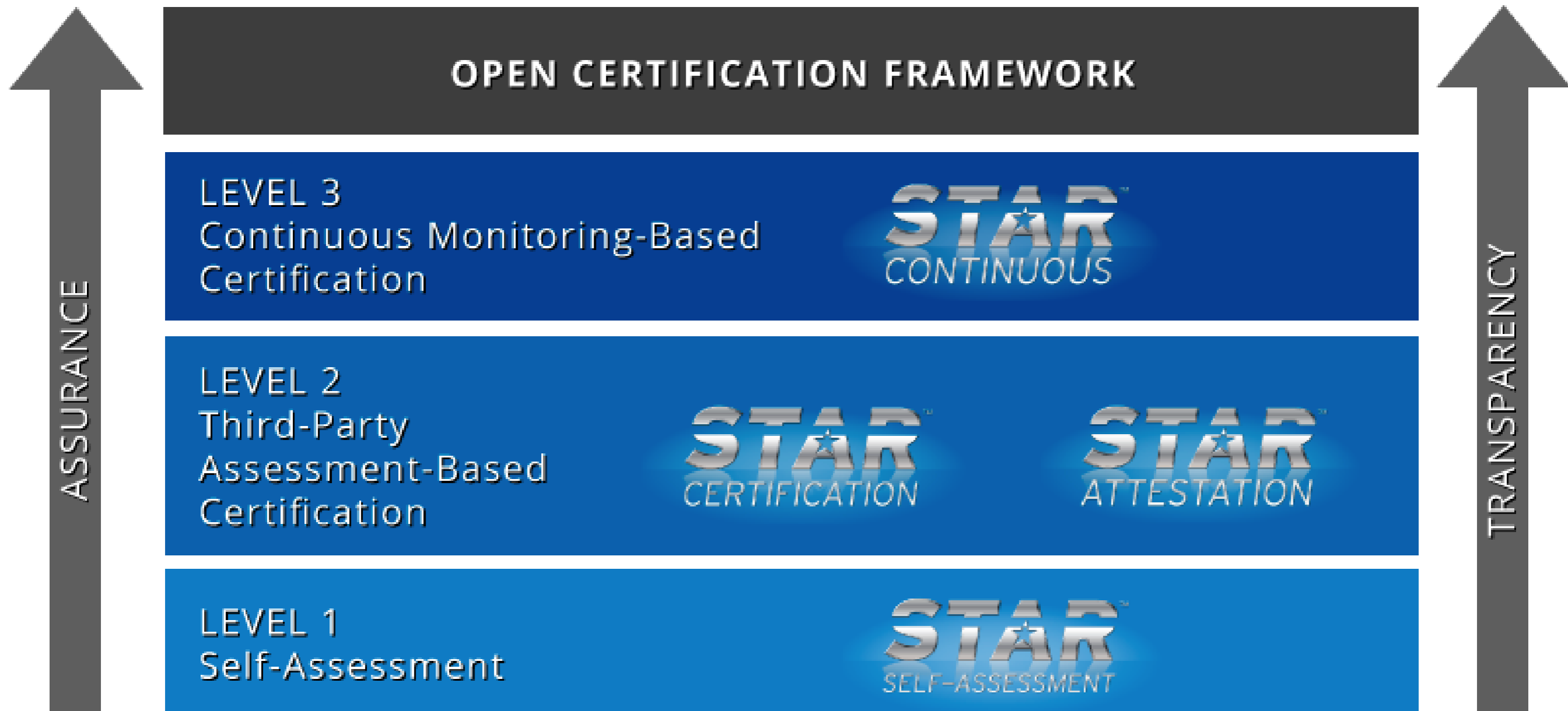
➤ It is based on a multilayered structure defined by **Open Certification Framework Working Group**

OCF: VISION STATEMENT

- The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
- The CSA Open Certification Framework is a program for flexible, incremental and multi-layered cloud provider certification according to the Cloud Security Alliance's industry leading security guidance and control objectives.
- The program will integrate with popular third-party assessment and attestation statements developed within the public accounting community to avoid duplication of effort and cost.

~Jim Reavis & Daniele Catteddu; CSA~

The OCF structure



The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

OCF Level 1



- Self Assessments based on Consensus Assessments Initiative Questionnaire and Cloud Control Matrix
- Voluntary industry action promoting transparency
- Open to ALL cloud providers
- Since the initial launch at the end of had tremendous growth
- 37 entries: including Amazon Web Services, Box.com, HP, Microsoft, Ping Identity, Red Hat, Skyhigh Networks, Symantec, TerreMark and many others

OCF Level 2

STANTM
STAR
CERTIFICATION

STANTM
STAR
ATTESTATION

OCF Level 2



- The STAR Attestation is positioned as STAR Certification at Level 2 of the Open Certification Framework and it is likewise STAR Certification is third party independent assessment of the security of a cloud service provider.
- Based on type 2 SOC attestations supplemented by the criteria in the Cloud Controls Matrix (CCM).
- Provides for robust reporting on the service provider's description of its system, and on the service provider's controls, including a description of the service auditor's tests of controls in a format very similar to the now obsolete SAS 70 reporting format, and current SSAE 16 (SOC 1) reporting, thereby facilitating market acceptance

OCF Level 3



- CSA STAR Continuous will be based on a continuous auditing/assessment of relevant security properties.
- It will be built on the following CSA best practices/standards:
 - Cloud Control Matrix (CCM)
 - Cloud Trust Protocol (CTP)
 - CloudAudit (A6)
- CSA STAR Continuous is currently under development and the target date of delivery is 2015.

What is CSA STAR Certification? 1

- The CSA STAR Certification is a **rigorous third party independent assessment** of the security of a cloud service provider.
- Technology-**neutral** certification leverages the requirements of the **ISO/IEC 27001:2005** & the **CSA CCM**
- Integrates ISO/IEC 27001:2005 with the CSA CCM as **additional or compensating controls**.
- **Measures the capability levels** of the cloud service.
- It assigns a '**Management Capability**' score to each of the CCM security domains.

What is CSA STAR Certification? 2

- Evaluates the efficiency of an organization's ISMS and ensures the scope, processes and objectives are "**Fit for Purpose.**"
- Help organizations **prioritize areas for improvement** and lead them towards **business excellence.**
- Enables effective **comparison** across other organizations in the applicable sector.
- Based upon the **Plan, Do, Check, Act** (PDCA) approach
- Enables the auditor to assess a company's performance, on **long-term sustainability and risks**, in addition to ensuring they are **SLA driven.**

Relation to other standards

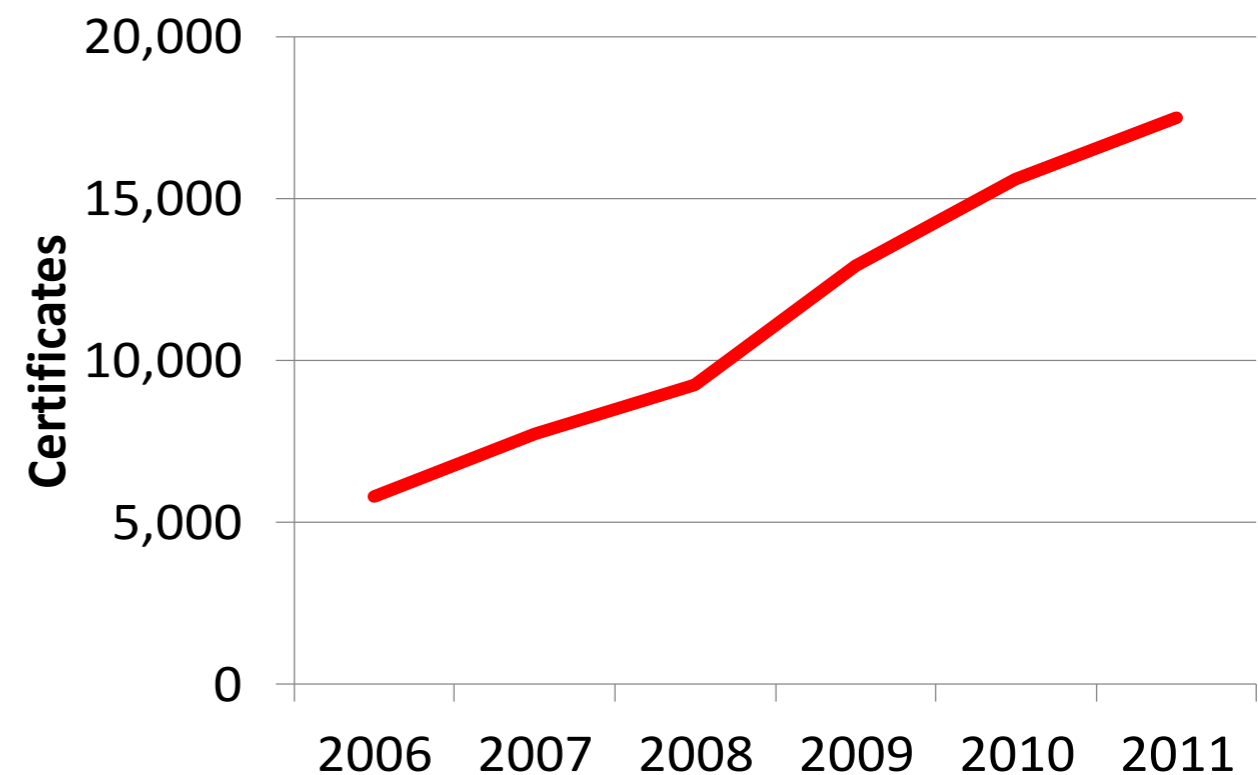
The STAR certification scheme is designed to comply with:

- **ISO/IEC 17021:2011**, Conformity assessment – Requirements for bodies providing audit and certification of management systems
- **ISO/IEC 27006:2011**, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- **ISO 19011**, Guidelines for auditing management systems

CSA STAR Certification & ISO 27001

WHY CSA STAR Certification builds on ISO27001?

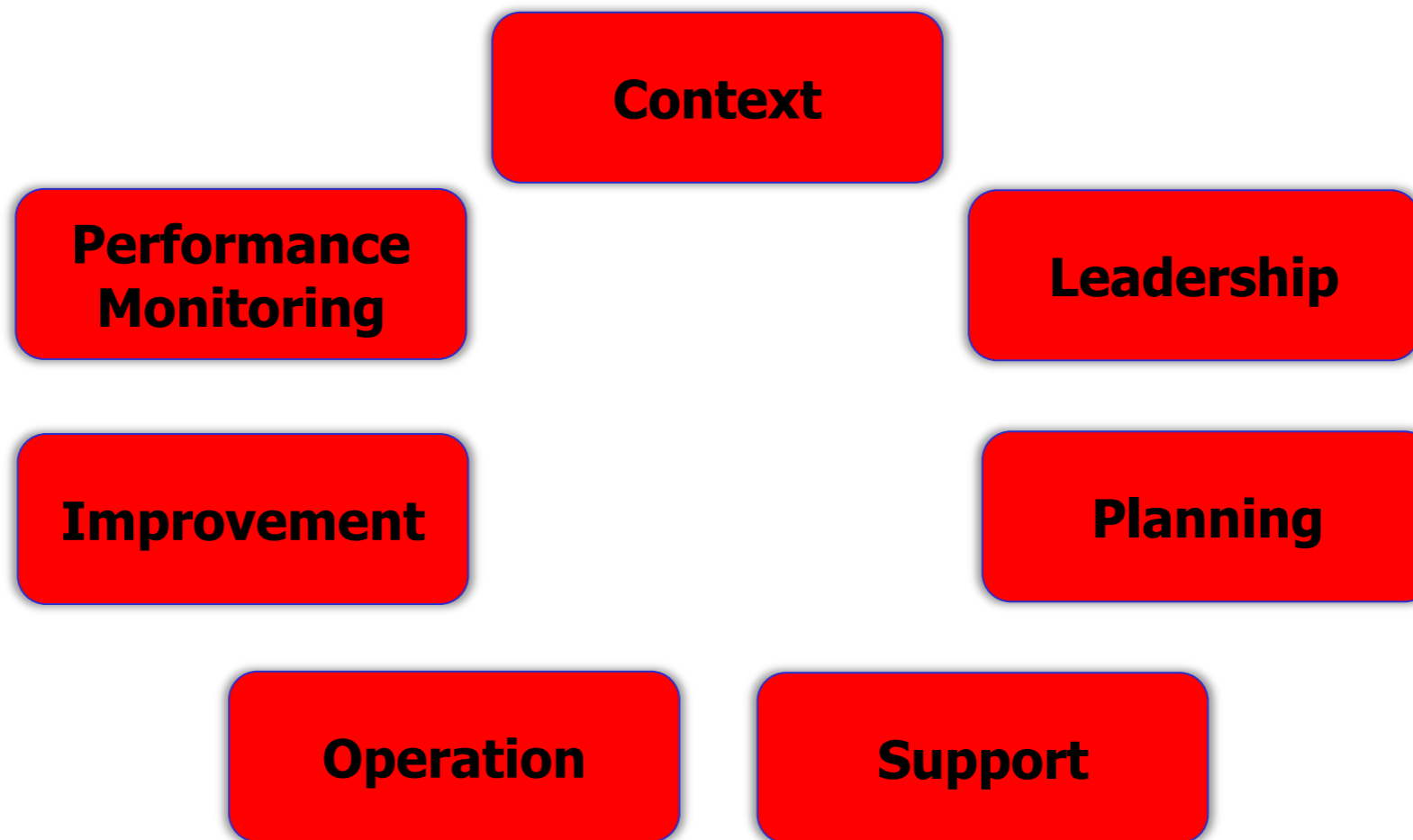
- Help organizations prioritize areas for improvement and lead them towards business excellence.
- ISO 27001 is the international standard for information security
- Considered as Gold Standard for information security
- There are over 17,500 organisations certified globally in over 120 countries.



bsi.

ISO 27001: how does it work?

- It is a management systems standard – it outlines the processes and procedures an organisation must have in place to manage Information Security issues in core areas of the business
- The standard does not stipulate exactly how the process should operate



ISO 27001: Criticisms

- ISO 27001 is updated every 8 years – the controls become obsolete faster than that
- It is a one size fits all standard but there are some industry specific concerns it does not cover, ie it is not Cloud relevant
- Any standard can become a lowest common denominator
- People can certify any scope they like within their organisation to mislead clients
- It doesn't support transparency

HOW it provides assurance to clients?

- ISO 27001 requires the organisation to evaluate their customers' requirements and expectation, and contractual requirements. It requires that they have implemented a system to achieve this.
- ISO 27001 requires the organisation has conducted a risk analysis that identifies the risks to meeting their customer's expectations.
- The Cloud Controls Matrix requires the organisation to address the specific issues that are critical to cloud security.
- The maturity model assesses how well managed activities in the control areas are.

Very important

No Certification can ever guarantee information is 100% secure however STAR certification ensures an organisation has an appropriate system for the type of information it is dealing with and that it is well managed and focused on cloud specific concerns.

THANK
YOU!

Reinier.landsman@cert2connect.com

Mob : +31(0)6 53103641