
cloud
CSA
security
alliance®

HOW STANDARDS PROLIFERATE:

(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.

SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

About the Cloud Security Alliance

- Global, not-for-profit organization
- Building security best practices for next generation IT
- Research and Educational Programs
- Cloud Provider Certification – CSA STAR
- User Certification - CCSK
- The globally authoritative source for Trust in the Cloud

"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."

OUR COMMUNITY

84,000+
INDIVIDUAL MEMBERS

75+
CHAPTERS

300+
CORPORATE MEMBERS

30+
ACTIVE WORKING GROUPS

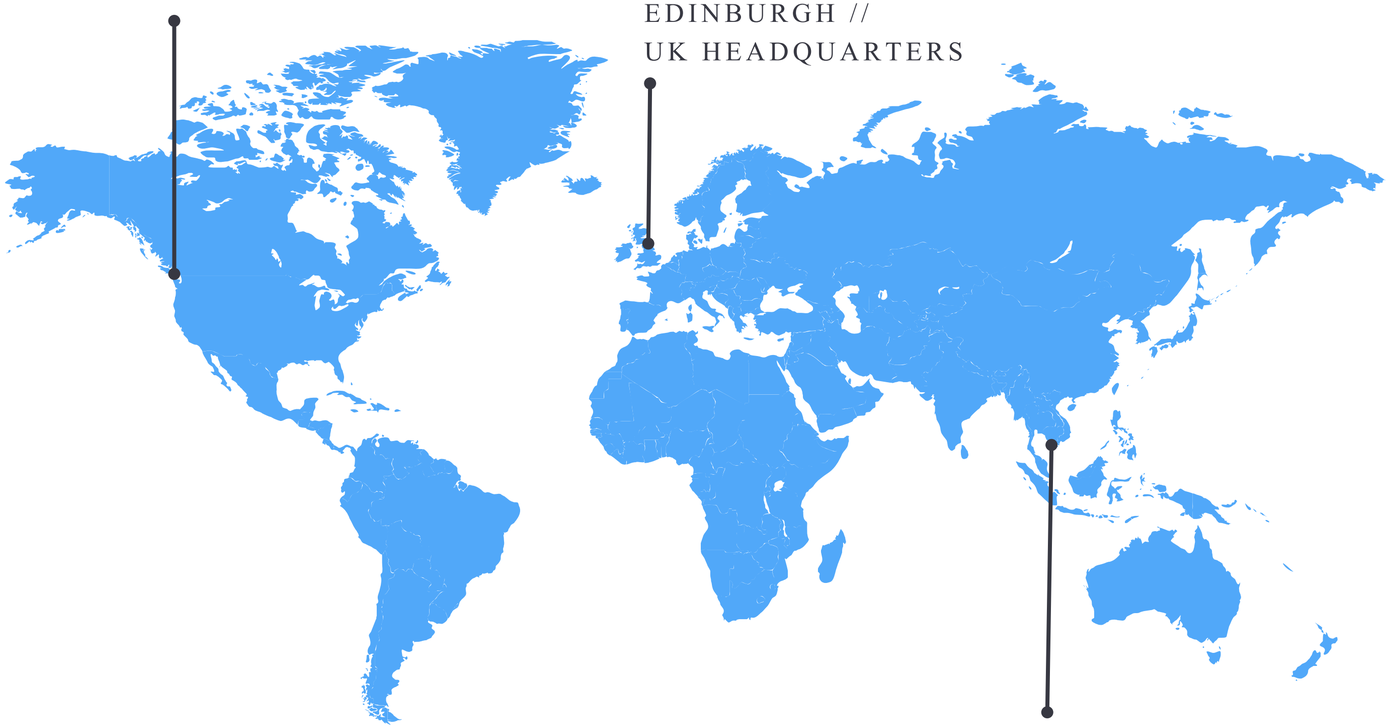
Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

2009
CSA FOUNDED

SEATTLE/BELLINGHAM, WA //
US HEADQUARTERS

EDINBURGH //
UK HEADQUARTERS



SINGAPORE //
ASIA PACIFIC
HEADQUARTERS

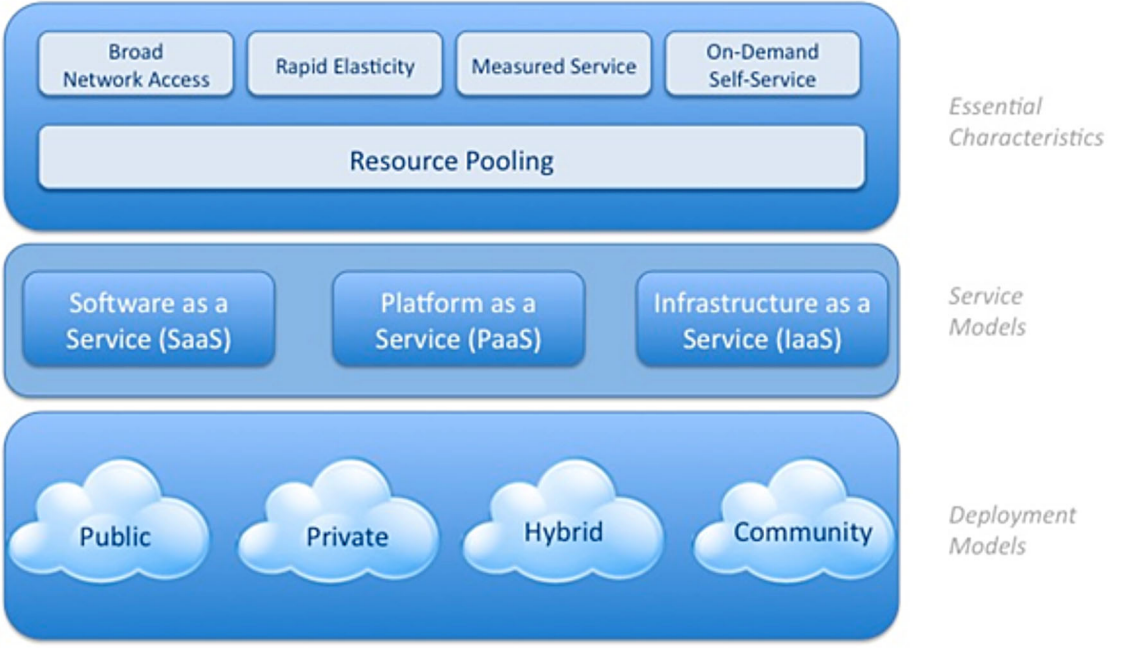
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance


Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

Trusted Cloud

Reference Architecture

Version 2.0

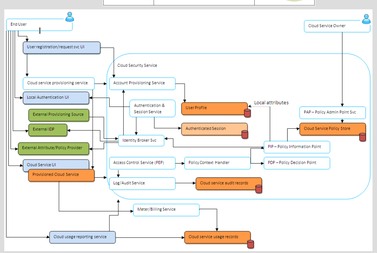
Guiding Principles

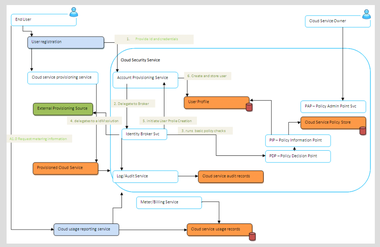
- Define protections that enable trust in the cloud.
- Develop cross-platform capabilities and patterns for proprietary and open-source providers.
- Will facilitate trusted and efficient access, administration and resiliency to the customer/consumer.
- Provide direction to secure information that is protected by regulations.
- The Architecture must facilitate proper and efficient identification, authentication, authorization, administration and auditability.
- Centralize security policy, maintenance operation and oversight functions.
- Access to information must be secure yet still easy to obtain.
- Delegate or Federate access control where appropriate.
- Must be easy to adopt and consume, supporting the design of security patterns
- The Architecture must be elastic, flexible and resilient supporting multi-tenant, multi-landlord platforms
- The architecture must address and support multiple levels of protection, including network, operating system, and application security needs.

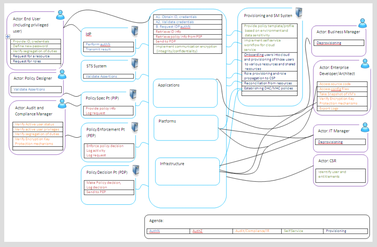
High Level Use Cases

End User to Cloud	Applications running on the cloud and accessed by end users	
Enterprise to Cloud to End User	Applications running in the public cloud and accessed by employees and customers	
Enterprise to Cloud	Cloud applications integrated with internal IT capabilities	

SaaS, PaaS, IaaS







Domain

Container

Process or Solution

Data

SABSA

ITIL v3

TOGAF

JERICHO

Business Operation Support Services (BOSS)

Compliance

- Audit Planning
- Independent Audits
- Third-Party Audits
- Internal Audits
- Contact/Authority Maintenance
- Information System Regulatory Mapping
- Intellectual Property Protection

Data Governance

- Data Ownership / Stewardship
- Data Classification
- Handling / Labeling / Security Policy
- Secure Disposal of Data
- Clear Desk Policy
- Rules for Information Leakage Prevention
- Rules for Data Retention

Operational Risk Management

- Operational Risk Committee
- Crisis Management
- Business Impact Analysis
- Key Risk Indicators
- Business Continuity
  - Planning
  - Testing
- Risk Management Framework
  - Business Assessment
  - Technical Assessment
- Independent Risk Management

Human Resources Security

- Employee Termination
- Employment Agreements
- Background Screening
- Job Descriptions
- Roles and Responsibilities
- Employee Awareness
- Employee Code of Conduct

Security Monitoring Services

- SIEM Platform
- Event Mining
- Database Monitoring
- Application Monitoring
- Honey Pot
- End-Point Monitoring
- Event Correlation
- Cloud Monitoring
- E-Mail Journaling
- Market Threat Intelligence
- Counter Threat Management
- SOC Portal
- Managed Security Services
- Knowledge Base
- Branding Protection
- Anti-Phishing
- Real-time internetwork defense (SCAP)
- User Behavior & Profile Patterns

Legal Services

- Contracts
- E-Discovery
- Incident Response Legal Preparation

Internal Investigations

- Forensic Analysis
- e-Mail Journaling

Information Technology Operation & Support (ITOS)

IT Operation

DRP

- Plan Management
- Test Management

IT Governance

- Architecture Governance
- Standards and Guidelines

Resource Management

- Segregation of Duties
- Contractors

PMO

- Program Mgmnt
- Project Mgmnt
- Remediation

Portfolio Management

- Maturity Model
- Roadmap
- Strategy Alignment

Service Delivery

Service Level Management

- Objectives
- Internal SLAs
- OLAs
- External SLAs
- Vendor Management
- Service Dashboard

Information Technology Resiliency

- Availability Management
- Resiliency Analysis
- Capacity Planning

Asset Management

- Service Costing
- Operational Budgeting
- Charge Back
- Investment Budgeting

Application Performance Monitoring

Service Support

Configuration Management

- Capacity Planning
- Software Management
- Physical Inventory
- Automated Asset Discovery
- Configuration Management

Incident Management

- Security Incident Response
- Automated Ticketing
- Self-Service
- Ticketing
- Cross Cloud Security Incident Response

Problem Management

- Event Classifiation
- Root Cause Analysis
- Trend Analysis
- Problem Resolution
- Orphan Incident Management

Knowledge Management

- Best practices
- Trend Analysis
- Benchmarking
- Security Job Aids
- Security FAQ

Change Management

- Service Provisioning
- Approval Workflow
- Change Review Board
- Planned Changes
  - Project Changes
  - Operational Chages
- Emergency Changes

Release Management

- Scheduling
- Testing
- Version Control
- Build
- Source Code Management

Presentation Services

Presentation Modality

Consumer Service Platform

- Social Media
- Colaboration
- Search
- E-Mail
- e-Readers

Enterprise Service Platform

- B2E
- B2M
- B2B
- B2C
- P2P

Presentation Platform

End-Points

- Mobile Devices
  - Mobile Device Management
- Portable Devices
- Fixed Devices
- Desktops
  - Company owned
  - Third-Party
  - Public Kiosk
- Medical Devices
- Smart Appliances
- Secure Sandbox

- Speech Recognition (IVR)
- Handwriting (ICR)

Application Services

Programming Interfaces

- Input Validation

Security Knowledge Lifecycle

- Security Design Patterns
- Attack Patterns
- Code Samples
- Security Application Framwrok - ACEGI

Integration Middleware

Development Process

Self-Service

- Security Code Review
- Application Vulnerability Scanning
- Stress and Volume Testing

Software Quality Assurance

Connectivity & Delivery

Abstraction

Information Services

Service Delivery

- Service Catalog
- SLAs
- OLAs
- Contracts
- Recovery Plans

Reporting Services

- Dashboard
- Data Mining
- Reporting Tools
- Business Intelligence

ITOS

- PMO
- Strategy
- Roadmap
- Problem Management
- Incident Management
- CMDB
- Knowledge Management
- Service Management
- Change Management

BOSS

- Risk Assessments
- Data Classification
- Process Ownership
- Audit Findings
- HR Data (Employees & Contractors)
- Business Strategy

Service Support

- Configuration Rules (Metadata)
- Service Events
- Knowledge Repository
- Configuration Management Database (CMDB)
- Change Logs

Data Governance

- Risk Assessments
- Non-Production Data
- Information Leakage Metadata
- Data Segregation

Risk Management

- GRC
- RA
- BIA
- DR & BC Plans
- VRA
- TVM

Security Monitoring

- Session Events
- Authorization Events
- Authentication Events
- Application Events
- Network Events
- Computer Events
- HIPS
- Transformation Services
- NIPS Events
- Privilege Usage Events
- Database Events
- ACLs
- CRLs
- Compliance Monitoring
- NIPS Events
- DLP EVents
- eDiscovery Events

User Directory Services

- Active Directory Services
- LDAP Repositories
- X.500 Repositories
- DBMS Repositories
- Meta Directory Services
- Registry Services
- Location Services
- Federated Services
- Virtual Directory Services

Infrastructure Services

Internal Infrastructure

Facility Security

- Controlled Physical Access
  - Barriers
  - Electronic Surveillance
  - Security Patrols
  - Physical Authentication
- Asset Handling
  - Data
  - Hardware
  - Software
- Environmental Risk Management
  - Physical Security
  - Equipment Location
  - Power Redundancy

Patch Management

- Compliance Monitoring
- Service Discovery

Servers

- Secure Build
- Image Management

Storage Services

Network Services

- Network Segmentation
- Authoritative Time Source

Equipment Maintenance

Availability Services

End Point

Virtual Infrastructure

Desktop "Client" Virtualization

- Local
- Remote
  - Session-Based
  - VM-Based (VDI)

Storage Virtualization

- Block-Based Virtualization
  - Host-Based
    - LDM
    - LVM
    - LUN
  - Storage Device-Based
  - Network-Based
    - Appliance
    - Switched
- File-Based Virtualization

Application Virtualization

- Client Application Streaming
- Server Application Streaming

Virtual Workspaces

- Vertical Isolation

Server Virtualization

Virtual Machines (Hosted Based)

- Full
- Paravirtualization
- Hardware-Assisted
- OS Virtualization
- TPM Virtualization
- Virtual Memory

Network

- Network Address Space
  - IPv4
  - IPv6
- External (VLAN)
- Internal (VNIC)

- Database Virtualization
- Mobile Device Virtualization
- Smartcard Virtualization

Security and Risk Management

Governance Risk & Compliance

- Compliance Management
- Policy Management
  - Exceptions
  - Self Assessment
- Vendor Management
- Audit Management
- IT Risk Management
- Technical Awareness and Training

InfoSec Management

- Capability Mapping
- Risk Portfolio Management
- Risk Dashboard
- Residual Risk Management

Privilege Management Infrastructure

Identity Management

- Domain Unique Identifier
- Federated IDM
- Identity Provisioning
- Attribute Provisioning

Authentication Services

- SAML Token
- Risk Based Auth
- Multifactor
- OTP
- Smart Card
- Password Management
- Biometrics
- Network Authentication
- Single Sign On
- Middleware Authentication
- WS-Security
- Identity Verification
- OTB AutN

Authorization Services

- Entitlement Review
- Policy Enforcement
- Policy Definition
- Policy Management
- Principal Data Management
- Resource Data Management
- XACML
- Role Management
- Obligation
- Out of the Box (OTB) AutZ

Privilege Usage Management

- Keystroke/Session Logging
- Password Vaulting
- Privilege Usage Gateway
- Resource Protection
- Hypervisor Governance and Compliance

Threat and Vulnerability Management

Compliance Testing

- Databases
- Servers
- Network

Vulnerability Management

- Application
- Infrastructure
- DB

Penetration Testing

- Internal
- External

Threat Management

- Source Code Scanning
- Risk Taxonomy

Infrastructure Protection Services

Server

- Behavioral Malware Prevention
- White Listing
- Sensitive File Protection
- Anti-Virus
- HIPS / HIDS
- Host Firewall

End-Point

- Anti-Virus, Anti-Spam, Anti-Malware
- HIPS /HIDS
- Host Firewall
- Media Lockdown
- Hardware Based Trusted Assets
- Behavioral Malware Prevention
- Inventory Control
- Content Filtering
- Forensic Tools
- White Listing

Network

- Behavioral Malware Prevention
- Firewall
- Content Filtering
- DPI
- NIPS / NIDS
- Wireless Protection
- Link Layer Network Security
- Black Listing Filtering

Application

- XML Applicance
- Application Firewall
- Real Time Filtering
- Secure Messaging
- Secure Collaboration

Data Protection

Data lifecycle management

- Meta Data Control
- Data De-Identification
- Data Masking
- Data Tagging
- eSignature (Unstructured data)
- Life cycle management
- Data Obscuring
- Data Seeding

Data Loss Prevention

- Data Discovery
- Network (Data in Transit)
- End-Point (Data in Use)
- Server (Data at Rest)

Intellectual Property Protection

- Intellectual Property
- Digital Rights Management

Cryptographic Services

- Key Management
  - Symmetric Keys
  - Asymmetric Keys
- PKI
- Signature Services
- Data-in-use Encryption (Memory)
- Data-in-Transit Encryption (Transitory, Fixed)
- Data-at-Rest Encryption (DB, File, SAN, Desktop, Mobile)

Policies and Standards

- Operational Security Baselines
- Job Aid Guidelines
- Role Based Awareness
- Information Security Policies
- Technical Security Standards
- Data/Asset Classification
- Best Practices & Regulatory correlation

cloud security alliance SM

Co-Chairs: Jairo Orea, Yaron Levi, Dan Logan.
Team: Richard Austin, Frank Simorjay, Yaron Levi, Jon-Michael Brook, Jarrod Stenberg, Ken Trant, Earle Humphreys, Vern Williams

Date: 02/25/2013

Key Research Areas

- Financial Services Stakeholder Platform
- Guidance V4
- Global Enterprise Advisory Board
- Software Defined Perimeter
- CCM/CAIQ/CTP/CloudAudit
- Security as a Service
- Internet of Things
- Quantum-Safe Computing
- CASB enablement: OpenAPI
- International Standardization Council
- Other
- *It is all free!*
  - https://cloudsecurityalliance.org/research

Findings of first “State of Cloud Security” report

- Good and Bad: cloud provider security is uneven
- Better alignment between providers and enterprises needed
- Need provider collaboration and transparency

- Global regulatory issues
- Major industry skills gap
- Cloud is changing nature of information security
- https://cloudsecurityalliance.org/download/state-of-cloud-security-2016/

CSA Top Threats to Cloud for 2016

1. Data Breaches
2. Compromised Credentials and IAM
3. Insecure APIs
4. System and App Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. APTs
8. Data Loss
9. Due Diligence
10. Nefarious Use and Abuse
11. Denial of Service
12. Shared Technology Issues

Top Threats™ To Cloud Computing

https://cloudsecurityalliance.org/group/top-threats/

THE TREACHEROUS 12

Top Threats to Cloud Computing + Industry Insights

CSA MEMBER 1

TOTAL ENTERPRISES DEFENDED: 87,268

cloud security alliance®

cloud security alliance℠

SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

SECURITY GUIDANCE

For Critical Areas of Focus In Cloud Computing v4.0

cloud security alliance®

Structural Changes to the Guidance

Major structural changes to the *Guidance* include the following:

- Removal of "*An editorial note on risk*." Risk management is instead addressed more deeply in the appropriate domains and through other CSA GRC projects.
- A new "Regional Examples" section was added to **DOMAIN 3** to provided a global perspective on legal frameworks governing data protection and privacy.
- Data security and information governance are better structured. **DOMAIN 5**, *Information Governance*, covers governance issues, while all operational data security issues are moved into **DOMAIN 11**.
- **DOMAIN 6** now addresses *Management Plane Security and Business Continuity* in the cloud. It was previously *Portability and Interoperability*. Appropriate content from version 3 is integrated in other areas and the rest is depreciated.
- **DOMAIN 7** is now dedicated to *Infrastructure Security*. In version 3 of the *Guidance*, **DOMAIN 7** was *Traditional Security, Business Continuity, and Disaster Recovery*. Relevant content is incorporated in the other appropriate domains, and non-cloud security guidance is depreciated in version 4.
- **DOMAIN 8** is now *Virtualization and Containers. Data Center Operations* from version 3 is fully depreciated to focus the *Guidance* on cloud computing specific issues. CSA determined that the community is better served by existing data center security standards.
- **DOMAIN 11** has expanded from *Encryption and Key Management* to *Data Security and Encryption* to incorporate non-governance material from **DOMAIN 5** and expand additional data security options.
- **DOMAINS 10 AND 12** were extensively rewritten and restructured to remove overlapping IAM recommendations and reflect real-world practices over unused standards.
- The content of **DOMAIN 13** is now integrated into **DOMAIN 8**, *Virtualization*, and the previous **DOMAIN 14**, *Security as a Service*, is now **DOMAIN 13**.
- **DOMAIN 14** is a new domain for *Related Technologies*, including Big Data, IoT, mobile devices, and serverless. Moving forward, this domain will enable the CSA to update the *Guidance* to include emerging technologies and practices related to cloud computing that may later be incorporated into other domains.

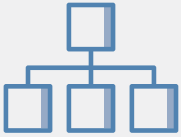
DOMAIN 1
Cloud Computing Concepts and Architectures

DOMAIN 2
Governance and Enterprise Risk Management

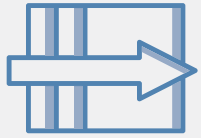
DOMAIN 3
Legal Issues, Contracts and Electronic Discovery

DOMAIN 4
Compliance and Audit Management

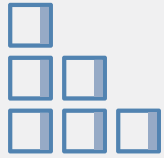
DOMAIN 5
Information Governance



DOMAIN 6
Management Plane and Business Continuity



DOMAIN 7
Infrastructure Security



DOMAIN 8
Virtualization and Containers

DOMAIN 9
Incident Response

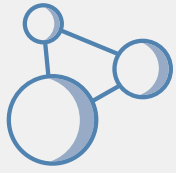
DOMAIN 10
Application Security

DOMAIN 11
Data Security and Encryption

DOMAIN 12
Identity, Entitlement, and Access Management

DOMAIN 13
Security as a Service

DOMAIN 14
Related Technologies



IMPACT OF CSA RESEARCH

CSA RESEARCH

CLOUD STANDARDS
ISC: International Standardization Council

CERTIFICATION
STAR: Security, Trust, & Assurance Registry (self-certification)
OCF: Open Certification Framework (third-party certification)

EDUCATION & TRAINING
CCSK TRAINING: Certificate of Cloud Security Knowledge

GUIDANCE & TOOLS
GRC STACK: Governance, Risk Management, and Compliance
CloudCERT: Responding to cloud vulnerabilities, threats, and incidents

DRIVING INNOVATION
Mobile, Big Data, Telecom, Innovation Initiative

GLOBAL REACH
Connecting to great minds and building a community of professionals:
- -Individuals
- -Chapters Worldwide
- -Corporations
- -Governments

LEGAL
Influencing legal, ethical, and privacy issues, and affecting change within legal perspectives

ASSESSOR/ AUDITOR
Developing globally accepted auditing controls & processes

ACADEMIA & GOVERNMENT
Creating partnerships and fostering education

TECHNOLOGY
Encouraging innovation and impacting cloud technologies

PRIVATE SECTOR
Enabling migration into the cloud

HEALTHCARE
Impacting patient care, privacy and research

CLOUD SERVICE PROVIDERS
Promoting transparency and security practices

STANDARDS DEVELOPMENT ORGANIZATIONS
Developing cloud standards

ENABLING INNOVATION
Creating markets, goods, and services

REDEFINING ROLES
Changing how we work

CREATING CULTURE
Influencing how we live

INFLUENCING CHANGE
Affecting the way we think

BUILDING ALLIANCES
Bridging the gap across nations and organizations

DEFINING TRUST
Creating assurance within the cloud

INDUSTRY IMPACT

WORKFORCE IMPACT

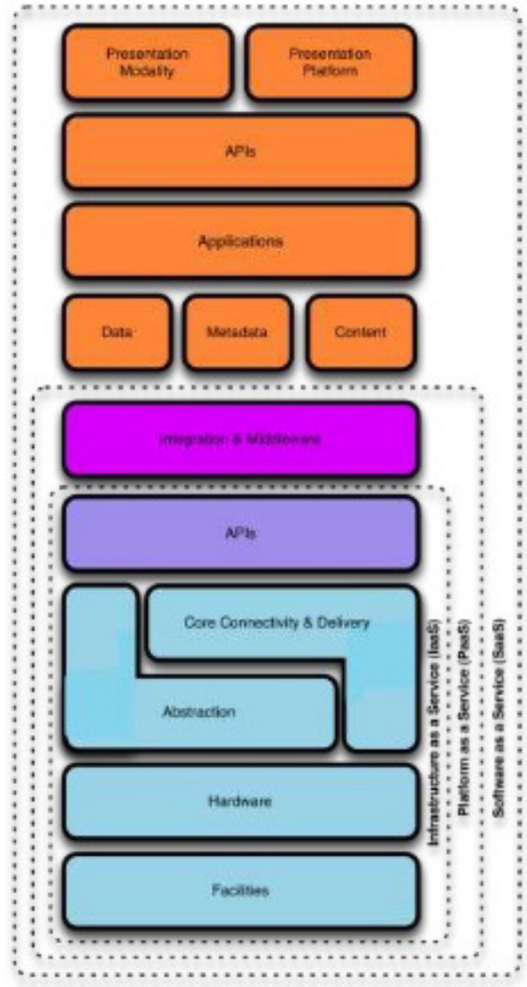
CSA®

What have leading organizations learned?

- Understanding different types of Clouds and your Role
- Due diligence is critical, Data is key
- Identity is very important
- Forcing legacy tools & architectures on cloud security problems doesn't work
- Heavy-handed blocking of cloud services backfires on infosec
- Looking for infosec capabilities delivered as a service

Different types of clouds

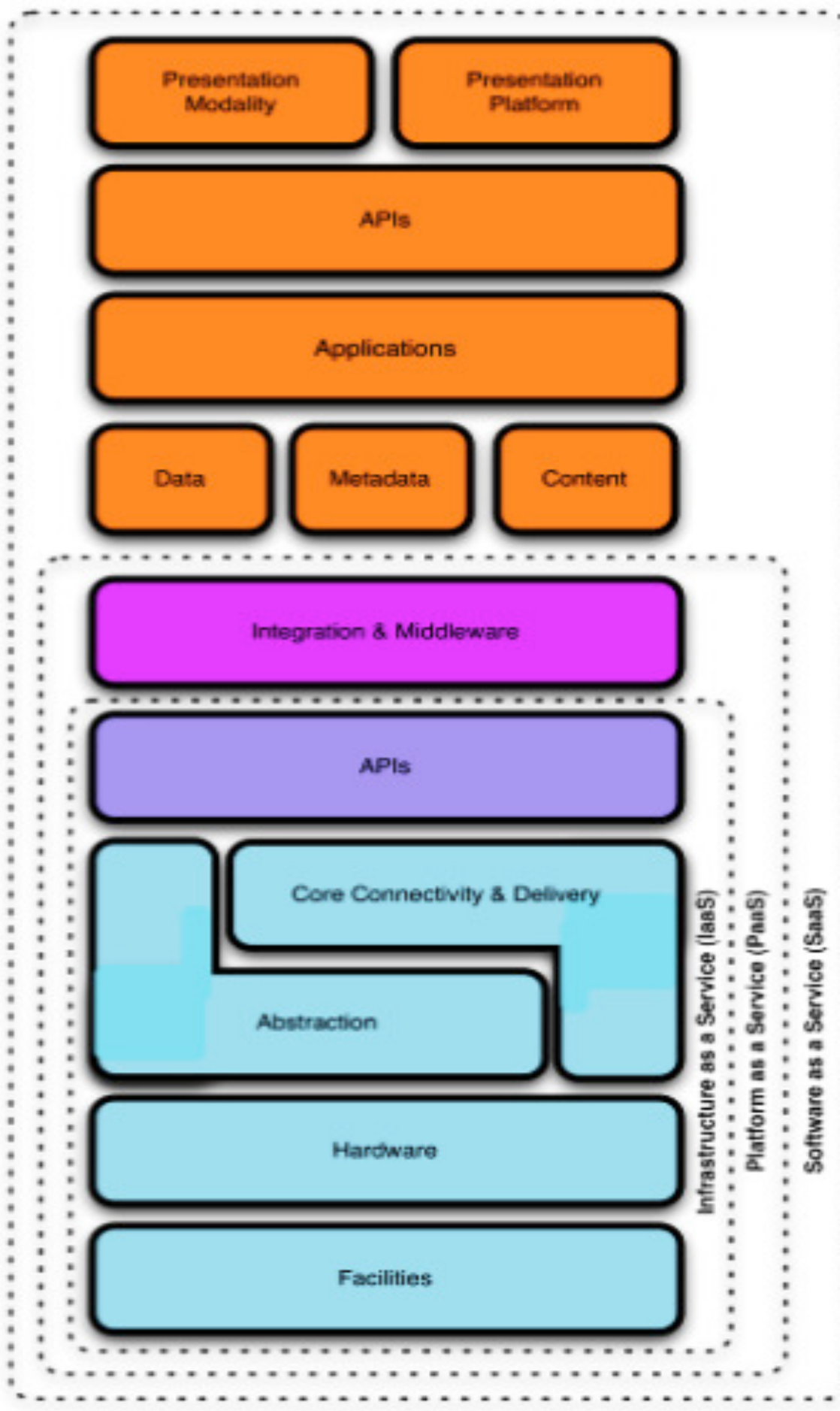
- Cloud as a layered model (eg OSI)
  - SaaS has implicit IaaS layers
- Market impacts architecture
  - Businesses occupy individual layers (e.g. cloud brokers)
  - Layers of abstraction emerge
  - Innovation/optimization in layers
- Everything becomes virtualized



CSA Cloud Reference Model

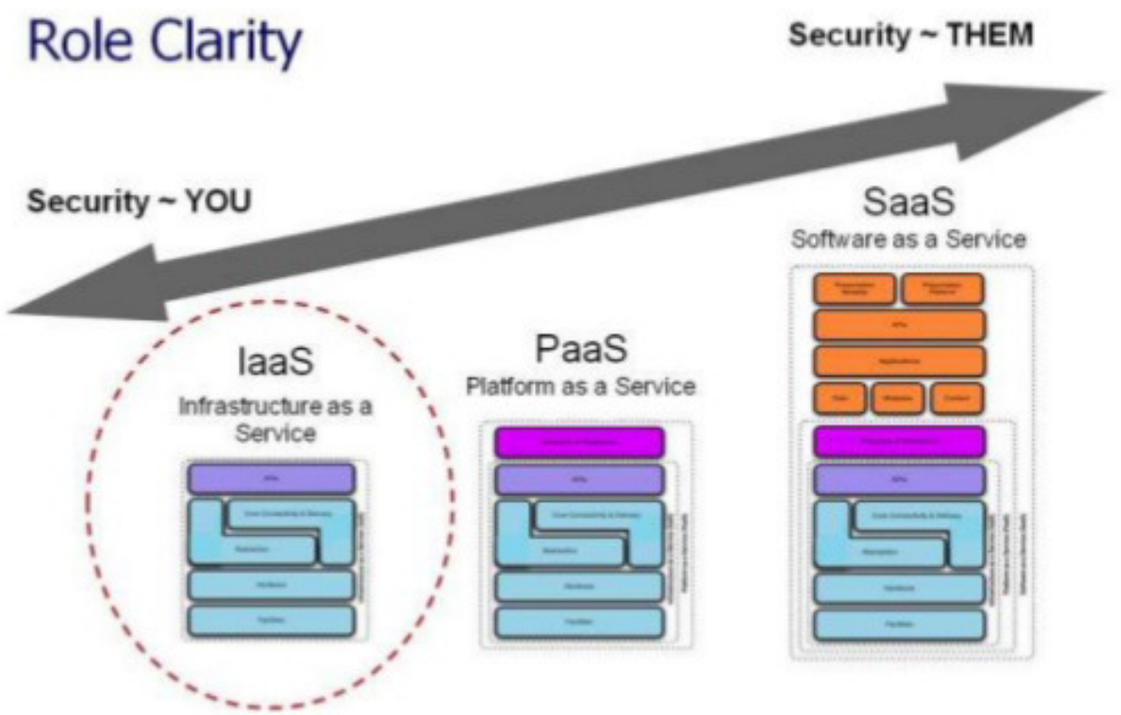
CSA's layered security framework

- SaaS layers on PaaS layers on IaaS layers
- Each layer might be a different company or discrete service
- SaaS companies that own the entire technology stack are rare
- Certifications must be aware of, and optimize the assurance of this reality



Customer role in different clouds

- In all clouds it is a shared responsibility
- IaaS is a greater responsibility for the customer to harden the service
- Provider is responsible for implementing most security in SaaS
  - Identity & data governance may still be in the tenant's realm
- Customer has the ultimate responsibility for security assurance



CUSTOMER

RESPONSIBLE FOR SECURITY *"IN"* THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)

AWS

RESPONSIBLE FOR SECURITY *"OF"* THE CLOUD

COMPUTE

STORAGE

DATABASE

NETWORKING

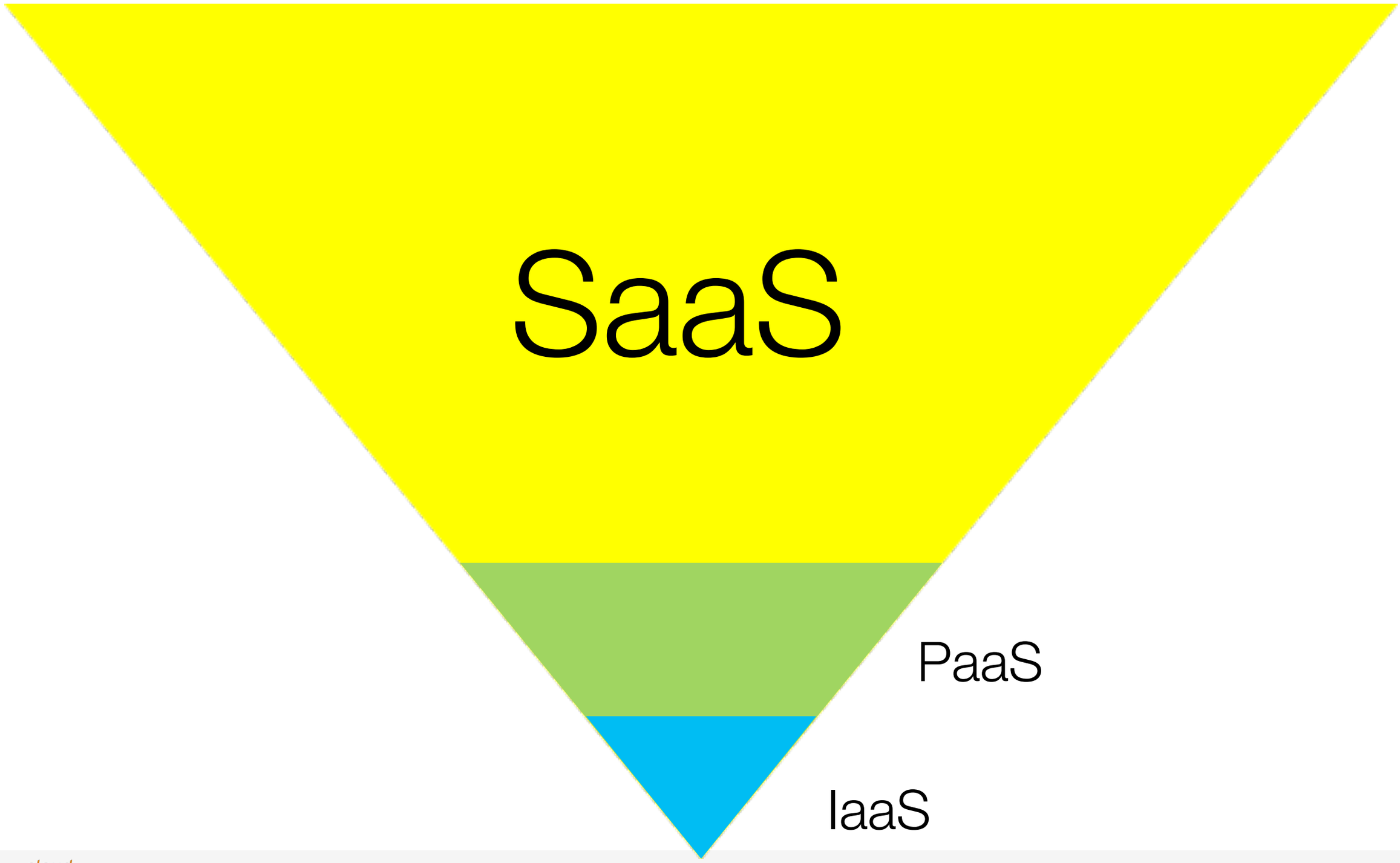
AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Cloud's upside down pyramid



Cloud Control Inheritance

CSA STAR™
Security, Trust & Assurance Registry

CCM™
Cloud Controls Matrix

CAI™

STARWATCH
Assurance on Demand

CSA's Tools for Cloud Due Diligence

- Cloud Controls Matrix (CCM)
  - Industry leading security controls framework for cloud - https://cloudsecurityalliance.org/group/cloud-controls-matrix/
- Consensus Assessment Initiative Questionnaire (CAIQ)
  - Assessment tool based on CCM - https://cloudsecurityalliance.org/group/consensus-assessments/
- CSA STAR (Security, Trust and Assurance Registry), Provider Assurance Program
  - Leverages CCM & CAIQ as its foundation - https://cloudsecurityalliance.org/star/
- CSA STARWatch
  - SaaS tool incorporating CCM/CAIQ - https://cloudsecurityalliance.org/star/

Cloud Controls Matrix (CCM)

- First ever baseline control framework specifically designed for Cloud supply chain risk management:
  - Delineates control ownership (Provider, Customer)
  - Ranks applicability to cloud provider type (SaaS vs PaaS vs IaaS)
  - An anchor for security and compliance posture measurement
  - Provides a framework of 16 control domains
- Controls map to global regulations and security standards: e.g. NIST, ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP – mappings growing virally

Cloud Controls Matrix (CCM)

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

133 CONTROLS

Cloud Controls Matrix v3.0.1

Consensus Assessment Initiative Questionnaire (CAIQ)

- Companion to CSA Cloud Controls Matrix (CCM)
- Series of Yes/No/NA questions used to assess compliance with CCM
  - Narrative may be included for each question to explain why the particular answer is given
- Helps organizations build assessment processes for cloud providers
- Helps cloud providers assess their own security posture
- Core team that originally built this were from the financial services industry

CCM & CAIQ Integration

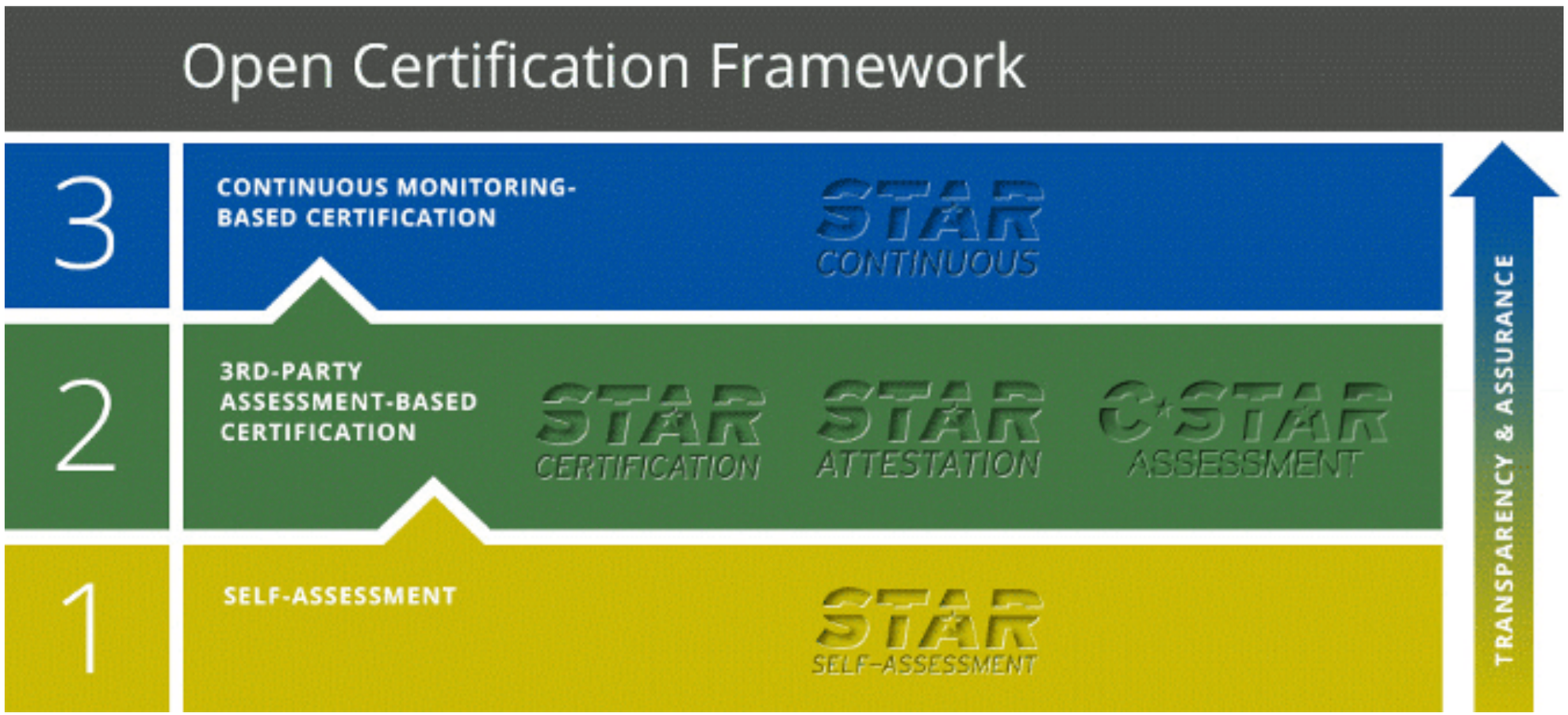
Control Group	CGID	CID	Control Specification	Consensus Assessment Questions
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?

CCM Controls Specification (using control ID BCR-07 as an example)

5 CAIQ questions that are related to this CCM control

CSA STAR Provider Program

- CSA STAR (Security, Trust and Assurance Registry), 3 Level Provider Certification Program
- Managed by CSA in partnership with world leading ISO certification bodies and audit firms
- Adopted Worldwide by Providers, Enterprises and Governments
- Promotes Transparency within Cloud Ecosystem



CSA STAR: Assisting Due Diligence

- Level 1 STAR: Self-Assessment
  - Public Registry of Cloud Provider self assessments based on either CCM or CAIQ
- Level 2 STAR 3rd Party Assessments
  - STAR Certification: Integrates ISO/IEC 27001:2013
    - CCM used to create the control scope
    - All major ISO 27001 certification bodies
  - STAR Attestation: Based upon AICPA SOC Type 2 Attestation Report
    - CCM used to create the control scope
    - Attestation provided by CPAs
- Ask for provider's STAR entry
  - If unavailable, ask provider to fill out CSA's Cloud Controls Matrix or Consensus Assessments Initiative Questionnaire

CSA STARWatch

Secure | https://star.watch/en

STARWATCH
Assurance on Demand

Registered Users, login with:

G Google | in LinkedIn | Twitter | Microsoft

Need an account? Sign up **here**.

This website uses cookies in order to establish a secure connection and provide the best browsing experience. Cookies can be removed from your browser's settings; however, our website is not able to fully function without them. By continuing to use this website, you agree to our use of cookies as documented in our Privacy Policy.

Licenses ▶ FAQ Contact Sign up About

Home

Reduce complexity and simplify workflows with CSA STARWatch

Simplify and streamline your assessment of cloud services with Cloud Security Alliance's STARWatch

Sign up today

Request a trial

You may also request a live demo to find out how STARWatch can help you assess Cloud Service Providers. Sign up today

Control applicability & inheritance

CSA_CCM_v3.0.1.xlsx - Excel — Jim Reavis

File | Home | Insert | Draw | Page Layout | Formulas | Data | Review | View | ACROBAT | Tell me what you want to do | Share

Clipboard | Font | Alignment | Number | Styles | Cells | Editing

AU105

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			S
			Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	S Pr
Encryption & Key Management Storage and Access	EKM-04	Platform and data-appropriate 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				X		X		X	X	X	
Governance and Risk Management Baseline Requirements	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at	X	X	X	X	X	X	X	X	X	X	

CSA CCM V3.0.1

Ready — 100%

Control applicability & inheritance

Clipboard | Font | Alignment | Number | Styles | Cells

A2 | Control Group

CAIQv3.0.1 **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1**

						Yes	No	Not Applicable
Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			
Application & Interface Security	AIS-01	AIS-01.3	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications)	Do you use manual source-code analysis to detect security defects in code prior to production?		Yes		
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		Yes		

CSA CAIQ v3.0.1 | Guiding Principles

Edit

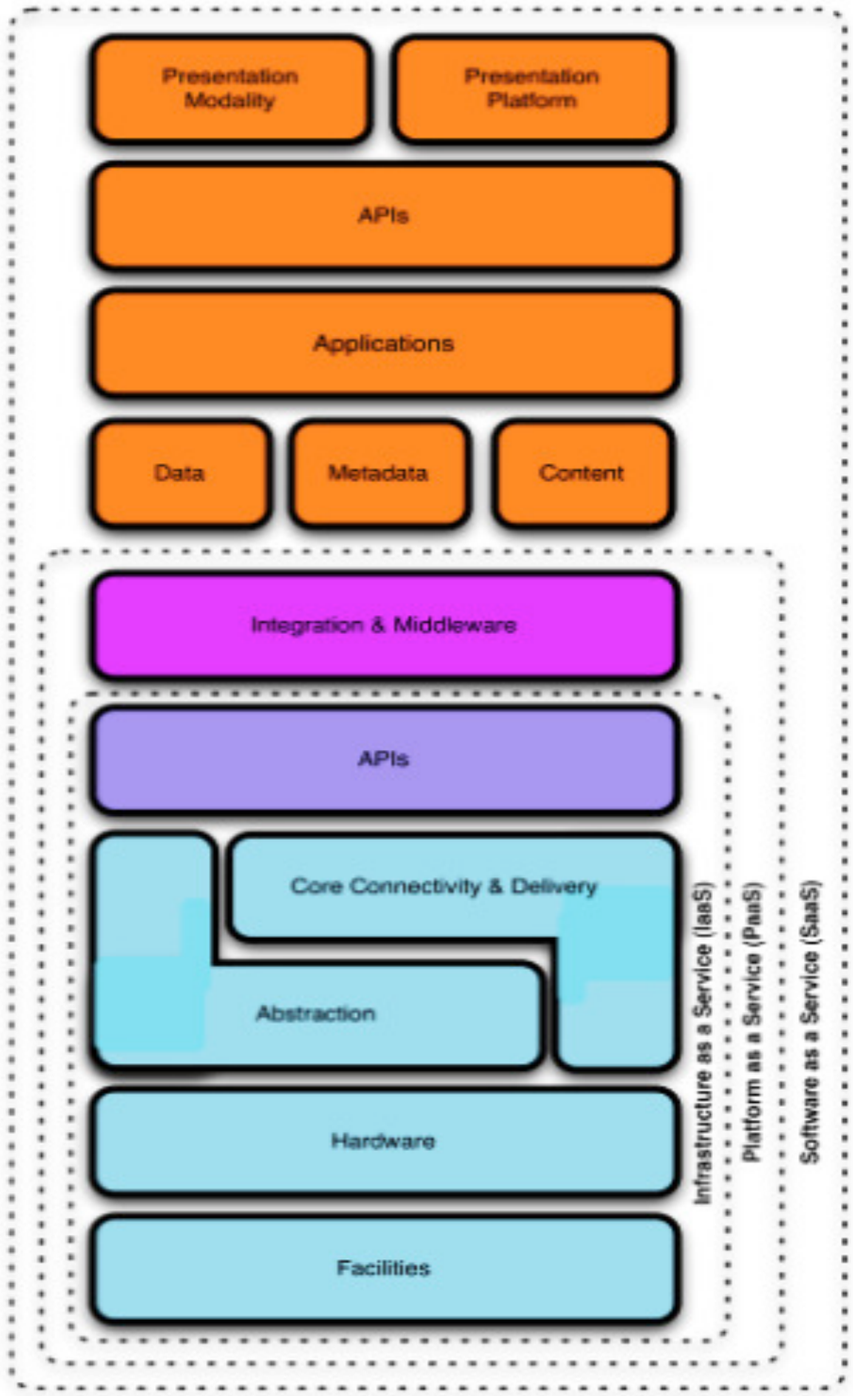
Real World Example

- Okta is an identity-as-a-service company
  - Occupies SaaS layers
  - Financial services customers

okta

- Amazon AWS provides the infrastructure

amazon web services™



Linking Okta & AWS control responses

- Okta answered 23 questions as “Not Applicable”, listing Amazon AWS as meeting these requirements
- https://cloudsecurityalliance.org/star-registrant/okta-inc/

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.2	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?			Not Applicable	Okta inherits such controls from our IaaS provider AWS. They are utilized for Okta systems management purposes only and not for customer use. For more information see http://aws.amazon.com/security.
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?			Not Applicable	
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?			Not Applicable	

CSA CAIQ v3.0.1 | Guiding Principles

Ready 88%

Linking Okta & AWS control responses

- Amazon provides a positive response for all questions Okta deemed “Not Applicable”
- https://cloudsecurityalliance.org/star-registrant/amazon-aws/#self

Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR -07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	BCR - 07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	
	BCR - 07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	
	BCR - 07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	

Value of control inheritance

- Speed
- Focus cloud providers on applicability
- Eliminate redundancy
- More complete & authoritative responses
- Smaller scoped audits can be conducted more frequently

- What it requires
  - Fact checkers
  - Analytics
  - Sharing
  - *Transparency!*

Microsoft Azure

Microsoft Azure Compliance Offerings

Globally Applicable

Compliance offerings covered in this section have global applicability across regulated industries and markets. They can often be relied upon by customers when addressing specific industry and regional compliance obligations. For example, ISO 27001 certification provides a baseline set of requirements for many other international standards and regulations.

1 CSA STAR Self-Assessment

The Cloud Security Alliance (CSA) is a nonprofit organization led by a broad coalition of industry practitioners, corporations, and other important stakeholders. It is dedicated to defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when transitioning their IT operations to the cloud. In 2013, the CSA and the British Standards Institution launched the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry in which cloud service providers (CSPs) can publish their CSA-related assessments based on the following components:

- Cloud Controls Matrix (CCM): a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a CSP.
- Consensus Assessments Initiative Questionnaire (CAIQ): a set of nearly 300 questions based on the CCM that a customer or cloud auditor may want to ask of CSPs to assess their compliance with CSA best practices.

STAR provides three levels of assurance. CSA STAR Self-Assessment is the introductory offering at Level 1, which is free and open to all CSPs. Going further up the assurance stack, Level 2 of the STAR program involves third-party assessment-based certifications, and Level 3 involves certifications based on continuous monitoring.

As part of the STAR Self-Assessment, CSPs can submit two different types of documents to indicate their compliance with CSA best practices: a completed CAIQ, or a report documenting compliance with CCM. For the CSA STAR Self-Assessment, Microsoft Azure publishes both CAIQ and CCM-based reports.

Applicability	Services in scope
Azure Azure Government	See respective ISO 27001 scope statements.

2 CSA STAR Certification

Microsoft Azure has obtained the Cloud Security Alliance (CSA) STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture. The CSA STAR Certification is based on achieving ISO 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM). It demonstrates that a cloud service provider conforms to the applicable requirements of ISO 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

CSA STAR LEVEL 1: CSA STAR Self-Assessment

AWS has completed the CSA STAR Self-Assessment and published the results to the AWS website. Please refer to the **CSA Consensus Assessments Initiative Questionnaire**. This is the latest CAIQ (v3) released by the CSA.

CSA STAR LEVEL 2: CSA STAR Attestation and Certification

Per the CSA definitions, AWS aligns with the CSA STAR Attestation and Certification via the determinations in our third party audits for SOC and ISO:

> CSA STAR Level 2 Attestation is based on SOC2, which can be **requested under NDA** - The SOC 2 report audit attests that AWS has been validated by a third party auditor to confirm that AWS' control objectives are appropriately designed and operating effectively.
>
> CSA STAR Level 2 Certification is based on **ISO 27001:2005**.

CSA STAR LEVEL 3: Continuous Monitoring

As noted on the **CSA website**, CSA is still defining the Level 3 Continuous Monitoring requirements. Although, for this reason, AWS cannot determine alignment, AWS does provide customers with the tools they need to meet continuous monitoring requirements. Customers can leverage the AWS Security by Design (SbD) program by providing control responsibilities outlines, the automation of security baselines, the configuration of security and the customer audit of controls for AWS customer infrastructure, operating systems, services and applications running in AWS. This standardized, automated, prescriptive and repeatable design can be deployed for common use cases, security standards and audit requirements across multiple industries and workloads. For more information visit the **Security by Design** page.

Government of Canada

Security Control Profile for Cloud-based GC IT Services

Protected B / Medium Integrity / Medium Availability

VERSION 1.0

28 February 2017

GCDOCS#21145124

Appendix A –Security Control Profile

The security controls and enhancements that constitute the GC cloud PBMM profile are listed in the table below. The table also shows the allocation of security controls to the GC and CSPs, the cloud components to which they apply as per Figure 3-1, and cross referenced to other related profiles and standards.

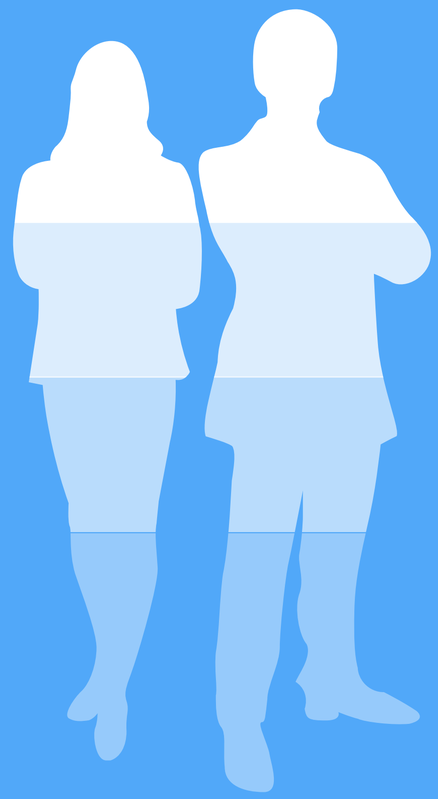
The following values are included in the table:

- X indicates that the control was selected or is applicable
- Not selected indicates that the control was not selected for inclusion in the profile
- Not allocated indicates that the control is selected, but not the responsibility for either the GC or the CSP to implement
- Not applicable indicates that the control is not included in the standard/profile (e.g. PM control family not included in ITSG-33 Annex 3 Controls Catalog)

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
			492	**437**	**348**								**433**	**325**			
AC-1	Access Control Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AIS-04 AAC-03 DSI-04 GRM-06 GRM-08 GRM-09 GRM-11 IAM-02 IAM-05 IAM-07 IAM-12 IVS-12	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.9.1.1 A.12.1.1 A.18.1.1 A.18.2.2

OUR ENVIRONMENT IN CHANGING

- DATA WILL CONTINUE TO EXPLODE
- THE REGULATORY & STANDARDS LANDSCAPE WILL CHANGE AND BECOME MORE COMPLEX
- NEW ATTACK SURFACES
- TECHNOLOGY LANDSCAPE CHANGES RAPIDLY



8.3% GROWTH RATE FOR INFORMATION SECURITY SPEND. FORCASTED TO BREAK 101 B BY 2020

33.3% BY 2020, A THIRD OF SUCCESSFUL ATTACKS EXPERIENCED BY ENTERPRISES WILL BE ON THEIR SHADOW IT RESOURCES

25% BY 2020, MORE THAN 25% OF IDENTIFIED ENTERPRISE ATTACKS WILL INVOLVE IOT

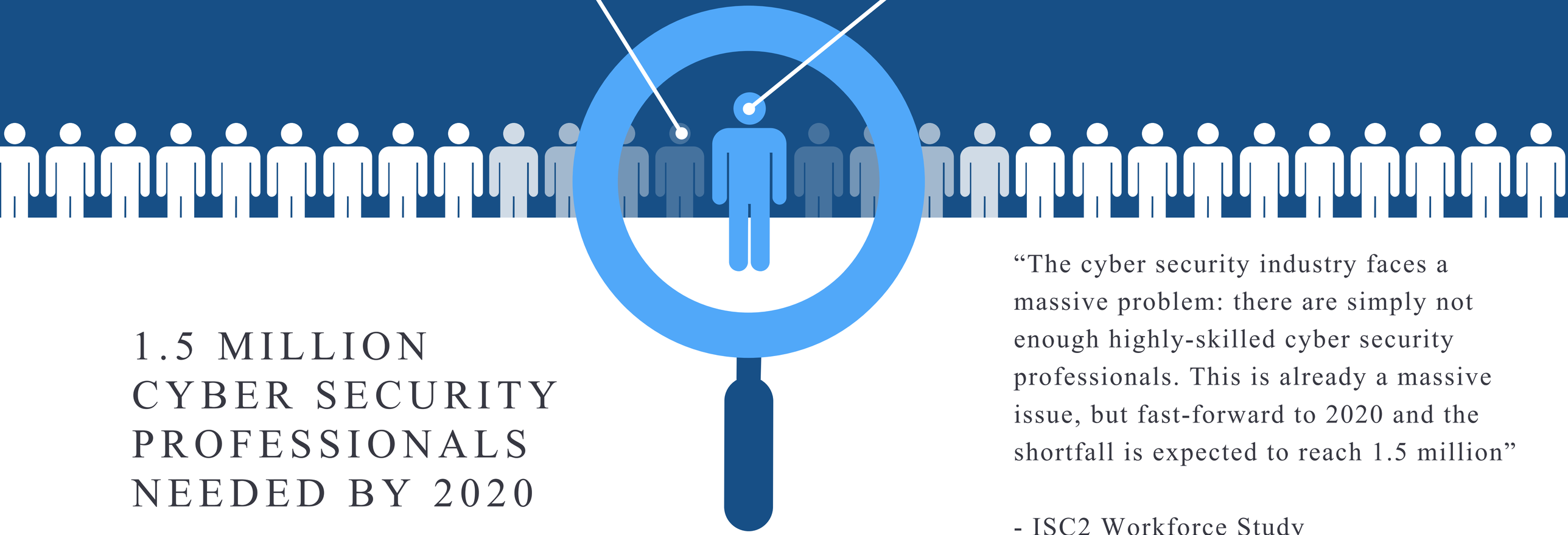
99% THROUGH 2020, 99% OF VULNERABILITIES EXPLOITED WILL CONTINUE TO BE ONES KNOWN BY SECURITY AND IT PROFESSIONALS FOR AT LEAST ONE YEAR.

CSA cloud security alliance®

cloud security alliance®

COLLEGE GRADUATES LACK THE SKILL AND EXPERIENCE

EXISTING EMPLOYEES CAN'T KEEP UP WITH THE CHANGES IN OUR INDUSTRY



1.5 MILLION CYBER SECURITY PROFESSIONALS NEEDED BY 2020

"The cyber security industry faces a massive problem: there are simply not enough highly-skilled cyber security professionals. This is already a massive issue, but fast-forward to 2020 and the shortfall is expected to reach 1.5 million"

- ISC2 Workforce Study

(ISC)²®

CCSK – User Certification

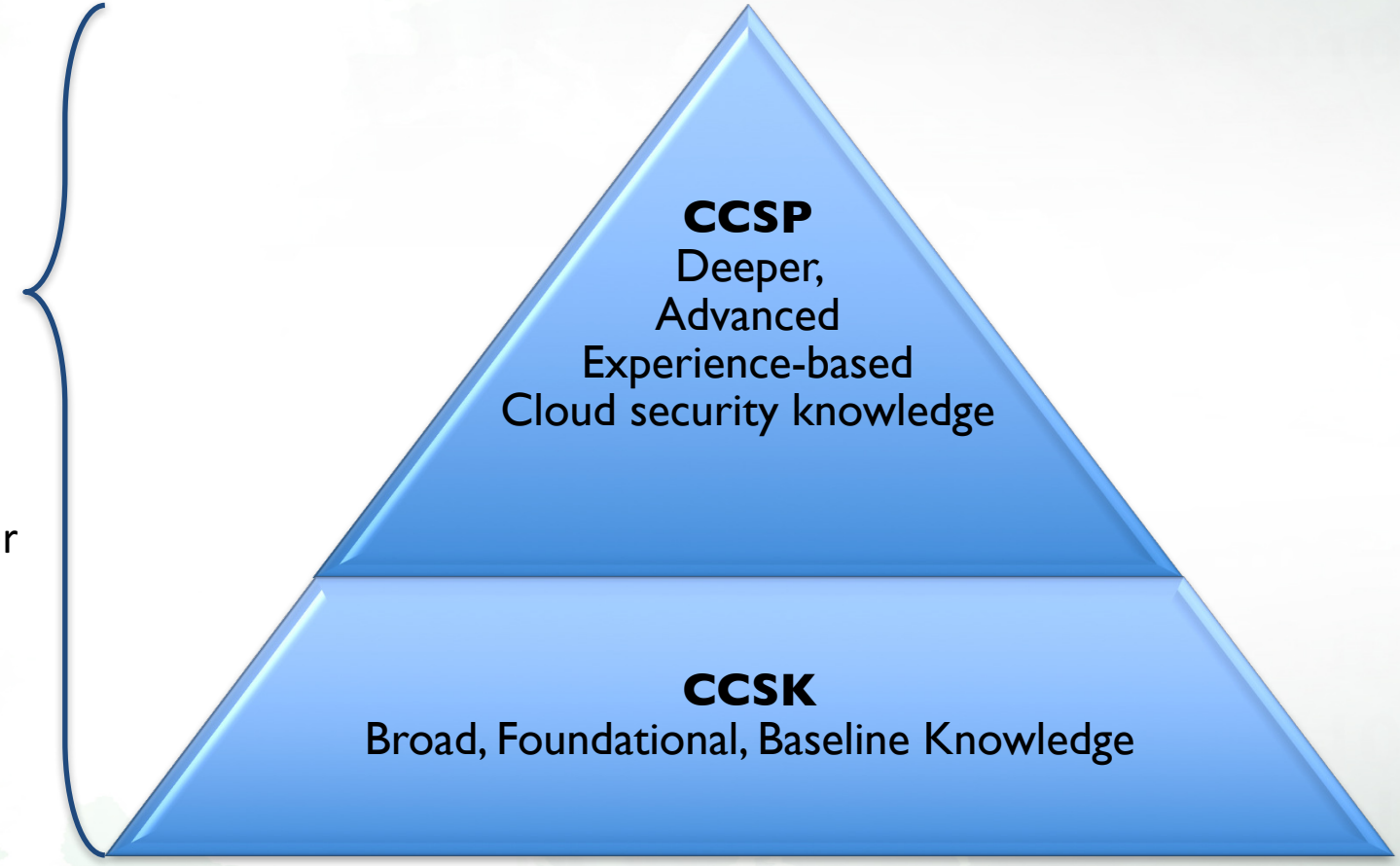
- *Certificate of Cloud Security Knowledge (CCSK)*
  - Benchmark of cloud security competency
  - Based on CSA guidance
  - Online web-based examination
  - www.cloudsecurityalliance.org/education/ccsk/
  - Partnered with (ISC)2 to develop complementary certification: CCSP
  - Close cloud security knowledge gaps

CCSP

cloud security alliance®

Complementary to Each

Both are vendor neutral and cover the Cloud Control Matrix of CSA



Amplify your message

- CSA is the largest cloud research organization in the world.
  - Over 85,000 Individual members
  - 75 chapters worldwide

- **Leverage** CSA Social Media:
  - CSA Blog – 500,000 annual web hits
  - Twitter – 5,000+ followers
  - LinkedIn - Reach all 80,000+ members

- **Showcase** your thought leaders through:
  - CloudBytes Webinar via BrightTALK – average 500+ views
  - Enterprise User Council call presentation – 85+ enterprise members
  - Participate in research webinars

Engage CSA membership

Network with 75 Chapters Worldwide

- 3 Regional Summits – Average 250+ attendees
- 50+ Local events – Average 150+ attendees
- Participate in research (areas of focus)

Unique sponsorship options:

- Sponsor research aligned with your competencies
- Conference sponsorships – Upcoming events
- Executive Membership
  - Become key advisory stakeholder to CSA
  - Collaborate quarterly with CSA Enterprise User membership
  - Sponsorship of CSA Summit @ RSA
  - Sponsorship of one research project

USEFUL CSA LINKS

CLOUD CONTROLS MATRIX (CCM)
https://cloudsecurityalliance.org/group/cloud-controls-matrix/

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ)
https://cloudsecurityalliance.org/group/consensus-assessments/

CSA STAR (Security, Trust and Assurance Registry), Provider Assurance Program
https://cloudsecurityalliance.org/star/

CSA CloudBytes Channel
https://cloudsecurityalliance.org/research/cloudbytes/#_overview

STARWatch
https://cloudsecurityalliance.org/star/watch/

DOWNLOAD CSA RESEARCH ARTIFACTS
https://cloudsecurityalliance.org/download

cloud CSA security alliance®


I SAW YOUR PRESENTATION
MY FAVORITE PART WAS THE END!
imgflip.com

THANK YOU

cloud security alliance®