MATES ED2MIT

Education and Training for Data Driven Maritime Industry

Tutorial A04.01

Cloud and Big Data Security and Compliance

Yuri Demchenko MATES Project

University of Amsterdam

Outline

Part 1. Big Data and Cloud Security

- Cloud security models, services and mechanisms
- Cloud Security best practices: AWS and Microsoft Azure

Part 2. Cloud Compliance and (Self-) Assessment

- Compliance standards, Security Controls
- CSA GRC Stack: Governance, Risk Management and Compliance
- PCI DSS Cloud Computing Guidelines

Part 3. Hands on: Big Data and Cloud Compliance

Cloud and security challenges

After a long period of experimentation, leading enterprises are getting serious about adopting the public cloud at scale

- Using the public cloud disrupts traditional cybersecurity models that many companies have built up over years.
- Companies need to evolve their cybersecurity practices dramatically in order to consume public-cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide.
  - McKinsey Research 2016: CISOs acknowledge cloud security as more advanced than typical enterprise IT security
- Recommended practices to develop public cloud security model:
  - Developing a cloud-centric cybersecurity model.
  - Redesigning a full set of cybersecurity controls for the public cloud.
  - Clarifying internal responsibilities for cybersecurity, compared to what providers will do.
  - Applying DevOps to cybersecurity: DevSecOps

Making a secure transition to the public cloud, By Arul Elumalai, James Kaplan, Mike Newborn, and Roger Roberts
https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/making-a-secure-transition-to-the-public-cloud

Adopting Public Cloud – Security Practices

- **Developing a cloud-centric cybersecurity model.**
  - Companies need to make choices about how to manage their perimeter in the cloud and how much they will rearchitect applications in a way that aligns with their risk tolerance, existing application architecture, resources available, and overall cloud strategy.
- **Redesigning a full set of cybersecurity controls for the public cloud.**
  - For each individual control, companies need to determine who should provide it and how rigorous they need to be.
- **Clarifying internal responsibilities for cybersecurity, compared to what providers will do.**
  - Public cloud requires a shared security model, with providers and their customers each responsible for specific functions. Companies need to understand this split of responsibilities—it will look very different from a traditional outsourcing arrangement—and redesign internal processes accordingly.
- **Applying DevOps to cybersecurity - DevSecOPs**
  - If a developer can spin up a server in seconds, but has to wait two weeks for the security team to sign off on the configuration, that attenuates the value of the public cloud’s agility. Companies need to make highly automated security services available to developers via APIs, just as they are doing for infrastructure services.

Cloud Computing Security – Challenges

- Fundamental security challenges and main user concerns in clouds
  - Data security: Where are my data? Are they protected? What control has cloud provider over data security and location?
  - Identity management and access control: Who has access to my personal/ID data?
- Two main tasks in making cloud secure and trustworthy
  - Secure operation of the cloud (provider) infrastructure
  - User controlled access control (security) infrastructure
    - Provide sufficient amount of security controls for competent user
- Cloud security infrastructure should provide a framework for dynamically provisioned cloud security services and infrastructure as a part of the main services

Security Basics: What should you know about Security?

- **Password is a basis for secure access** but it is not enough to secure your applications and services.
  - There is whole stack of network and infrastructure or platform security services and mechanisms which need to be applied in a consistent way to ensure high system ***dependability*** and ***availability***
- Basis for secure communication and data transfer are the security protocols and security mechanisms
  - Security services are defined for communicating entities and can work at different layers
  - Security mechanisms can be used by services and functional components to achieve one or another aspect of security
- Security is an overloaded term and may mean different aspects

  Network/communication Security - Data Security – Application Security - Operation Security – System Security

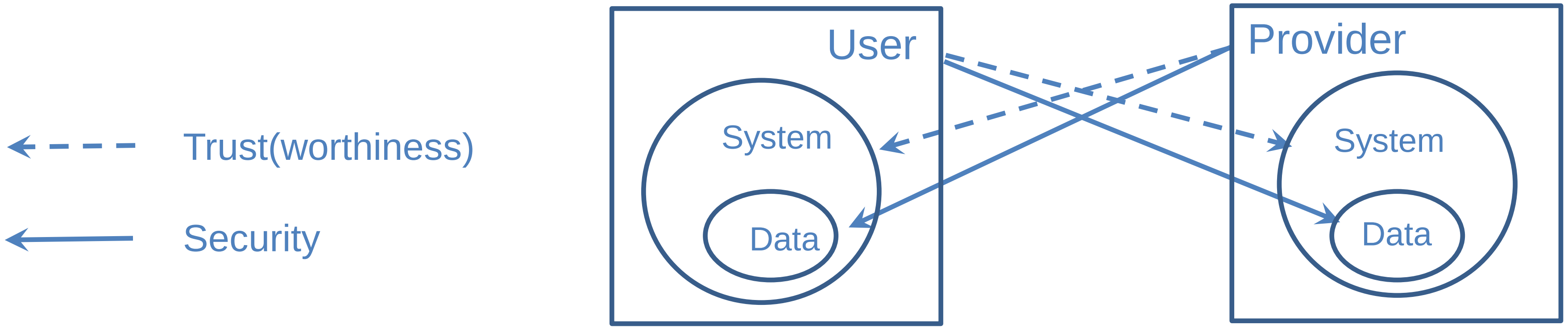
- What kind of data to protect
  - **Application Data – Personal Data (User ID, personal information) – Infrastructure management data**
- Data security must be considered for at least 3 aspects

  Data in transfer (Communication) – Data in-rest (Stored) – Data at run-time (Processed)

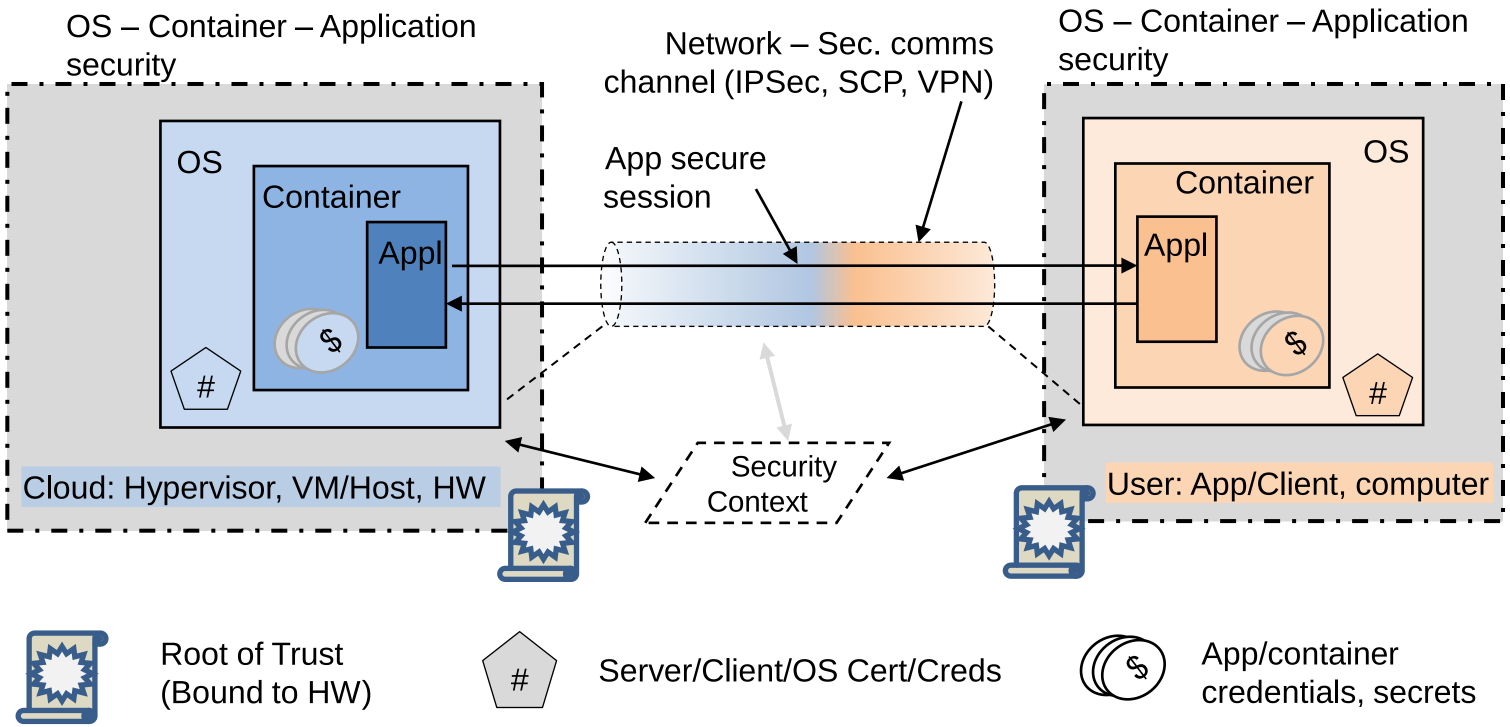
- Relations between Security and Trust
  - Trust or trust relations is a foundation of the security protocols and services

Different sides of Security and Trust

- Modern paradigm of remote distributed services and online/downloadable digital content provisioning makes security and trust relations between User and Provider more complex
- User and Service Provider – the two actors concerned with own Data/Content security and each other System/Platform trustworthiness
- Two other aspects of security/trust
  - Data stored vs Data processed
  - System Idle vs Active (running User session)



Cloud, OS, Network and Applications Trust Layers

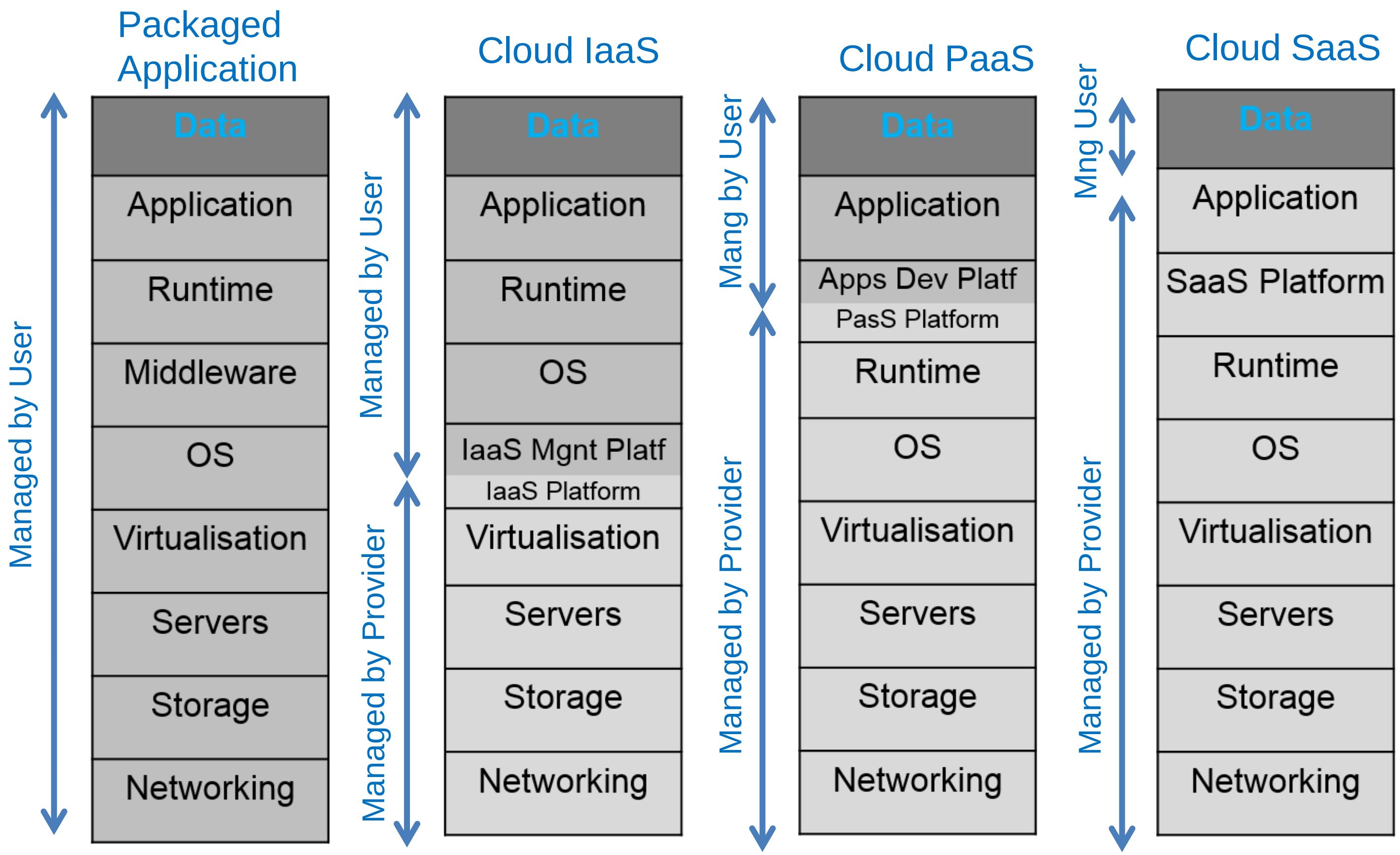

OS – Container – Application security
Network – Sec. comms channel (IPSec, SCP, VPN)
OS – Container – Application security
OS
Container
Appl
#
App secure session
OS
Container
Appl
#
Cloud: Hypervisor, VM/Host, HW
Security Context
User: App/Client, computer
Root of Trust (Bound to HW)
#
Server/Client/OS Cert/Creds
App/container credentials, secrets

- Consistent security must provide security at all layers correspondingly relying on trust credentials at each layer
  - Application – Container - Operating systems (security kernel) + Cloud platform
  - Network/communication – Runtime - Storage
- Two security models: Trusted Computing Base (TCB) for cloud platform and OSI/Internet security cloud based applications
  - Client/server and Service Oriented Architecture vs OS and hypervisor run-time
- Root of trust is based on the security credentials bound to hardware mediated through OS to runtime environment

Cloud Environment and Issues to be addressed

- Virtualised services and environment
- On-demand provisioning and dynamic scalability
- Multi-tenant platform security and multi-user services access control
  - Tenants’ storage and runtime separation in cloud
  - Fine grained access control in the tenants’ applications
- New cloud oriented security services models
  - Provider – Customer/Tenant - User
    - Enterprise as a Customer, and employees as Users
- Uncontrolled execution and data storage environment
  - Promising homomorphic/elastic encryption (still at research stage)
- Security services are provisioned on-demand (as part of virtualised infrastructure) and require bootstrapping with the customer services and trust domain
  - Bootstrapping cloud and customer trust domains to ensure trusted environment for data processing and storage
- Integration with customer legacy security services and infrastructure
  - Campus/office local network/accounts

Responsibilities Split in IaaS, PaaS, SaaS



Packaged Application
Managed by User
Data
Application
Runtime
Middleware
OS
Virtualisation
Servers
Storage
Networking

Cloud IaaS
Managed by User
Managed by Provider
Data
Application
Runtime
OS
IaaS Mgnt Platf
IaaS Platform
Virtualisation
Servers
Storage
Networking

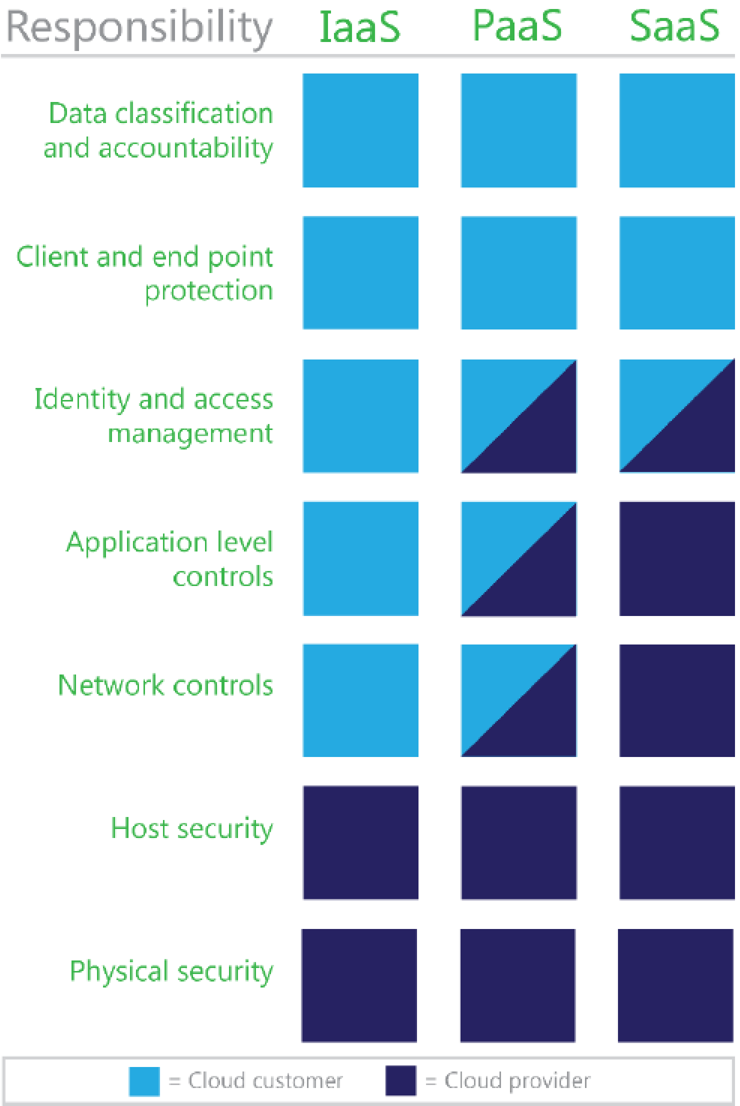
Cloud PaaS
Mang by User
Managed by Provider
Data
Application
Apps Dev Platf
PasS Platform
Runtime
OS
Virtualisation
Servers
Storage
Networking

Cloud SaaS
Mng User
Managed by Provider
Data
Application
SaaS Platform
Runtime
OS
Virtualisation
Servers
Storage
Networking

Security management responsibilities split between Customer and Provider for IaaS, PaaS, SaaS service models

- Updating firmware and software for platform and for customer managed components
- Firewall is intrusion prevention is a responsibility of the cloud provider
- Certification and compliance of the cloud platform doesn’t imply security and compliance of the customer controlled components

Data Protection Obligations by CSP and Customers (PCI DSS model)

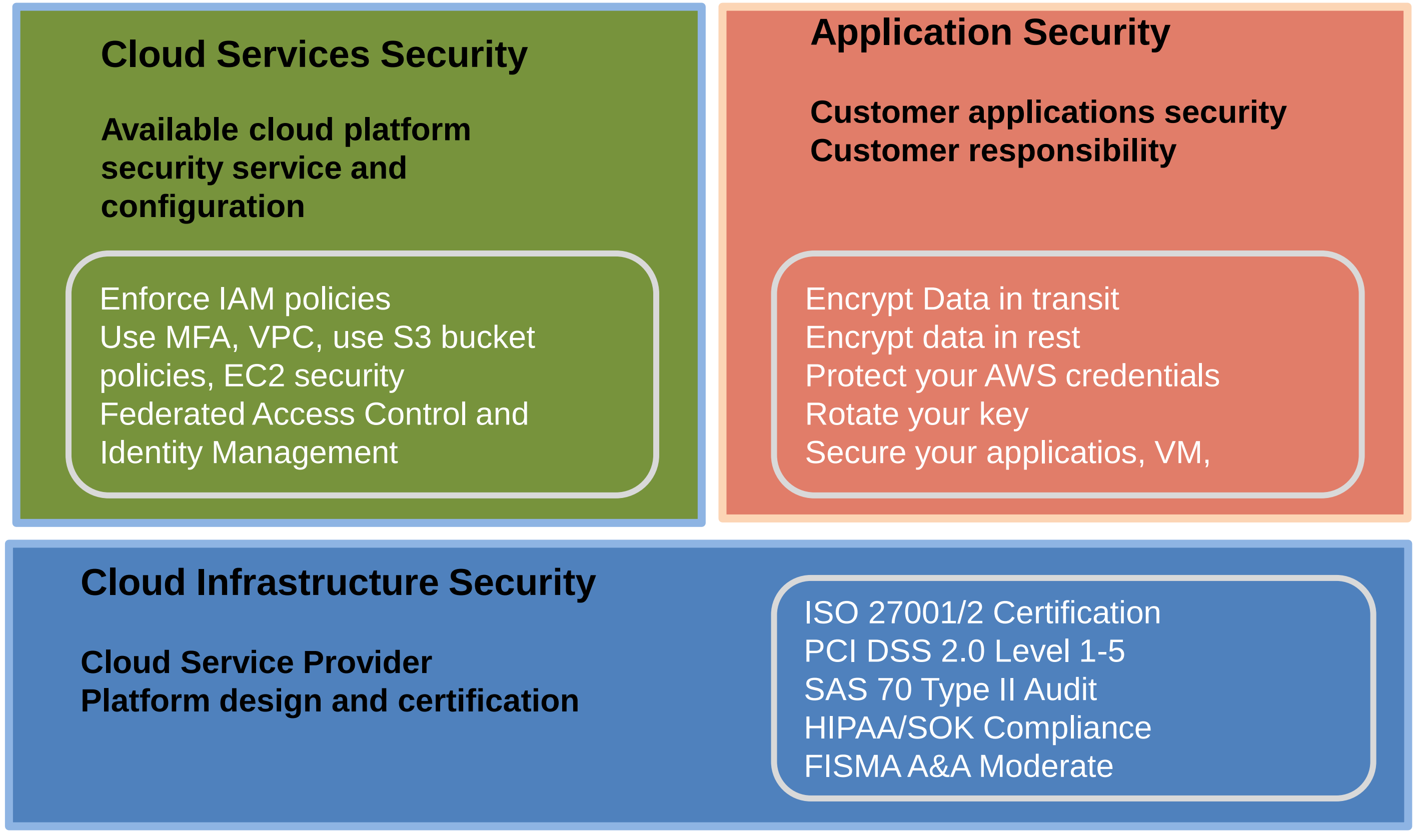


Responsibility	IaaS	PaaS	SaaS
Data classification and accountability	🟦	🟦	🟦
Client and end point protection	🟦	🟦	🟦
Identity and access management	🟦	◩	◩
Application level controls	🟦	◩	⬛
Network controls	🟦	◩	⬛
Host security	⬛	⬛	⬛
Physical security	⬛	⬛	⬛

🟦 = Cloud customer ⬛ = Cloud provider

- Although customers are responsible for classifying their data, **cloud providers should make written commitments** to customers about the privacy of the customer data stored within their cloud.
- These commitments should include **information about privacy and security practices, data use limitations, and regulatory compliance**.
- Cloud providers should make **certifications and audit reports** that demonstrate compliance with key standards and regulations
- Customers should not migrate data to a cloud provider that cannot address their data protection needs.

Amazon Web Services Security Model



Cloud Services Security

Available cloud platform security service and configuration

Enforce IAM policies
Use MFA, VPC, use S3 bucket policies, EC2 security
Federated Access Control and Identity Management

Application Security

Customer applications security
Customer responsibility

Encrypt Data in transit
Encrypt data in rest
Protect your AWS credentials
Rotate your key
Secure your applicatios, VM,

Cloud Infrastructure Security

Cloud Service Provider
Platform design and certification

ISO 27001/2 Certification
PCI DSS 2.0 Level 1-5
SAS 70 Type II Audit
HIPAA/SOK Compliance
FISMA A&A Moderate

Security is declared as one of critical importance to AWS cloud that is targeted to protect customer information and data from integrity compromise, leakage, accidental or deliberate theft, and deletion.

- The AWS infrastructure is designed with the high availability and sufficient redundancy to ensure reliable services operation.

AWS Security – Shared Responsibility Model

AWS implements the ***Shared Responsibility Model*** that splits responsibility for the security of different layers and components between AWS as a provider and a customer or tenant.

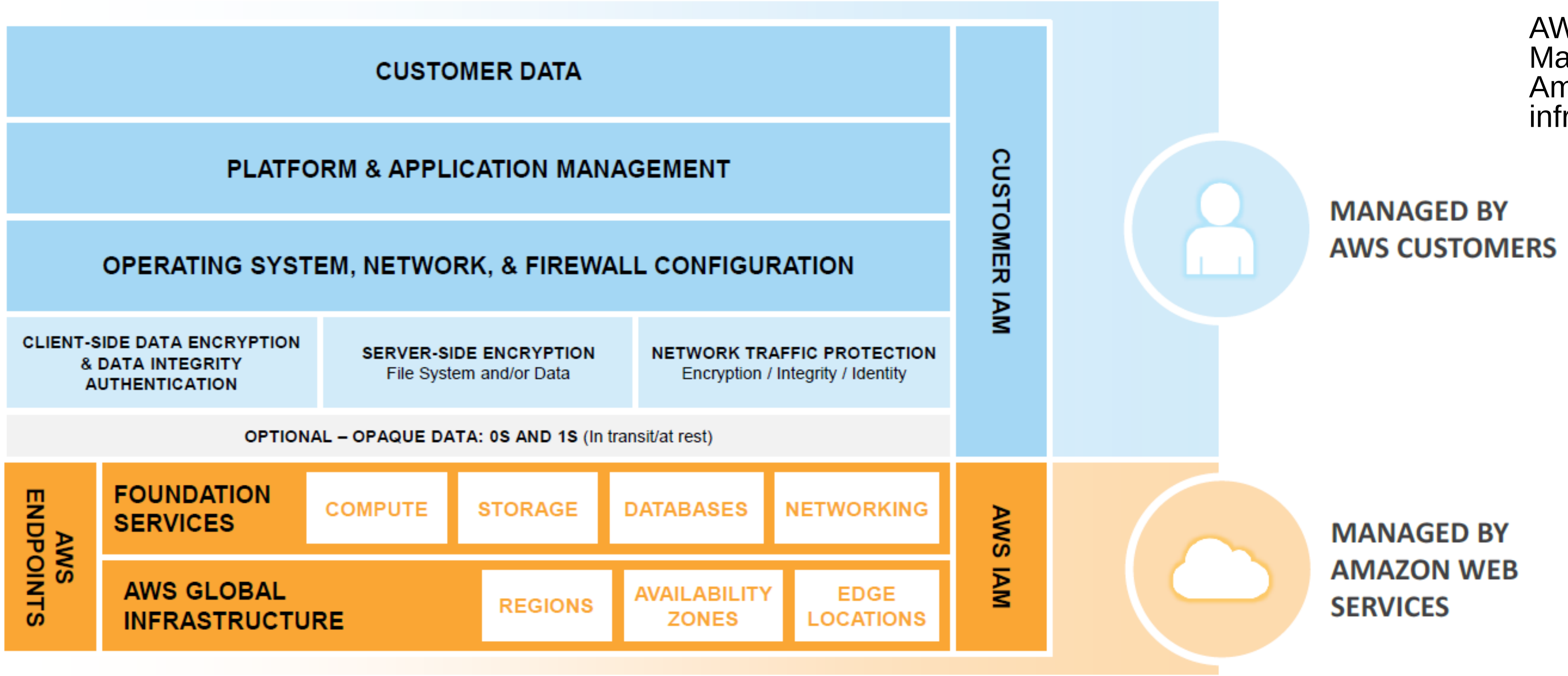
AWS as a cloud provider ensures the security of the cloud infrastructure and cloud platform services:

- Facilities
- Physical security of datacentre
- Network infrastructure
- Virtualisation platform and infrastructure

While **the customer** is responsible for security of the following components:

- Amazon Machine instances, OS, and applications
  - Note, the customer is responsible for security update and patching of the guest OS and installed applications
- Data in transit, data at rest, and data stores
- Credentials, policies and configurations
- Comply with the Acceptable Use Policy (AUP), ensure correct use of the cloud platform

Example: Security responsibility sharing in AWS IaaS infrastructure services


CUSTOMER DATA
PLATFORM & APPLICATION 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
OPTIONAL – OPAQUE DATA: 0S AND 1S (In transit/at rest)
CUSTOMER IAM
AWS ENDPOINTS
FOUNDATION SERVICES
COMPUTE
STORAGE
DATABASES
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS
AWS IAM
MANAGED BY AWS CUSTOMERS
MANAGED BY AMAZON WEB SERVICES

AWS Identity and Access Management (IAM) over Amazon EC2 and S3 infrastructure services

- For other cloud service models PaaS and SaaS the responsibility of AWS goes up to OS, network and firewall for PaaS, and also includes the application platform and container for SaaS.
  - However, the responsibility for data remains with the customer.

[ref] Todorov, D. & Ozkan, Y. (November 2013) ‘AWS security best practices’, Amazon Web Services [Online]. Available from: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

AWS Security Recommendations: Customer side

Recommended **security best practices** at each layer

- Protect your Amazon account
- Control internal access to AWS resources
- Limit external access to your cloud
- Protect data in transit and at rest
- Secure data assets
- Secure your compute assets (OS, instances, App)
- Backup for easy recover
- Keep track of your cloud resources (using monitoring service)

Security methods for customer cloud infrastructure

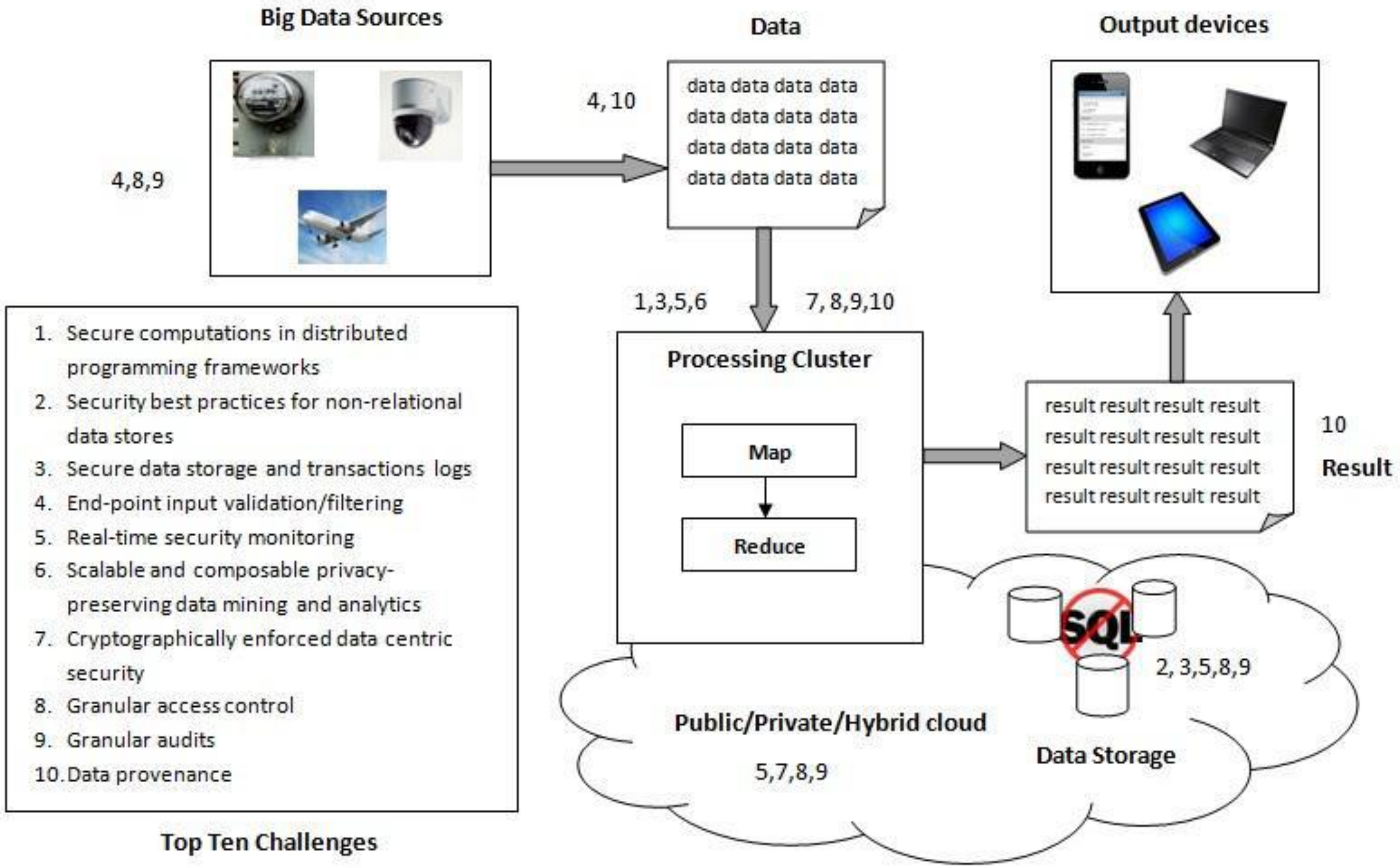
- Virtual Private Cloud (VPC) to create a secure environment for your cloud services in AWS
- Security zoning and network segmentation based on security groups, Network Access Control Lists, host based firewalls
- Network security and secure access for users and applications
- Threats protection layer in traffic flow to ensure protection against Denial of Service (DoS) attacks

[ref] D.Todorov, Y.Ozkan. AWS Security Best Practices. November 2013 [online] http://bit.lu/aws- security-best-practices-new

Big Data Security

- Expanded Top Ten Big Data Security and Privacy Challenges. CSA Report, 16 June 2013.
  - https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf
- CSA Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy at
  - https://cloudsecurityalliance.org/download/big-data-security-and-privacy-handbook/
  - 10 recommendations are provided for each of CSA Top Ten Big Data Security Challenges

CSA Top Ten Big Data Security and Privacy Challenges



1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transactions logs
4. End-point input validation/filtering
5. Real-time security monitoring
6. Scalable and composable privacy-preserving data mining and analytics
7. Cryptographically enforced data centric security
8. Granular access control
9. Granular audits
10. Data provenance

Top Ten Challenges

Expanded Top Ten Big Data Security and Privacy Challenges. CSA Report, 16 June 2013.
https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf

CSA Top Ten Big Data Security Challenges by Functional Groups (1)

Cloud Security Alliance also published their ‘Expanded Top Ten Big Data Security and Privacy Challenges’ document as early as in June 2013.

Top Ten challenges are grouped into four functional groups:

A. Infrastructure security

TT01. Secure computations in distributed programming frameworks
TT03. Secure data storage and transactions logs
TT04. End-point input validation/filtering
TT05. Real-time security/compliance monitoring

B. Access control and policy

TT02. Security best practices for non-relational data stores
TT08. Granular access control and data centric access policies

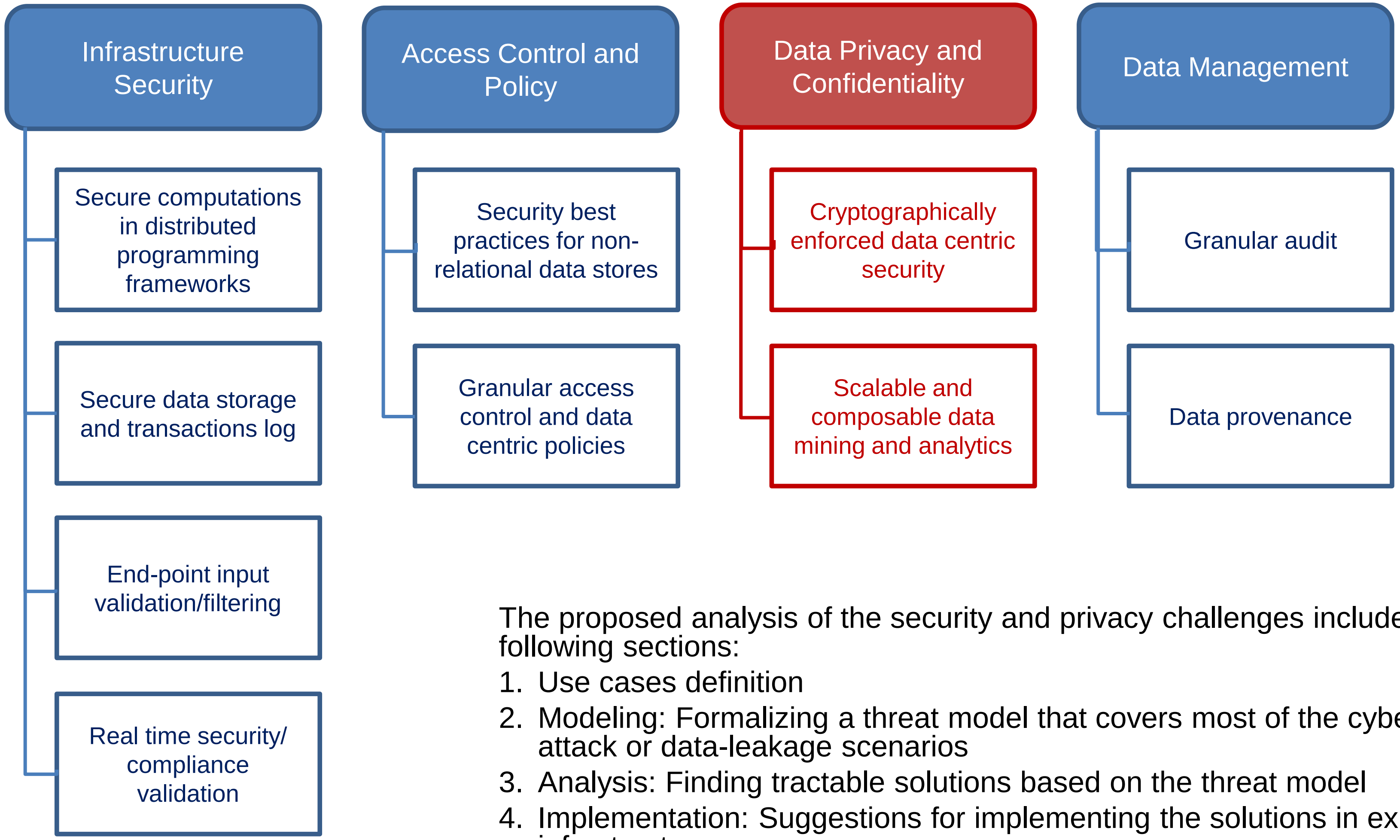
C. Data Privacy and Confidentiality

TT06. Scalable and composable privacy-preserving data mining and analytics
TT07 Cryptographically enforced data centric security

D. Data Management

TT09. Granular audits
TT10. Data provenance

CSA Top Ten Big Data Security Challenges by Functional Groups (2)



Infrastructure Security
Secure computations in distributed programming frameworks
Secure data storage and transactions log
End-point input validation/filtering
Real time security/ compliance validation
Access Control and Policy
Security best practices for non-relational data stores
Granular access control and data centric policies
Data Privacy and Confidentiality
Cryptographically enforced data centric security
Scalable and composable data mining and analytics
Data Management
Granular audit
Data provenance

The proposed analysis of the security and privacy challenges includes the following sections:

1. Use cases definition
2. Modeling: Formalizing a threat model that covers most of the cyber-attack or data-leakage scenarios
3. Analysis: Finding tractable solutions based on the threat model
4. Implementation: Suggestions for implementing the solutions in existing infrastructures

CSA TT5. Real-Time Security/Compliance Monitoring Best Practices in the Big Data Security

- ***A. Infrastructure security***

Use case:

Most industries and government agencies will benefit from real-time security analytics. Common uses include utilizing the technology to answer questions such as, “Who is accessing which data from which resource at what time,” “Are we under attack,” or “Is there a breach of compliance standard C because of action A?”

5.1 Apply big data analytics to detect anomalous connections to cluster

5.2 Mine logging events

5.3 Implement front-end systems

5.4 Consider cloud-level security

5.5 Utilize cluster-level security

5.6 Apply application-level security

5.7 Adhere to laws and regulations

5.8 Reflect on ethical considerations

5.9 Monitor evasion attacks

5.10 Track data-poisoning attacks

CSA Top Ten TT07. Cryptographically Enforced Data-Centric Security

- ***C. Data Privacy and Confidentiality***

Use case:

On-demand provisioned and distributed character of the Big Data infrastructure, especially if it is cloud based, make it practically unfeasible to achieve full protection of data at all infrastructure layers and during the whole data lifecycle, unless data remain encrypted all time.

7.1 Construct system to search, filter for encrypted data

7.2 Secure outsourcing of computation using fully homomorphic encryption

7.3 Limit features of homomorphic implementation

7.4 Apply relational encryption to enable comparison of encrypted data

7.5 Reconcile authentication and anonymity

7.6 Implement identity-based encryption

7.7 Utilize attribute-based encryption and access control

7.8 Use oblivious RAM for privacy preservation

7.9 Incorporate privacy-preserving public auditing

7.10 Consider convergent encryption for deduplication

CSA Top Ten TT10.0 Data Provenance

- ***D. Data Management***

Use case:

Several key security applications require a digital record with details about its creation. Examples include detecting **insider trading for financial companies** or determining the **accuracy of the data source for research** investigations. These security assessments are time-sensitive in nature and require fast algorithms to handle the provenance metadata containing this information. In addition, data provenance complements **audit logs** for compliance requirements, such as PCI or Sarbanes-Oxley.

10.1 Develop infrastructure authentication protocol

10.2 Ensure accurate, periodic status updates

10.3 Verify data integrity

10.4 Ensure consistency between provenance and data

10.5 Implement effective encryption methods

10.6 Use access control

10.7 Satisfy data independent persistence

10.8 Utilize dynamic fine-grained access control

10.9 Implement scalable fine-grained access control

10.10 Establish flexible revocation mechanisms

Part 2. Cloud Compliance

- Compliance standards, Security Controls
- CSA GRC Stack: Governance, Risk Management and Compliance

Security and Compliance

- Security is commonly defined as a set of technical, physical, and administrative controls in order to ensure normal operation of a system or application
  - Security is often associated with the CIA triad Confidentiality, Integrity, Availability
  - Appropriate level of security requires organizations to take measures and comply to the numerous security controls

- Compliance is a certification or confirmation that the system or an organization meets the requirements of specified standards, established legislation, regulatory guidelines or industry best practices that can be jointly defined as compliance framework
  - A compliance framework can includes business processes and internal controls the organization has in place to adhere to these standards and requirements
  - The framework should also map different requirements to internal controls and processes to eliminate redundancies

- Why it is important for cloud?
  - When moving to cloud, the organization moves from internal security and operational environment/context (that may not be formally defined) to external operational security that will become a part of SLA (or business requirement) with CSP
- Problem with achieving compliance for cloud based applications/solutions
  - Audit requirements are not designed for virtualised distributed environment
  - Lack of visibility in cloud: large CSP such as Amazon and Google are “walled/curtained gardens”
  - Requirements to allow CSP audit may involve Non-Disclosure Agreement (NDA) and risk of provider lock-in

Regulatory requirements to be considered for cloud compliance – General Standards

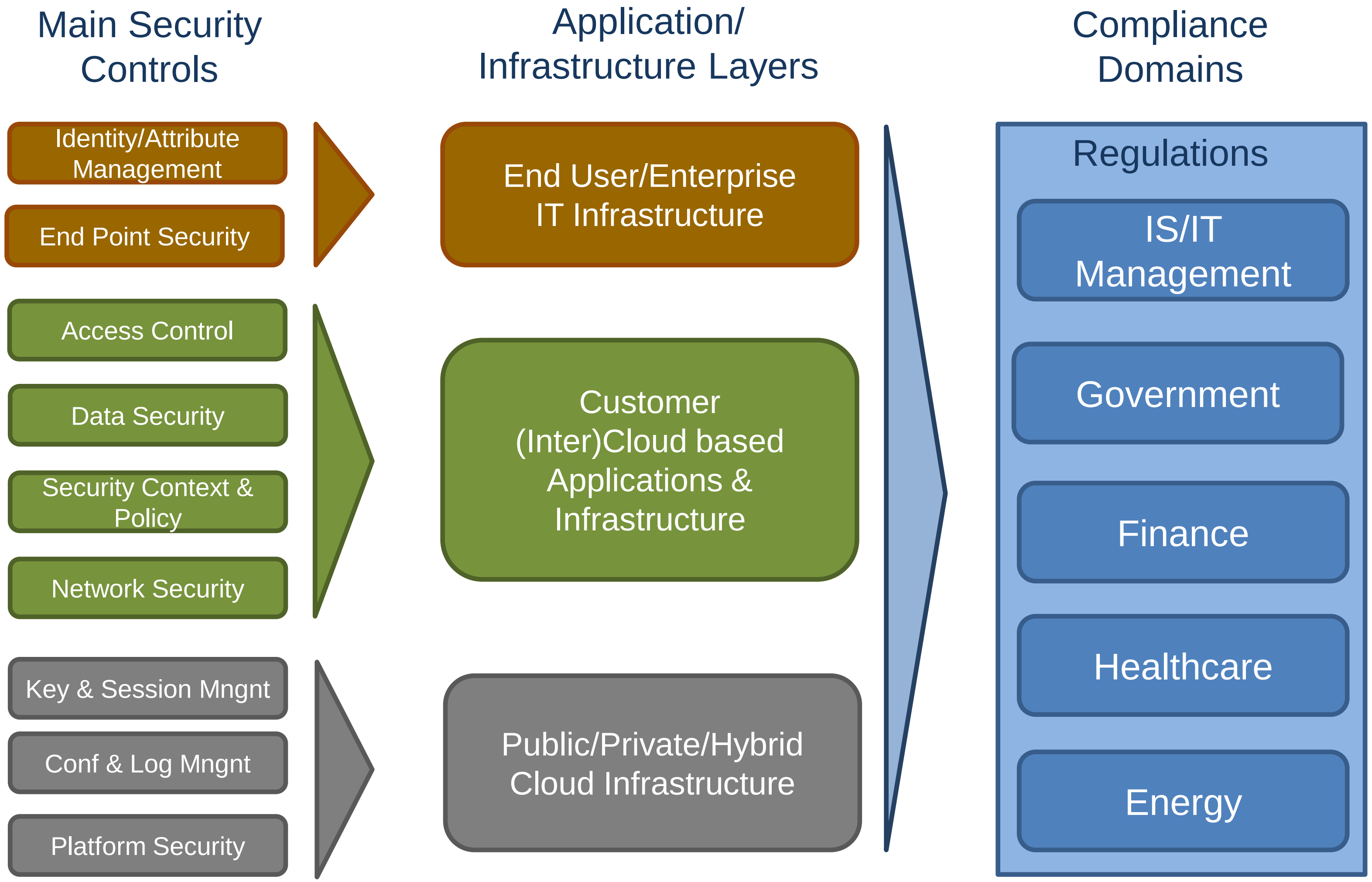
General standards and recommendations

- ISO/IEC 27001:2005 Certification on security infrastructure
  - Industry standard: the risk-based information security management program that follows a plan-do-check-act process
- NIST SP 800-53 Security Controls and ISO/IEC 15408 Evaluation Cirteria
- HIPAA/HITECH - The U.S. Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)
  - Act created by the US federal government include provisions to protect patients' private information.
- NIST SP 800-144 Guidelines for Security and Privacy in Cloud Computing
- Cloud Security Alliance (CSA) Security Guidance for Critical Area of focus in Cloud Computing
- ENISA Cloud Computing Security Risk Assessment
- EU GDPR – General Data Protection Regulation

Industry and Governmental Regulatory Requirements (USA)

- Service Organisation Control SOC 1 (SSAE 16/ISAE 3402) and SOC 2 and 3 (AT 101)
  - SOC 2 is a detailed attestation report (often restricted) for service organizations that contains strict standards for security, availability, processing integrity, confidentiality, and privacy.
  - SOC 3 is a general purpose report which summarizes the SOC 2 audit
- Sarbanes Oxley Act (SOX) also known as "Corporate and Auditing Accountability and Responsibility Act" set enhanced standards for all US public company boards, management and public accounting firms.
  - According to SOX act, top management must individually certify the accuracy of financial information.
- The Federal Information Security Management Act of 2002 (FISMA)
  - Describes security requirements for the protection of information and information systems in Federal systems
- Department of Defense Information Certification Accreditation Process (DIACAP)
- Federal Risk and Authorization Management Program (FedRAMP)
  - As of June 6, 2014, US federal agencies must utilize only cloud providers assessed and authorized through FedRAMP. List of authorized cloud providers is published:
    - Authorisation: AWS East-West US and AWS Governmental Community Cloud, SalesForce, USDA
    - Provisional Authorisation: Akamai, AT&T, IBM, Hewlett-Packard, Lockheed Martin, Microsoft Azure, Oracle

Mapping Compliance and Cloud Infrastructure Components



Main Security Controls

Application/ Infrastructure Layers

Compliance Domains

Identity/Attribute Management

End Point Security

End User/Enterprise IT Infrastructure

Access Control

Data Security

Security Context & Policy

Network Security

Customer (Inter)Cloud based Applications & Infrastructure

Key & Session Mngnt

Conf & Log Mngnt

Platform Security

Public/Private/Hybrid Cloud Infrastructure

Regulations

IS/IT Management

Government

Finance

Healthcare

Energy

Security and Compliance Questions

The main questions that security and compliance auditors would ask you

- Where is our data going to reside?
- Who is going to look after it?
- Who is going to be able to see it?
- Is it going to be the people that manage the infrastructure for us?
- Is it going to be internal and external people?
- And if we use a public cloud how secure is that cloud platform for us?
- Is the cloud going to be segregated from other organisations’ data?

Case study: Certification/Compliance by Amazon AWS Cloud

The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best-practices including:

- ISO/IEC 27001:2005
- SOC 1, SOC2, SOC3
- FIPS 140-2
- CSA
- PCI DSS Level 1
- HIPAA
- ITAR
- DIACAP and FISMA
- FedRAMP (SM)
- MPAA

Amazon Cloud is certified for hosting US Governmental services

http://aws.amazon.com/compliance/

Case study: Certification/Compliance by Microsoft Azure

Microsoft services/infrastructure meets the following key certifications, attestations and compliance capabilities

- ISO/IEC 27001:2005 Certification on security infrastructure
- SOC 1 (SSAE 16/ISAE 3402) and SOC 2 and 3 (AT 101)
  - Obtained in 2008 and 2012
- Cloud Security Alliance (CSA) Cloud Controls Matrix
- NIST SP 800-144 Guidelines for Security and Privacy in Cloud Computing
- PCI Data Security Standard Certification level 1
- HIPAA and HITECH
- FISMA Certification and Accreditation – since 2010
- Various state, federal, and international Privacy Laws(95/46/EC, e.g. EU Data Protection Directive, California SB 1386, etc.)

http://www.windowsazure.com/en-us/support/trust-center/compliance/

A Complete Cloud Security Governance, Risk, and Compliance (GRC) Stack

https://cloudsecurityalliance.org/research/grc-stack/

Delivering	← Stack Pack →	Description
Continuous monitoring … with a purpose	CTP™	Cloud Trust Protocol (CTP) • Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers
Claims, offers, and the basis for auditing service delivery	Cloud Audit™	• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
Pre-audit checklists and questionnaires to inventory controls	CAI™	Consensus Assessments Initiative (CAI) • Industry-accepted ways to document what security controls exist
The recommended foundations for controls	CCM™	Cloud Control Matrix (CCM) • Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider

CSA3.0 Security Guidance for Critical Area of Focus in Cloud Computing

The CSA3.0 defines 13 domains of the security concerns for Cloud Computing that are divided into two broad categories that define corresponding security controls.

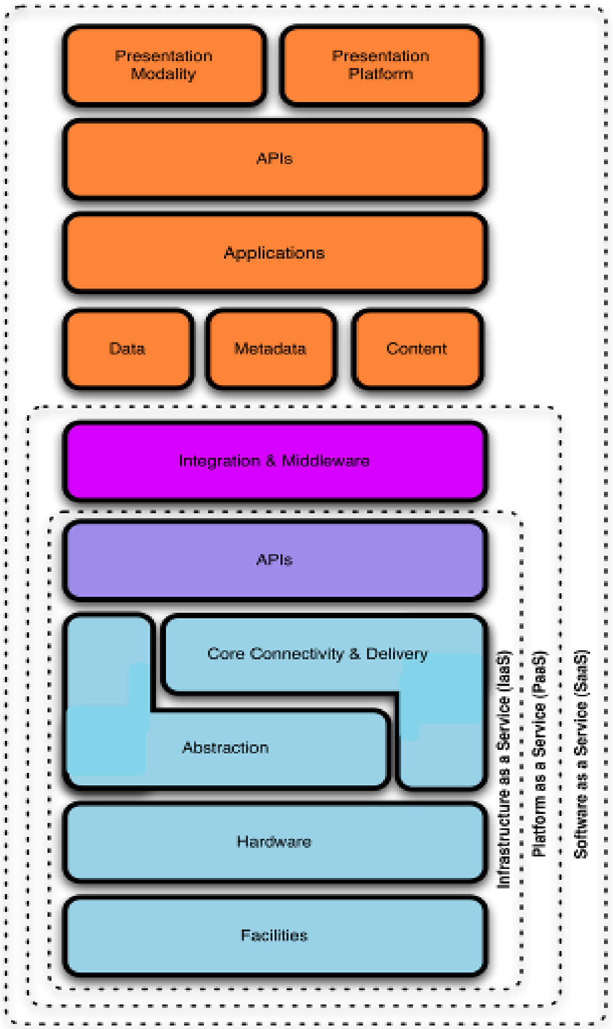
Governance domains

1. Governance and Enterprise Risk Management
2. Legal Issues: Contracts and Electronic Discovery
3. Compliance and Audit
4. Information Management and Data Security
5. Portability and Interoperability

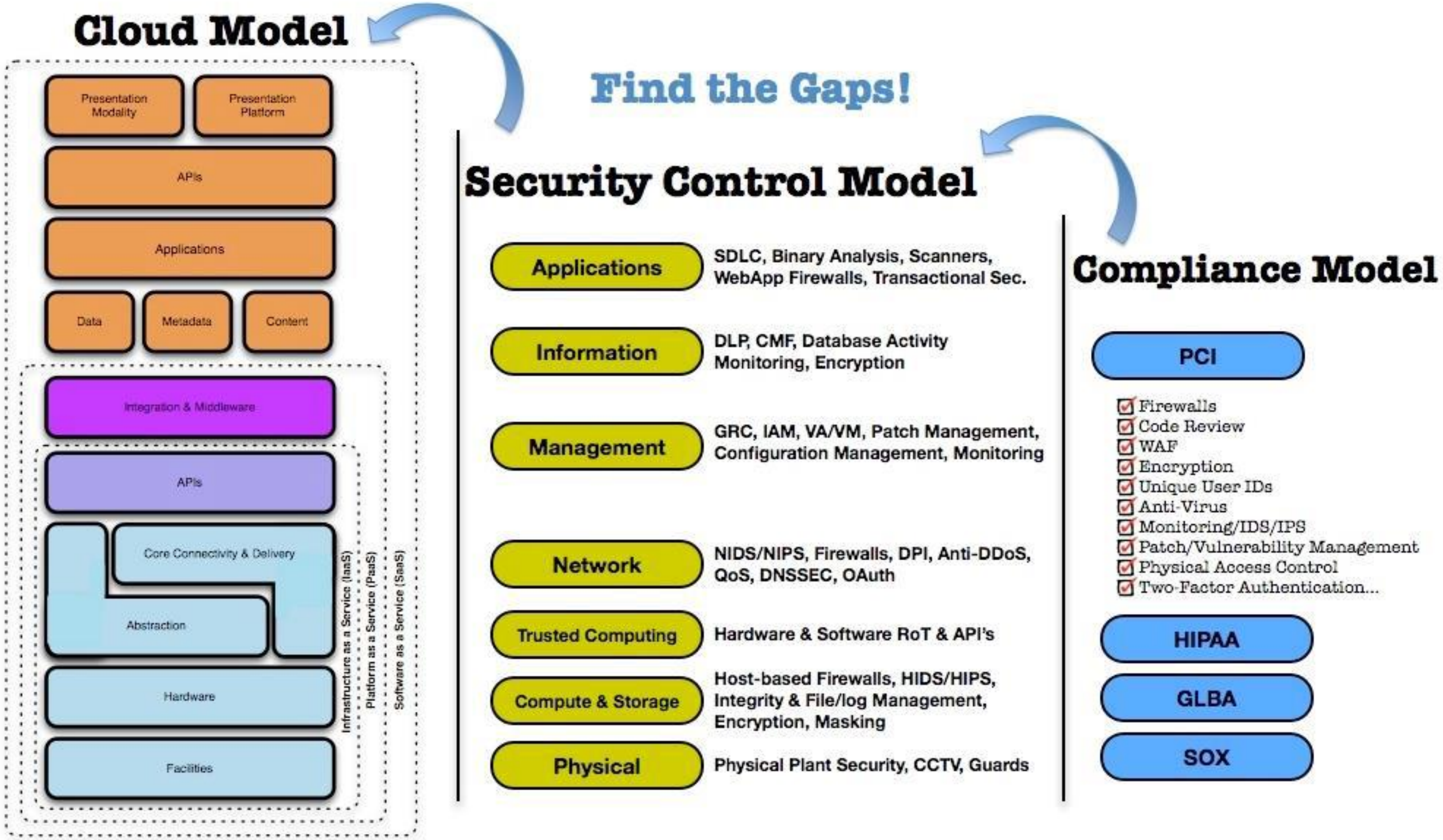
Operational Domains

6. Traditional Security, Business Continuity and Disaster Recovery
7. Data Center Operations
8. Incident Response, Notification and Remediation
9. Application Security
10. Encryption and Key Management
11. Identity and Access Management
12. Virtualization
13. Security as a Service

CSA3.0 Cloud Services Model



CSA3.0: Mapping the Cloud Model to the Security Control & Compliance



Cloud Model

Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

Integration & Middleware

APIs

Core Connectivity & Delivery

Abstraction

Hardware

Facilities

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

SP500-292 (CCRA), CSA3.0

ISO/IEC 27002:2013 InfoSec Controls

PCI DSS V3.0 (2013)

[ref] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2013)
https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

What is the Cloud Controls Matrix (CCM)?

- Baseline control framework specifically designed for managing risk in the Cloud Supply Chain:
  - Addressing the inter and intra-organizational challenges of persistent information security by clearly delineating control ownership.
  - Providing an anchor point and common language for balanced measurement of security and compliance postures.
  - Providing the holistic adherence to the vast and ever evolving landscape of global data privacy regulations and security standards.
- Serves as the basis for new industry standards and certifications.

CCM Control Groups:

1. Compliance (CO)
2. Data Governance (DG)
3. Facility Security (FS)
4. Human Resources (HR)
5. Information Security (IS)
6. Legal (LG) .
7. Operations Management (OM)
8. Risk Management (RI)
9. Release Management (RM)
10. Resiliency (RS)
11. Security Architecture (SA)

98 security controls in total

CSA Consensus Assessment Initiative

- A cloud supply chain risk management and due diligence questionnaire
- ~ 200 yes/no questions that map directly to the CCM, and thus, in turn, to many industry standards.
- Can be used by both CSPs for self-assessment or by potential customers for the following purposes
  - to identify the presence of security controls and practices for cloud offerings
  - procurement negotiation
  - contract inclusion
  - to quantify SLAs
- For potential customers, the CSA Consensus Assessment Initiative Questionnaire (CAIQ) is intended to be part of an initial assessment followed by further clarifying questions of the provider as it is applicable to their particular needs.
  - v1.1 published in Sept 2011; v3.0.1 is available from 2014

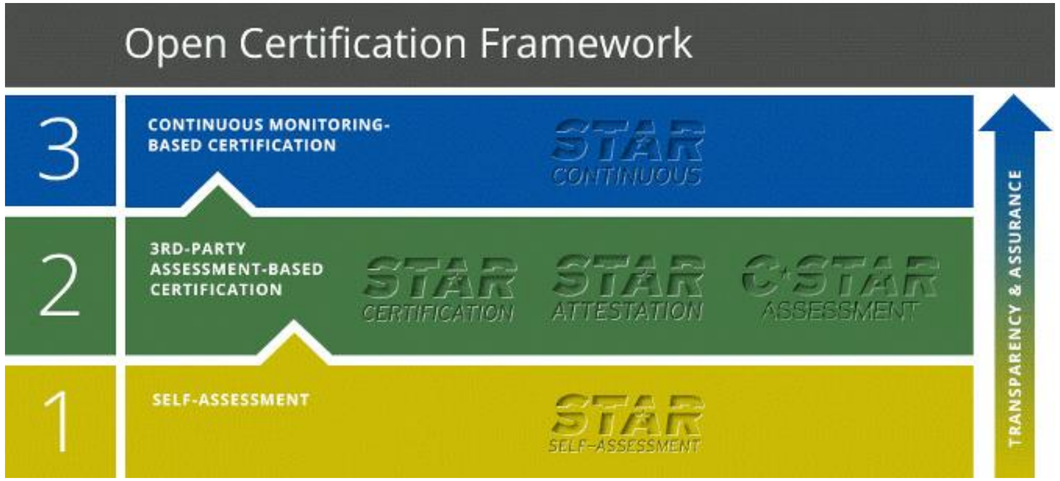
CAIQ Guiding Principles

The following are the principles that the working group utilized as guidance when developing the CAIQ:

- The questionnaire is organized using CSA 13 governing & operating domains divided into “control areas” within CSA’s Control Matrix structure
- Questions are to assist both cloud providers in general principles of cloud security and clients in vetting cloud providers on the security of their offering and company security profile
- CAIQ not intended to duplicate or replace existing industry security assessments but to contain questions unique or critical to the cloud computing model in each control area
- Each question should be able to be answered yes or no
- If a question can’t be answered yes or no then it was separated into two or more questions to allow yes or no answers.
- Questions are intended to foster further detailed questions to provider by client specific to client’s cloud security needs. This was done to limit number of questions to make the assessment feasible and since each client may have unique follow-on questions or may not be concerned with all “follow-on questions

CSA STAR: Security, Trust and Assurance Registry

- Public Registry of Cloud Provider self assessments
  - https://cloudsecurityalliance.org/star/#_registry
- Leverages GRC Stack Projects
  - Consensus Assessments Initiative Questionnaire
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
- Documents the security controls provided by various cloud computing offerings
- Encourage transparency of security practices within cloud providers
- Permanent effort to drive transparency, competition, innovation and self regulation with agility – crowdsourcing cloud security



Open Certification Framework

3 CONTINUOUS MONITORING-BASED CERTIFICATION — STAR CONTINUOUS

2 3RD-PARTY ASSESSMENT-BASED CERTIFICATION — STAR CERTIFICATION, STAR ATTESTATION, C-STAR ASSESSMENT

1 SELF-ASSESSMENT — STAR SELF-ASSESSMENT

TRANSPARENCY & ASSURANCE

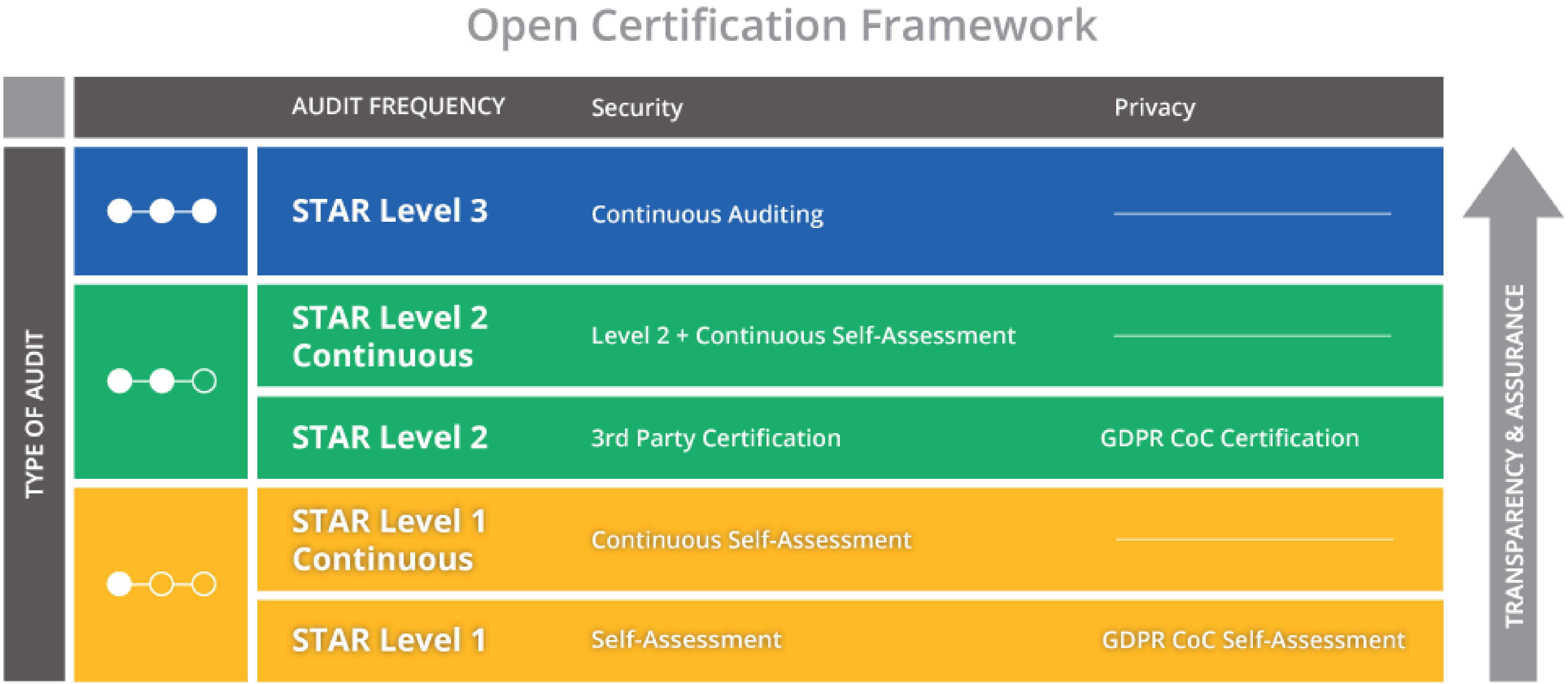
CSA STAR Assessment and Certification

CCM™ Cloud Controls Matrix

CAI™ Consensus Assessments Initiative

Open Certification Framework – Current Practice

https://cloudsecurityalliance.org/star/#star_m



Open Certification Framework

TYPE OF AUDIT

	AUDIT FREQUENCY	Security	Privacy
●–●–●	STAR Level 3	Continuous Auditing	—
●–●–○	STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment	—
	STAR Level 2	3rd Party Certification	GDPR CoC Certification
●–○–○	STAR Level 1 Continuous	Continuous Self-Assessment	—
	STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment

TRANSPARENCY & ASSURANCE

CSA STAR Compliance Levels

LEVEL ONE: CSA STAR Self-Assessment

- CSA STAR Self-Assessment is a free offering that documents the security controls provided by CSPs, thereby helping users assess the security of cloud providers
- Cloud providers either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), or to submit a report documenting compliance with Cloud Controls Matrix (CCM).

LEVEL TWO: CSA STAR Attestation

- CSA STAR Attestation is a 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 Cloud Controls Matrix.

LEVEL TWO: CSA STAR Certification

- The CSA STAR Certification is 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 Cloud Controls Matrix.

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.

Listing at https://cloudsecurityalliance.org/star/#star_m

STAR Listing Process

- Provider fills out CAIQ or customizes CCM
- Uploads document at /star repository
- CSA performs basic verification
    - Authorized listing from provider
    - Delete SPAM, “poisoned” listing
    - Basic content accuracy check
- CSA digitally signs and posts at /star
- Does not provide: automation, 3rd party assessment, relative/absolute scoring, real-time controls monitoring, etc
- Ultimate assurance is real time GRC (enabled by CloudAudit) complemented by CSA STAR and 3rd party attestation.

Why not certification or 3rd party assessment?

- Complex to do certification right
  - Many uses of cloud, many customer needs
  - Different risk profiles for each
- CSA is supporting broad industry consortia and standards bodies
  - ISO, ITU-T
  - Common Assurance Maturity Model (CAMM – 3rd Party assessment)
  - GRC Stack aligns with common requirements (e.g. PCI/DSS, HIPAA, FedRAMP, 27001, CoBIT, etc)
- Self assessment & transparency complements all
  - STAR could be part of SSAE 16 SOC II report (SAS 70 replacement)

Summary and take away

- Cloud compliance provides a basis for wider cloud services adoption and inter-cloud integration.
- Compliance is supported by numerous standards, legislation, regulatory guidelines and industry best practices that jointly define a compliance framework
  - Knowing major cloud compliance standards is necessary for correct cloud services design, deployment and operation

Additional materials

- Security and compliance standards

General standards and regulatory requirements related to security and privacy

General Regulatory Requirements for Cloud Compliance

- ISO/IEC 27001:2005 Certification on security infrastructure (http://www.bsigroup.com/en-GB/iso-27001-information-security/)
- Payment Card Industry Data Security Standard (PCI- DSS) and PCI DSS Cloud Computing Guidelines (https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf)
- NIST SP 800-144 Guidelines for Security and Privacy in Cloud Computing (http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf)
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

The major industry and government related documents:

- Service Organisation Control SOC 1 (SSAE 16/ISAE 3402) and SOC 2 and 3 (AT 101) (http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx), including
- Sarbanes Oxley Act (SOX, https://www.sec.gov/about/laws/soa2002.pdf) also known as "Corporate and Auditing Accountability and Responsibility Act"
- HIPAA/HITECH (The U.S. Health Insurance Portability and Accountability Act (HIPAA) and HITECH (Health Information Technology for Economic and Clinical Health) http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf)
- The Federal Information Security Management Act of 2002 (FISMA, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf)
- Federal Risk and Authorisation Management Program (FedRAMP) (http://www.gsa.gov/portal/category/102383)
  - Directory of Compliant Cloud Systems - http://cloud.cio.gov/fedramp/cloud-systems
- Department of Defense Information Certification Accreditation Process (DIACAP) (http://www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf)

Cloud Security and Big Data Security Standards and BCP

- Cloud Security Alliance https://cloudsecurityalliance.org/
  - Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2013) https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/
  - Expanded Top Ten Big Data Security and Privacy Challenges. CSA Report, 16 June 2013. https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf
  - CSA Enterprise Architecture: The Security and Risk Management domain. https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/
- European Union Agency for Network and Information Security
  - ENISA Cloud Computing Risk Assessment (2010) http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
  - ENISA Threat Landscape 2013, Overview of current and emerging cyber-threats, 11 December 2013 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport

- U.S.-EU Safe Harbor List, U.S. Government [online] http://www.export.gov/safeharbor/eu/eg_main_018365.asp
  - U.S.-EU Safe Harbor Framework Documents [online] http://www.export.gov/safeharbor/eu/eg_main_018493.asp