Cloud Security and Cloud Compliance

Cloud Security Services and Mechanisms:

How can modern clouds provide secure and trusted environment for data and business applications?

Yuri Demchenko
Complex Cyber Infrastructure Group
SNE, University of Amsterdam

5 March 2020

Outline

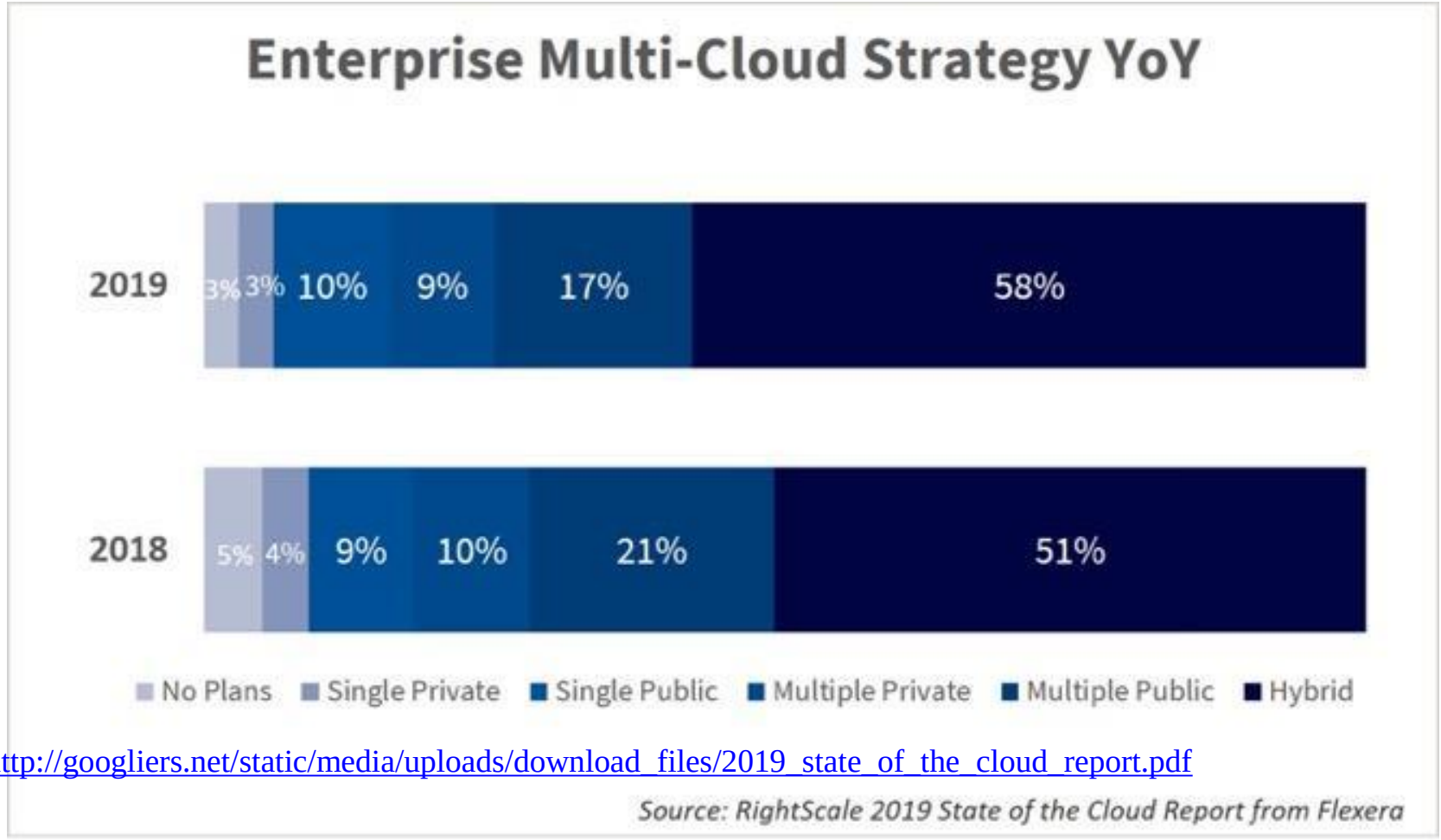
- Introduction: Cloud adoption is growing
- Shared Responsibility Security Model in Cloud
- Case Study: AWS Security
- Cloud Compliance and Cloud Security Alliance (CSA)
  - CSA GRC Stack: Governance, Risk Management and Compliance
  - Consensus Assessment Initiative Questionnaire (CAIQ)
- Example CAIQ Excel workbook

Optional

- DevSecOps = DevOps + SSDL (Security Services Development Lifecycle)
- Case Study: Trusted Data Market infrastructure and IDS Connector
- Discussion: Research topics in Cloud Security and Trust

Cloud Facts: Cloud adoption is growing

- Cloud adoption is growing: Enterprise Cloud Strategy 2019



http://googliers.net/static/media/uploads/download_files/2019_state_of_the_cloud_report.pdf

Cloud Observations

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

- Cloud is an ultimate platform for Big Data
  - Data gravity vs Investments gravity
    - Migration choice: 10 yrs of legacy data vs expected explosive data growth
  - Working with data and data analytics in cloud is much easier
    - Hybrid cloud and data analytics solution is growing
    - **Data Lakes**: heterogeneous data formats, namespaces, filesystems
- Migration to cloud takes 1-2 years, requires competent planning (new staff competences required)
  - Demand for cloud migration/integration services/companies
  - Growing adoption of the DevOps culture in services development and operation
- Most of new projects are on cloud

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/customer controlled access control (security) infrastructure
    - Provide sufficient amount of security controls for competent user
- Security services are provisioned **on-demand** (as part of virtualised infrastructure) and require **bootstrapping (federation)** with the customer services and trust domain

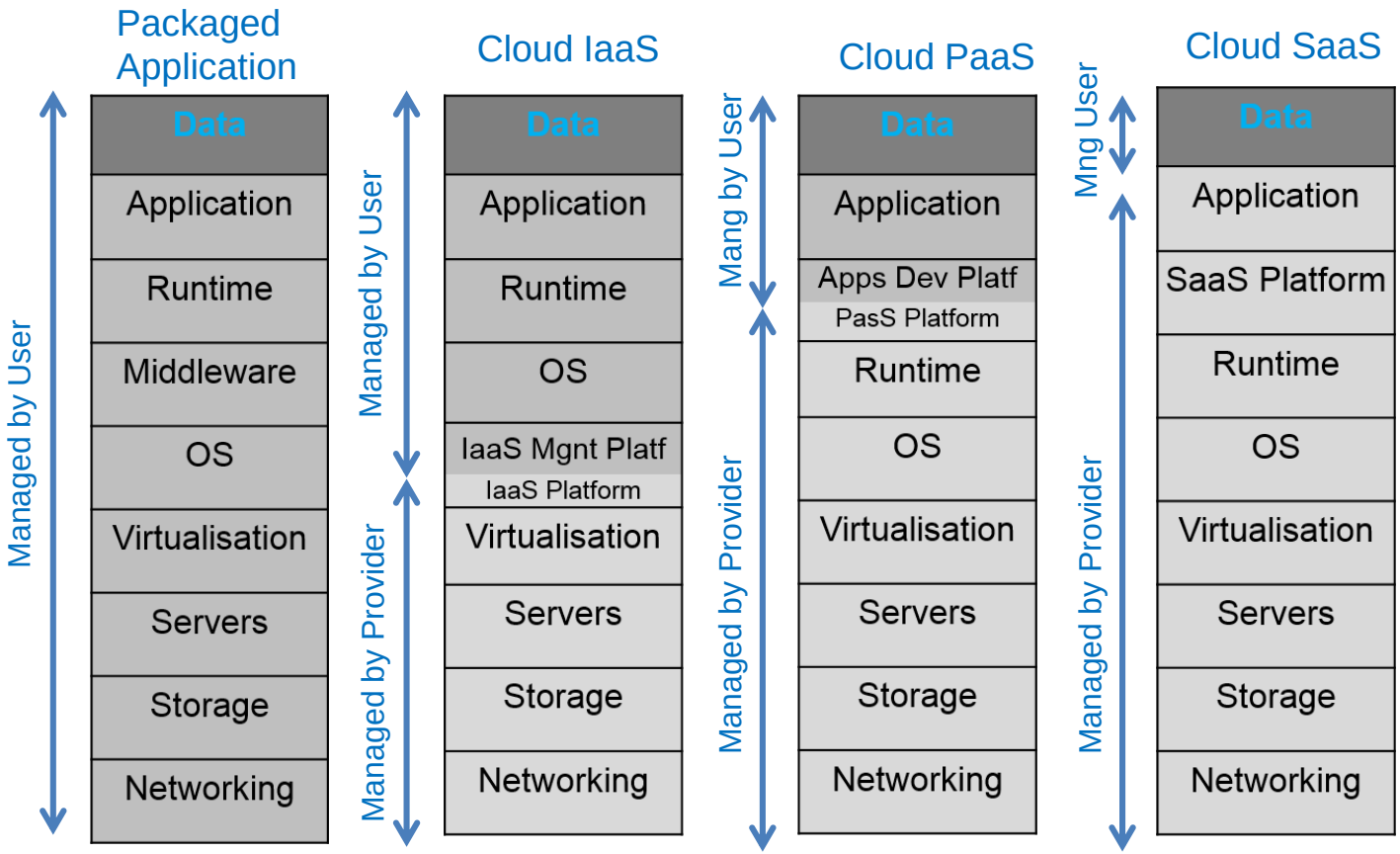
Adopting Public Cloud – Security Practices

- **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.

Part 1: Cloud Security and AWS Example

- Shared responsibility model
- AWS Security

Split of Responsibilities in Cloud IaaS, PaaS, SaaS



Data is always responsibility of Customer

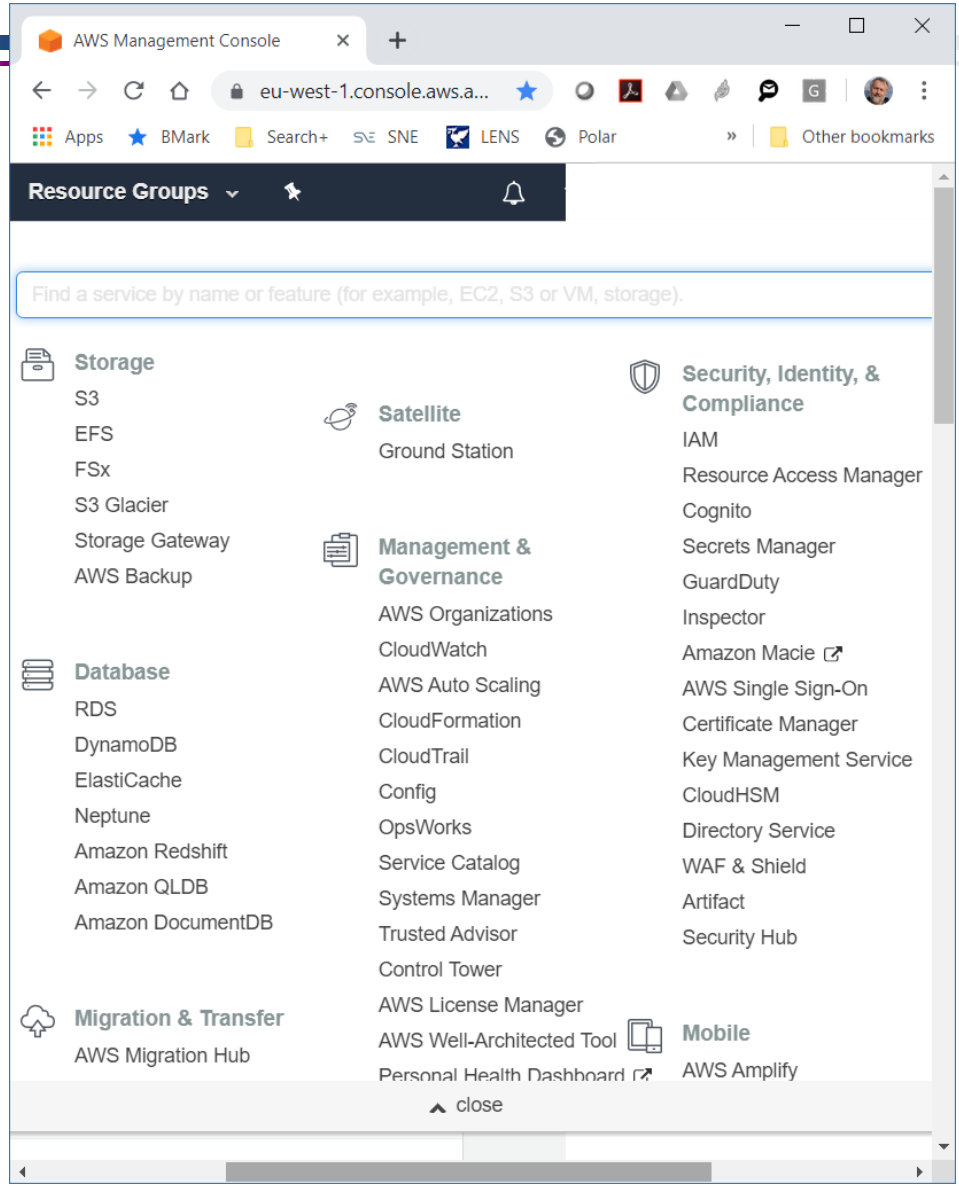
Cloud Provider provides tools for assisting customers in secure deployment, operation and testing

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

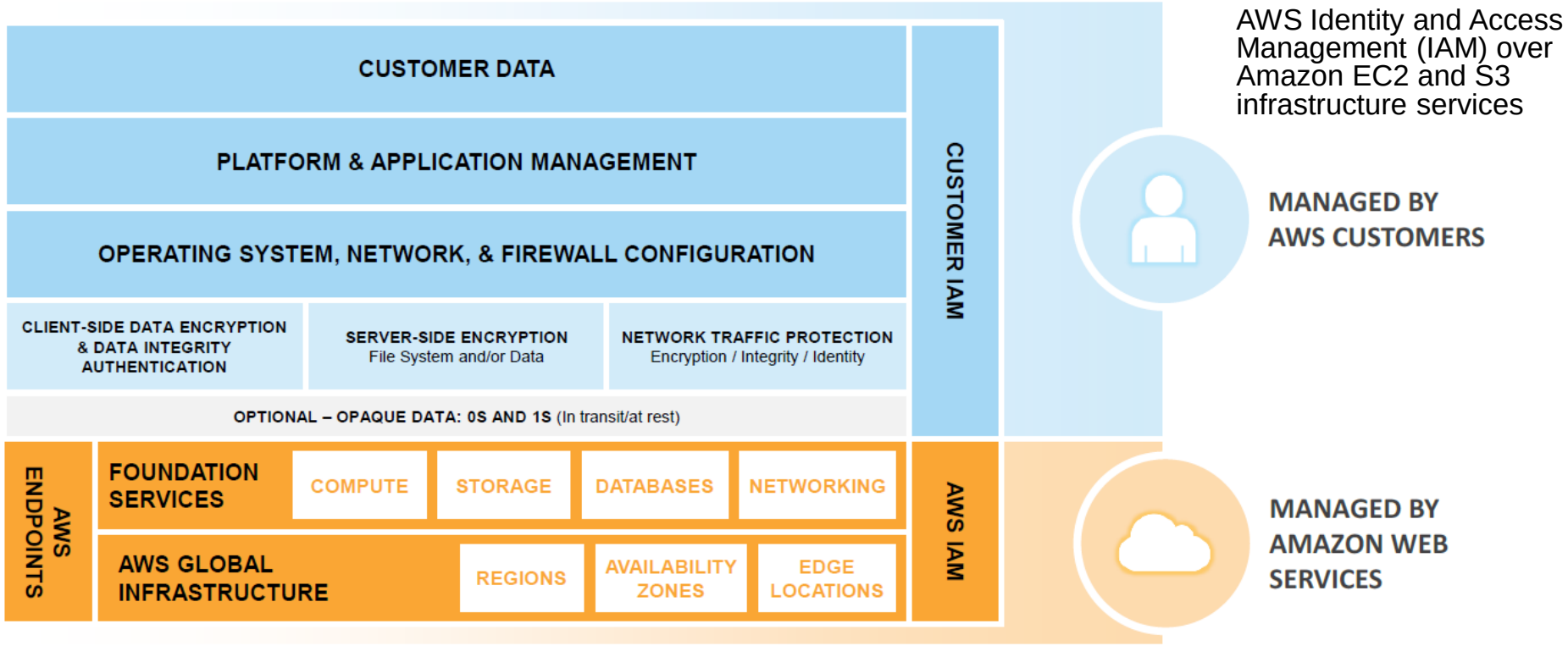
- Updating firmware and software for platform and for customer managed components
- Firewall is intrusion prevention and a responsibility of the cloud provider
- Certification and compliance of the cloud platform doesn't imply security and compliance of the customer controlled components

Case Study: AWS Security Mechanisms

- VPC – Virtual Private Cloud
  - VPN – Virtual Private Network
    - Private and Public subnets
  - VPG – VPN Private Gateway
  - IGW – Internet Gateway
- HTTPS and TLS/SSL, SSH, KPI
- AIM – Access and Identity Management
- Other security services
  - AWS SSO
  - Cognito – Identity Federation
  - Macie - Data visibility security service
  - CloudHSM - Managed hardware security module (HSM)



Example: Security responsibility sharing in AWS IaaS infrastructure services

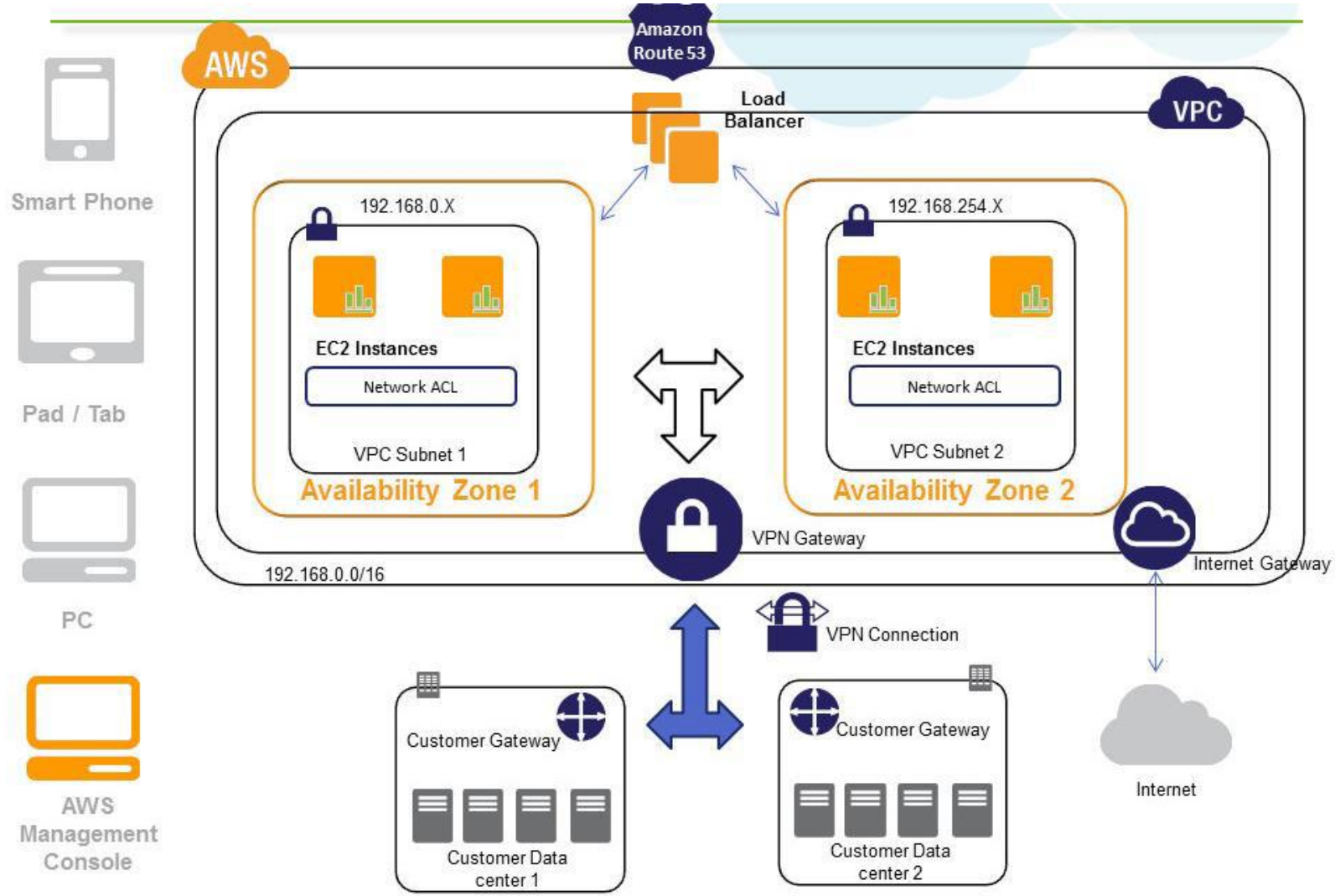


- For other cloud service models PaaS and SaaS the responsibility of AWS goes up to OS, network and firewall for PaaS, and also includes the application platform and container for SaaS.
  - However, the responsibility for data remains with the customer.

[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

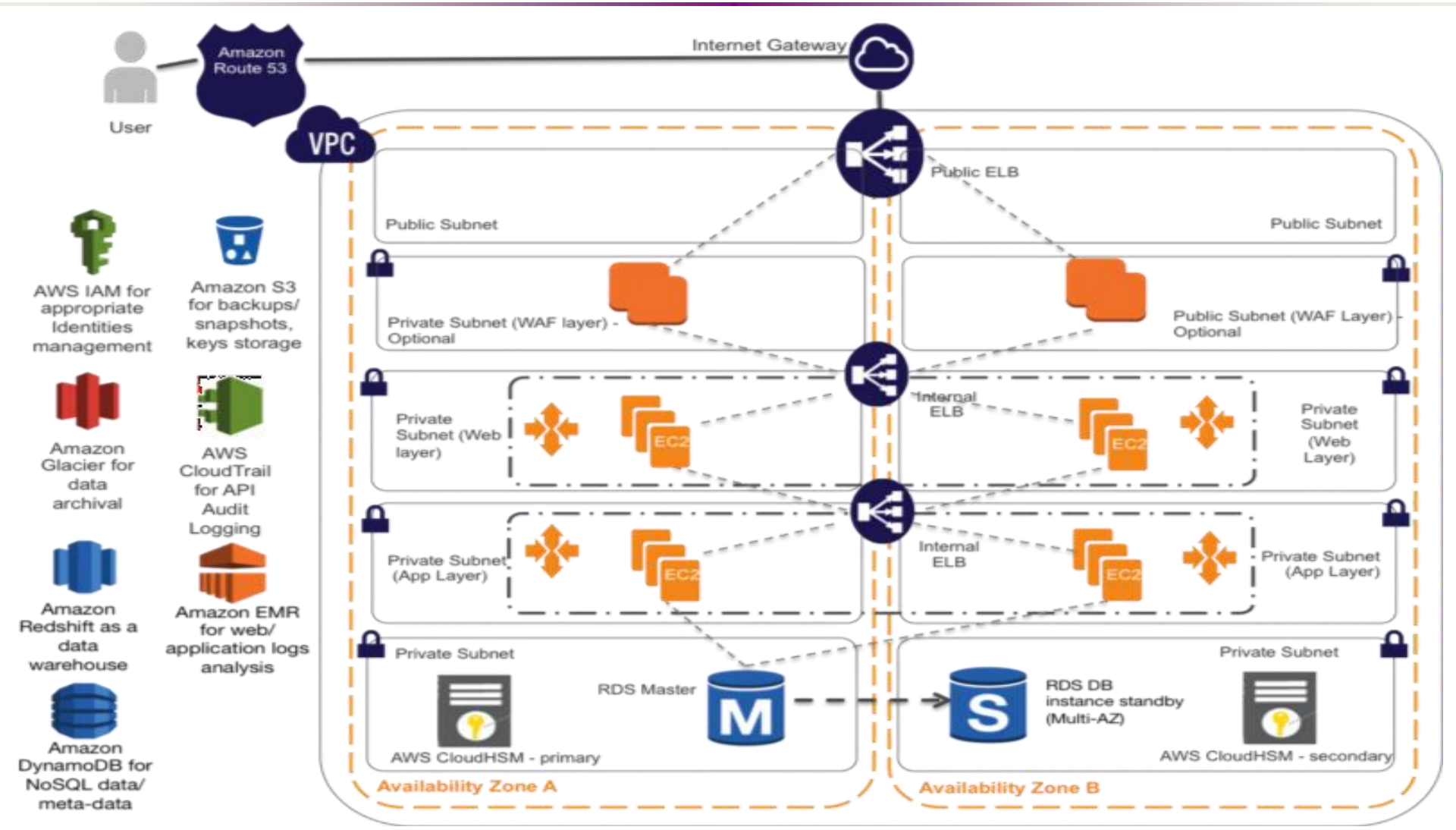
AWS VPC Structure

Spanning Availability Zones but Limited to Region

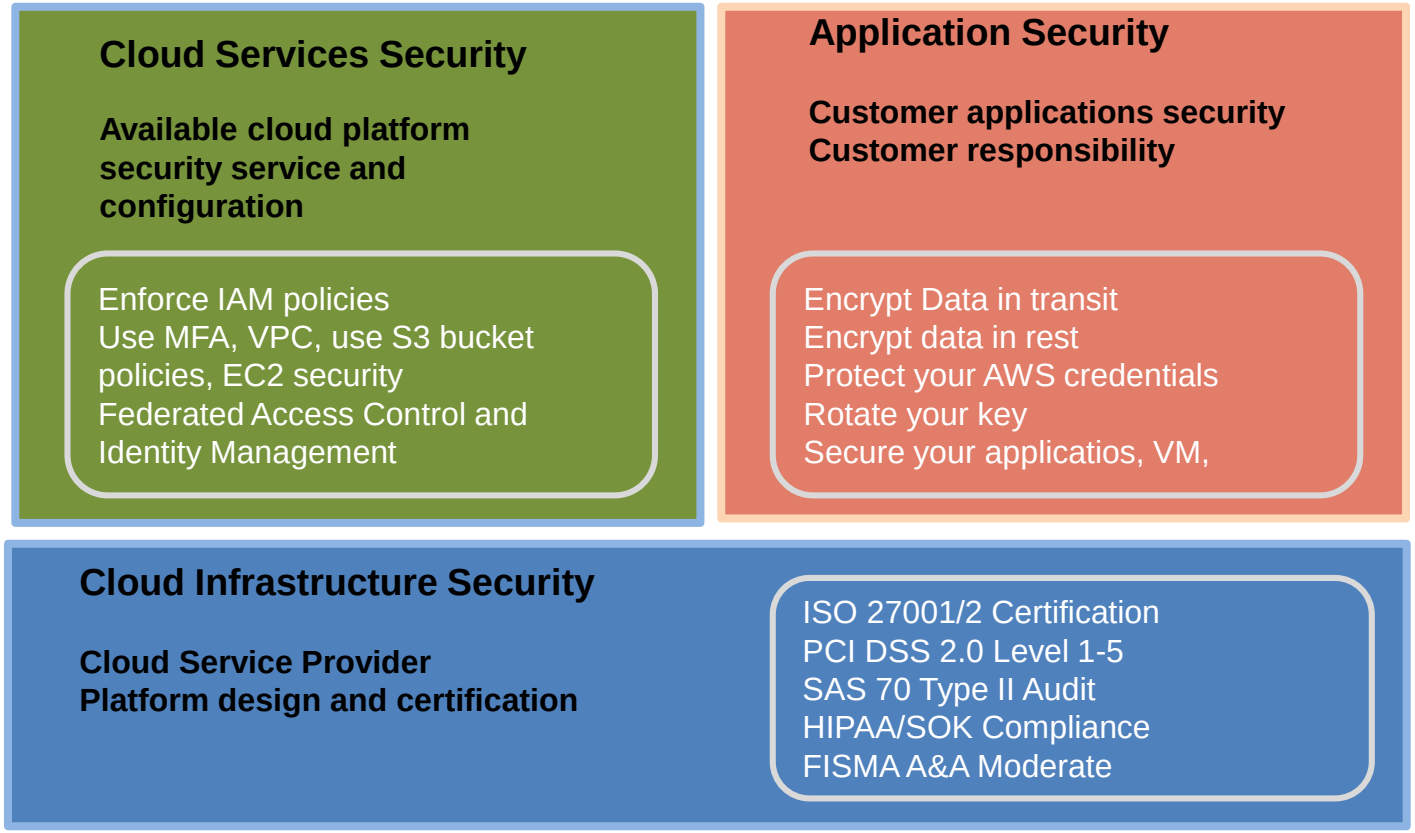


Example: Architecting Healthcare Application for HIPAA Compliance: VPC and Multiple Private Subnets

https://aws.amazon.com/blogs/startups/architecting-your-healthcare-application-for-hipaa-compliancepart-1/



Amazon Web Services Security Model



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.

Part 2. Cloud Compliance

- Compliance standards, Security Controls
- CSA GRC Stack: Governance, Risk Management and Compliance
- Compliance Assessment Initiative Questionnaire (CAIQ)

Security and Compliance

- Security and compliance are related and in some cases interchangeable
- **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 – Example 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 Criteria
- 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
- GDPR (General Data Protection Regulation)

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

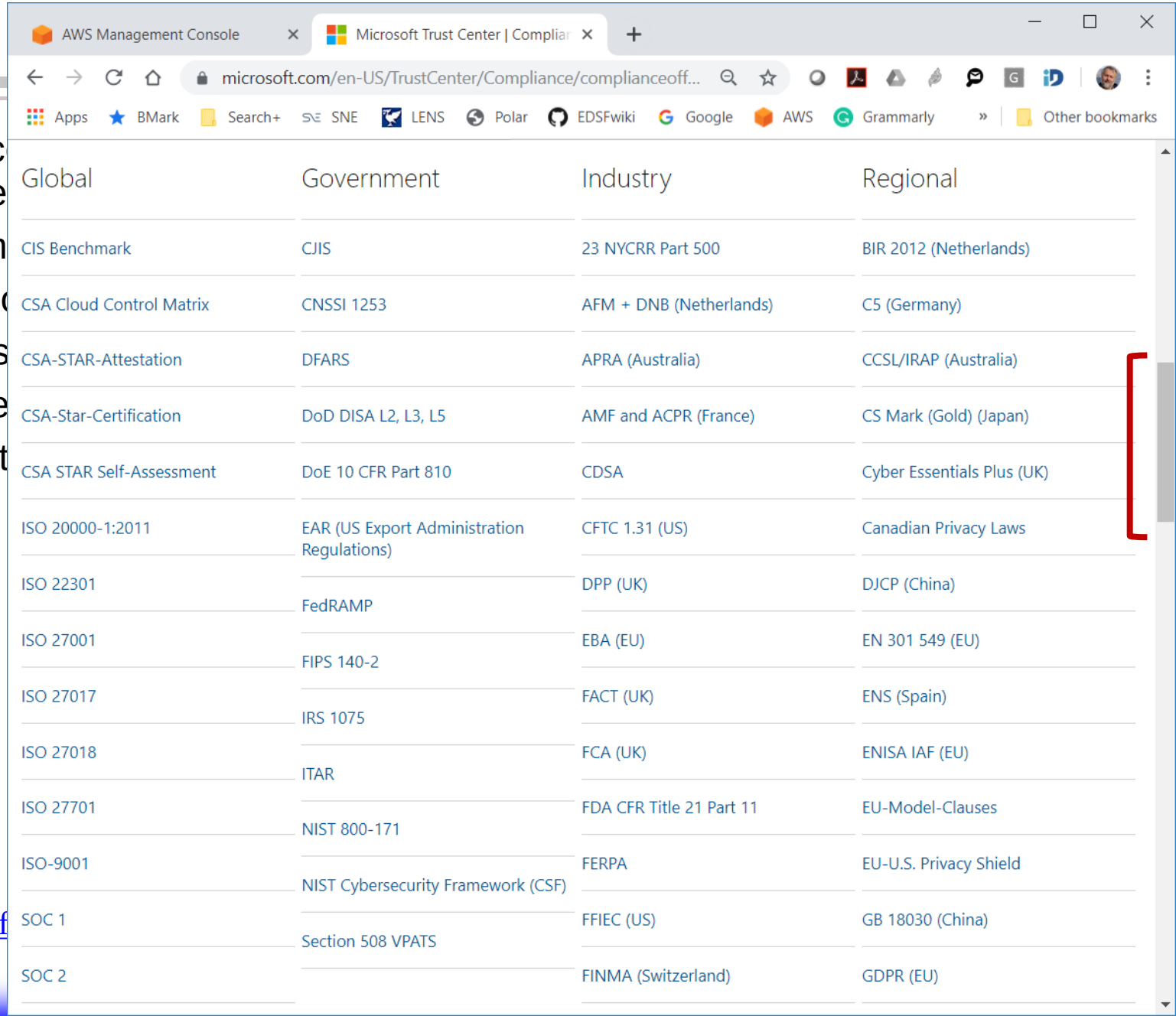
http://aws.amazon.com/compliance/

Case study: Compliance by Microsoft Azure

Microsoft servic
and compliance

- Current com
- Office 365 c
- Service Trus
- Microsoft Se
- Audit Report

https://www.microsof



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		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		• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
Pre-audit checklists and questionnaires to inventory controls		Consensus Assessments Initiative (CAI) • Industry-accepted ways to document what security controls exist
The recommended foundations for controls		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

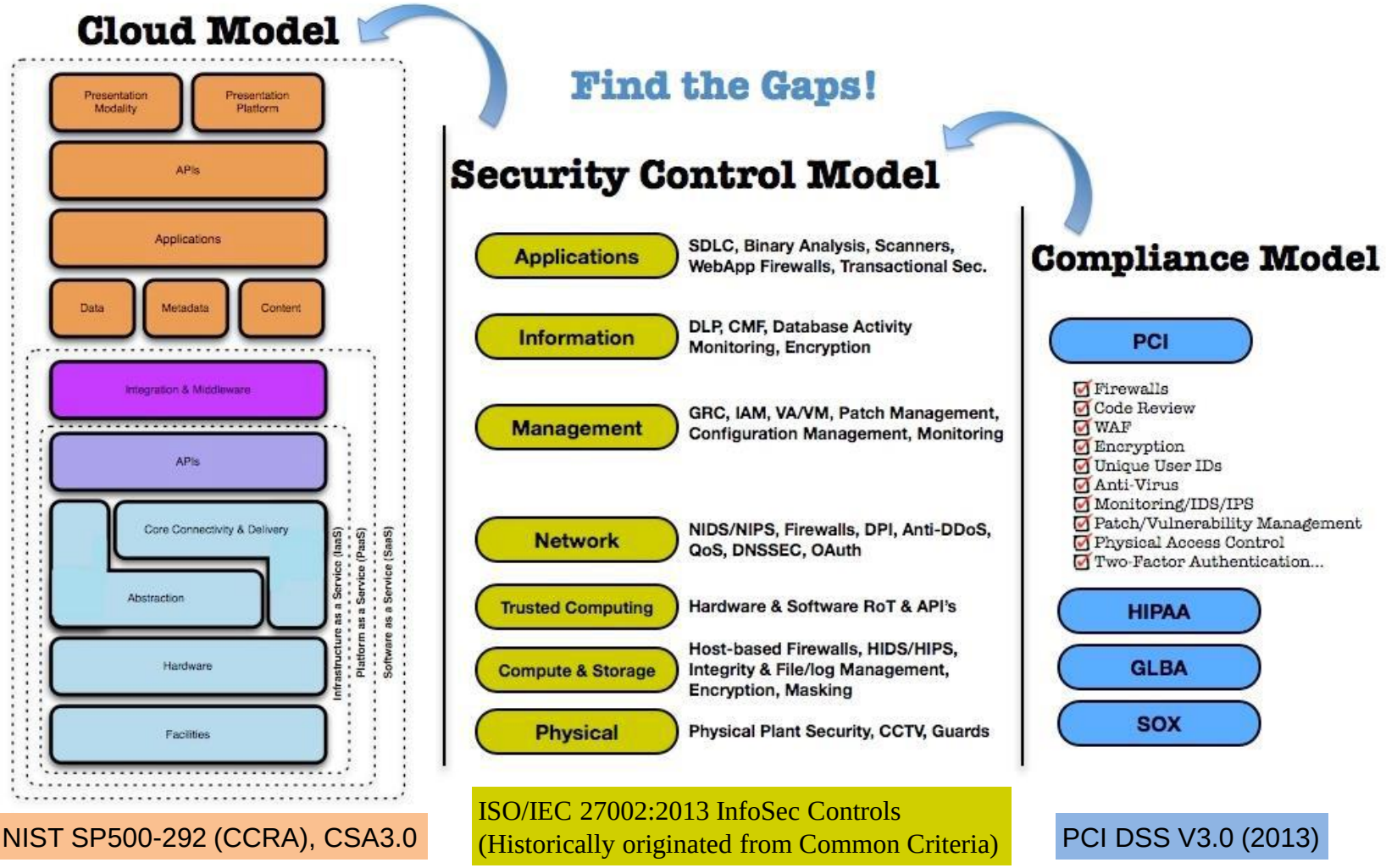
Cloud Security Alliance (CSA) GRC Stack: Governance, Risk Management and Compliance

The GRC Stack provides a toolkit for enterprises, cloud providers, security solution providers, IT auditors and other stakeholders to assess both private and public clouds against industry established best practices, standards and critical compliance requirements. https://cloudsecurityalliance.org/research/grc-stack/

- **Cloud Controls Matrix (CCM)** is designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider (https://cloudsecurityalliance.org/research/ccm/)
  - The CCM gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains
  - Defined in accordance to industry-accepted security standards, regulations, and controls frameworks such as the HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI, HIPAA and NIST.

- **Consensus Assessments Initiative Questionnaire (CAIQ)** provides an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency (https://cloudsecurityalliance.org/research/cai/)
  - Provided in a form of questionnaire in the spreadsheet format, a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.
  - ~ 200 yes/no questions that map directly to the CCM, and thus, in turn, to many industry standards.
  - **CAIQ answers by companies and certification are posted on the STAR website**
    - From self-assessment to certification and monitoring

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



NIST SP500-292 (CCRA), CSA3.0

ISO/IEC 27002:2013 InfoSec Controls
(Historically originated from Common Criteria)

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/

CSA3.0 Security Guidance for Critical Area of Focus in Cloud Computing – Cloud Controls Matrix (CCM)

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

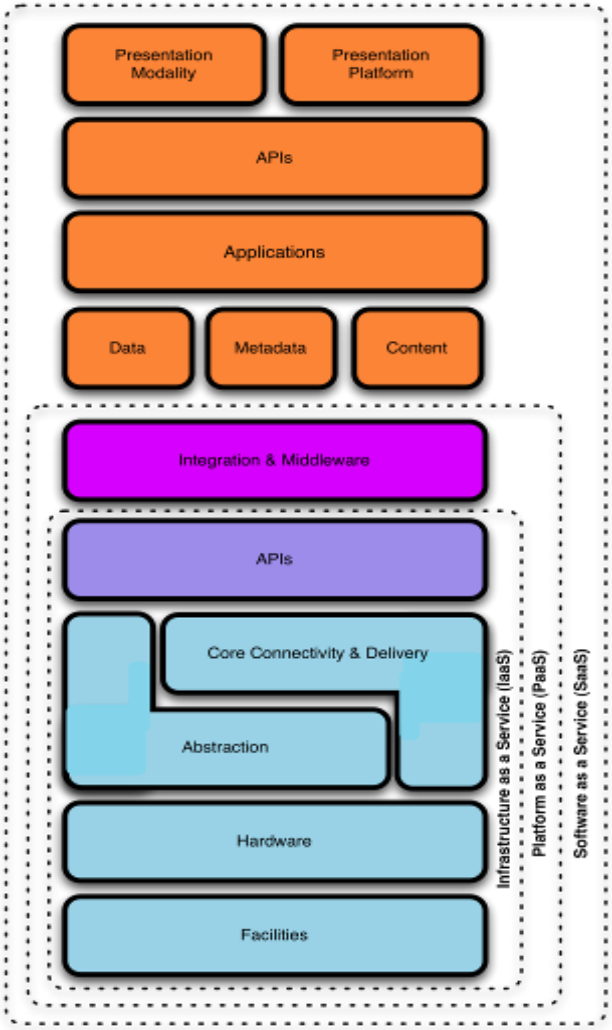
Governance domains

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



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, v3.1 updated in 2020

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

Recent CSA Publications

- **Top Threats to Cloud Computing: The Egregious 11 (2019)**
  - Contains stories about recent cloud breaches: all due to customer lame design and compromised credentials
- Top Threats to Cloud Computing: Deep Dive (2019)
  - A case study analysis for The Treacherous 12 Top Threats to Cloud Computing and relative industry breach analysis
- The Six Pillars of Security (2019)
  - Achieving Reflexive Security through integration of security < development and Operations
- Cloud Octagon Model (2019)
  - Model for Improving Accuracy and Completeness of cloud Computing risk assessment
-

Part 3. Demonstration: CSA CAIQ and PCI SAQ

Cloud Compliance Assessment tools

- CSA CAIQ and PCI DSS Dashboard
  - CSA Cloud Controls Matrix (CCM) v3.0.1

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

    https://downloads.cloudsecurityalliance.org/initiatives/ccm/ccm-v3.0.1.zip
  - CSA Consensus Assessment Initiative Questionnaire (CAIQ) v3.0.1

    https://cloudsecurityalliance.org/research/cai/

    https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/

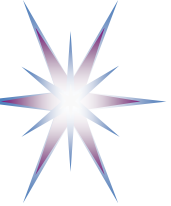
- PCI DSS Self Assessment Questionnaire (SAQ)
  - https://www.pcisecuritystandards.org/document_library?category=saqs#results
  - Questionnaire is designed for different categories of user: from full outsourcing cards operations to card payment service

Research topics in Cloud Security

- Federated Identity Management and Access Control in hybrid enterprise-CSP infrastructure + Identity provisioning
- Cloud Access and Security Brokers: Security with Trusted Third Party
- VPC infrastructure security model and analysis
- Bootstrapping cloud based VPC and enterprise or applications trust domains
  - Leveraging Zero Trust model in networking security
  - Leveraging TPM and Trusted Computing Platform Architecture
- Data protection in clouds at all stages of data processing (Data Lifecycle)
  - Data Sovereignty and Data Ownership attribute/property
  - Computationally Enforceable Policies and data provenance: Mapping to CCM/CAIQ
  - Data Management Infrastructure for AI and Digital Twins
  - Blockchain enabled data provenance in multi-platform multi-cloud environment
- Personal information protection in cloud based multitenant multi-tier applications
- Cloud infrastructure to enable GDPR + FAIR data principles

Summary and take away

- Cloud Security impose new security challenges
- Cloud Security is based on the core security principles and models
- Shared responsibility is the basic model cloud security
- 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
  - CCM and CAIG provide bridge between technical and legal/regulatory domains
- IDSA architecture and Trusted Data Market as example of critically trusted environment in cloud



Discussion and Questions

Additional information

- IDS Connector and LUCON details
- CSA Big Data Security Top Ten

Measures to ensure security in Cloud

- DevSecOps
- Cloud Security Configuration Monitoring
- Example: Trusted Data Market
- IDS Connector Security Model
- LUCON – IDS Implementation

DevSecOps and SSDL

- SSDL – Security Services Development Lifecycle
  - Developed by Microsoft in 2000s and widely accepted by industry

SSDL = Security and Privacy by Design

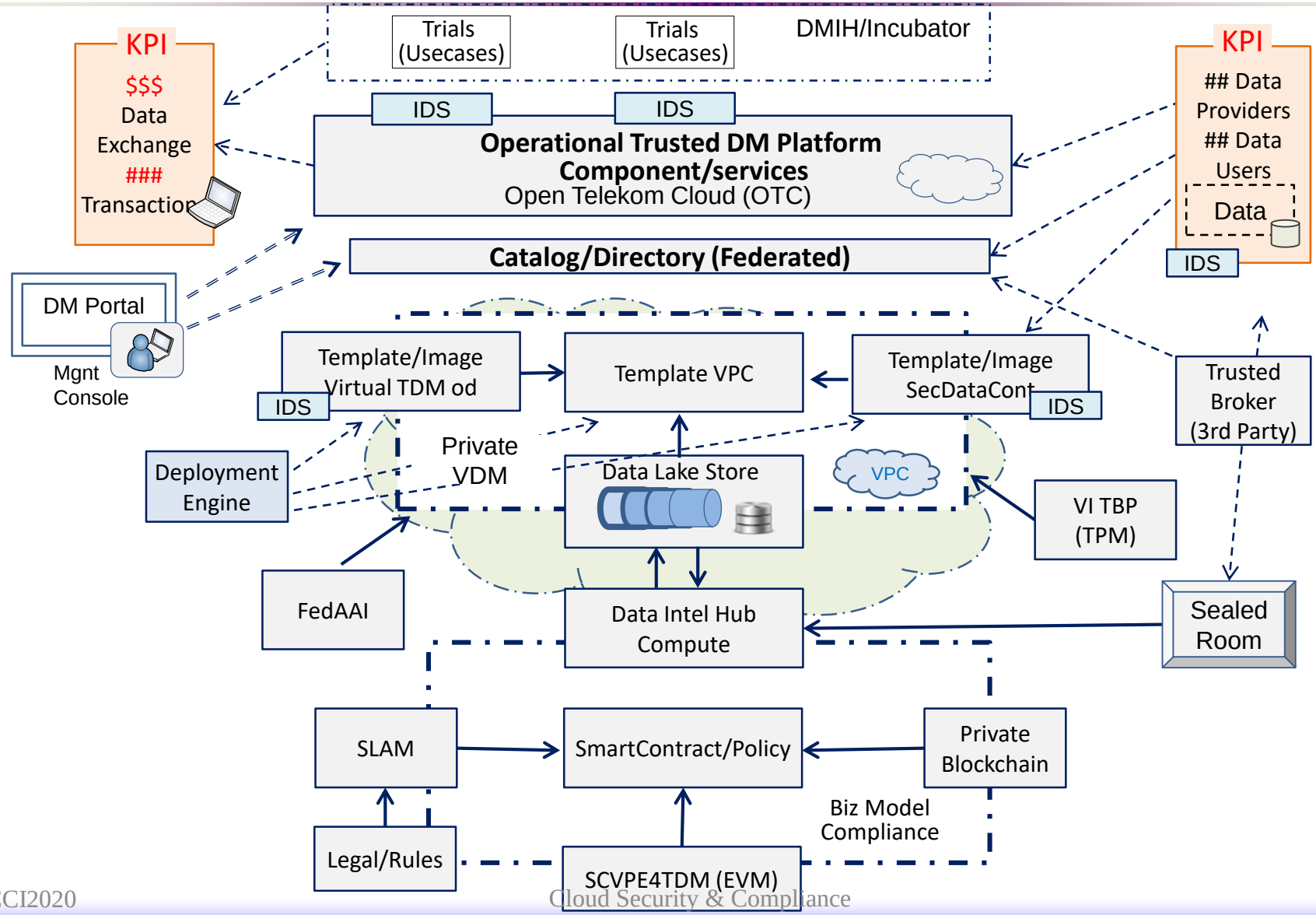
- Security design principles by big software vendors Amazon, Apple, Google

- DevOps meets Security -> DevSecOps
- DevSecOps as alternative to Waterfall model where security is treated as non-functional requirement and is addressed at later stages of development

Cloud Security Configuration Monitoring

- AWS Tools
  - AWS Config – Monitor configuration changes
  - AWS CloudTrail - Create a trail to retain a record of events
  - Amazon Inspector - analyzes the behavior of AWS resources and helps identify potential security issues
  - Amazon GuardDuty – Activity monitoring & Intelligent threat detection
- Third party tools
  - https://www.threatstack.com
  - https://www.alienvault.com
  - https://evident.io – multicloud solution
- InSpec is compliance as code service https://www.inspec.io
  - Turns compliance, security, and other policy requirements into automated tests
  - Includes compliance requirements into code

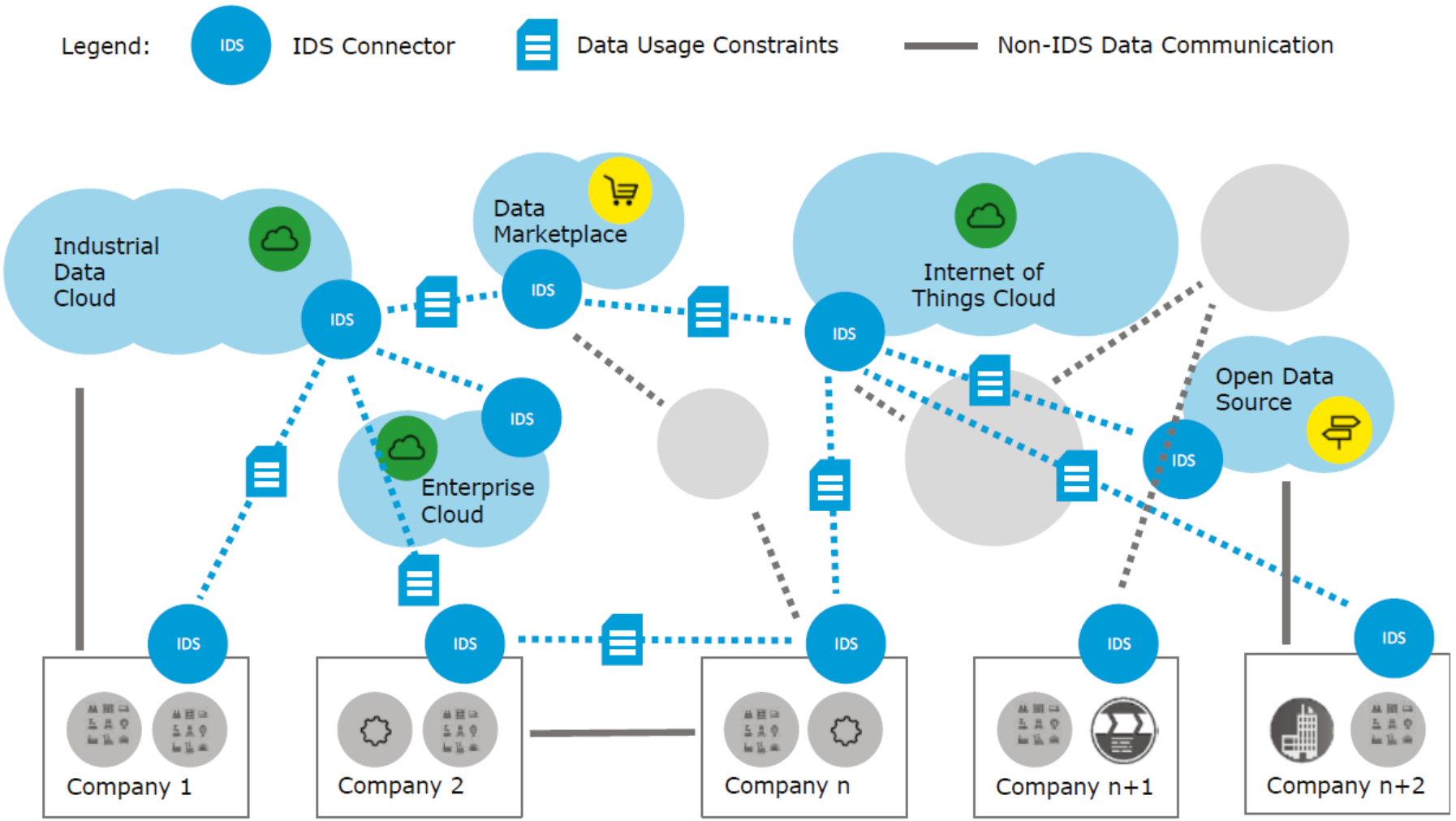
Case Study: Trusted Data Market Infrastructure and composable components



TDM Infrastructure Templates and DevOps tools

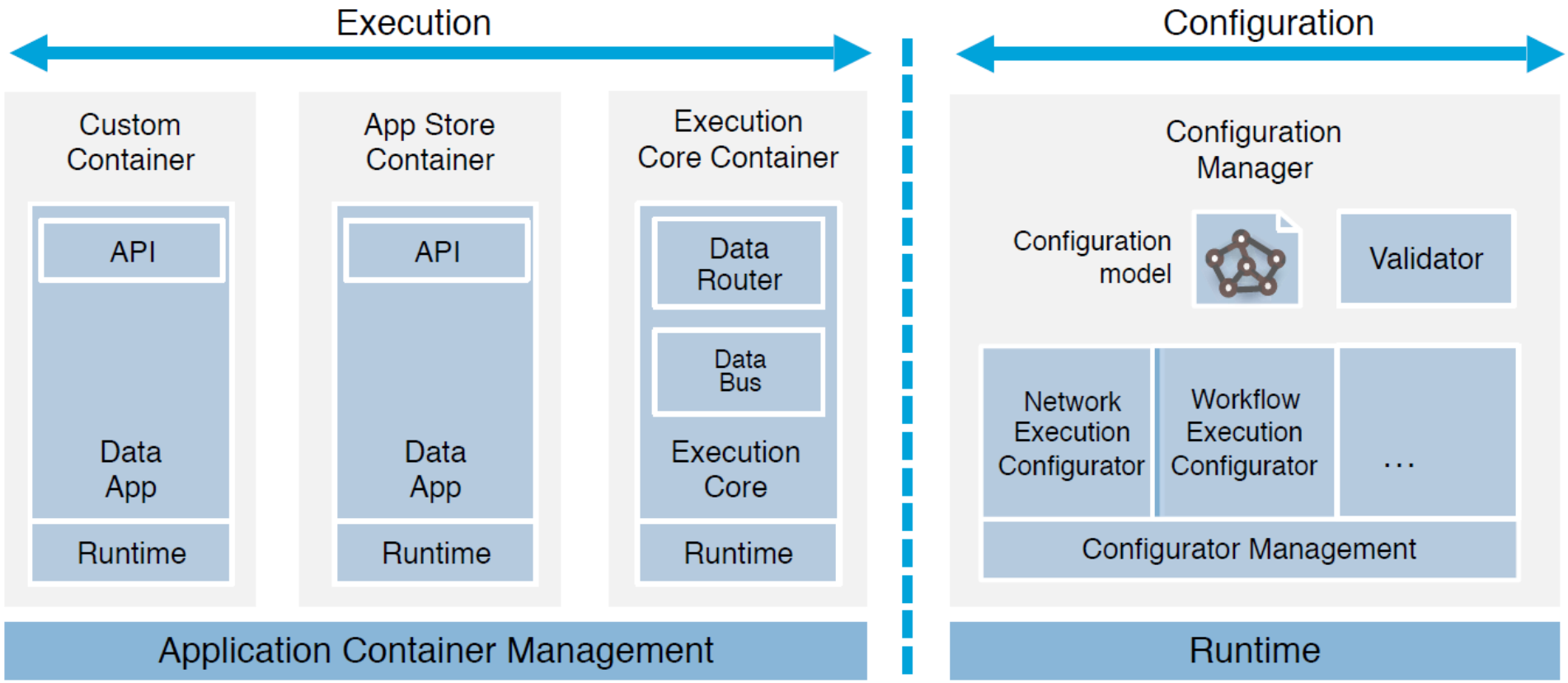
- DM infrastructure is provisioned on demand for each cooperating groups of partners
  - Digitally Enforceable Policy/Contract is embedded into infrastructure
- DM infrastructure template is composed of basic infrastructure patterns described
  - For platform dependent patterns in the formats of cloud platform
    - AWS: CloudFormation
    - Azure: Azure Resource Manager (ARM)
  - For general infrastructure descriptions/templates
    - Ansible – YAML based, combines computational and network resources
    - Others: Chef (directly supported by AWS), Puppet, Terraform (directly supported by Azure)
  - Blockchain enabled Virtual Private execution Engine (SCVPE)

Leveraging IDS Architecture and Connector with Cloud



- IDS Connector is the main functional component
- No specifically defined infrastructure

Reference Architecture Data Connector

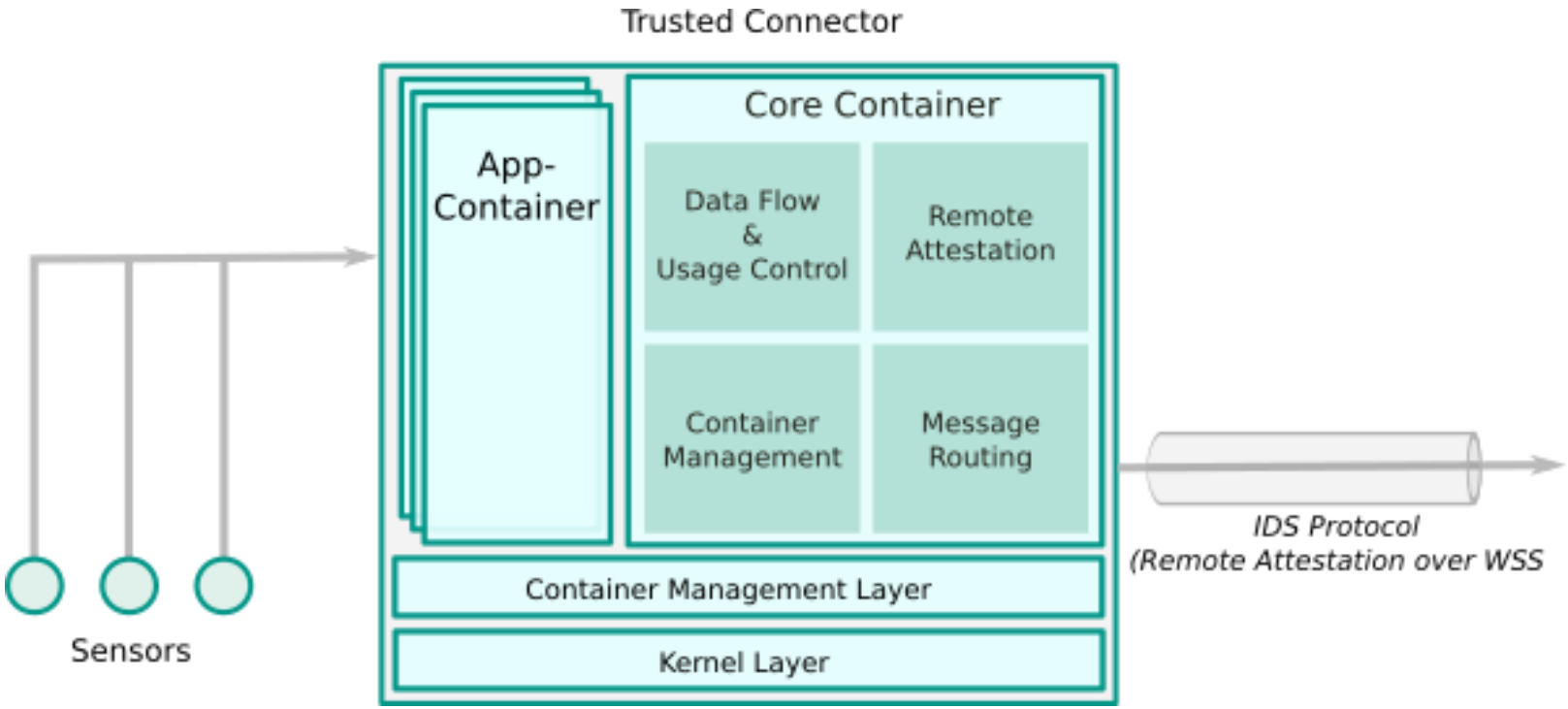


- Execution and configuration
- Application container

- Already DIN Standard 2020

LUCON: Trusted Connector Implementation

https://industrial-data-space.github.io/trusted-connector-documentation/

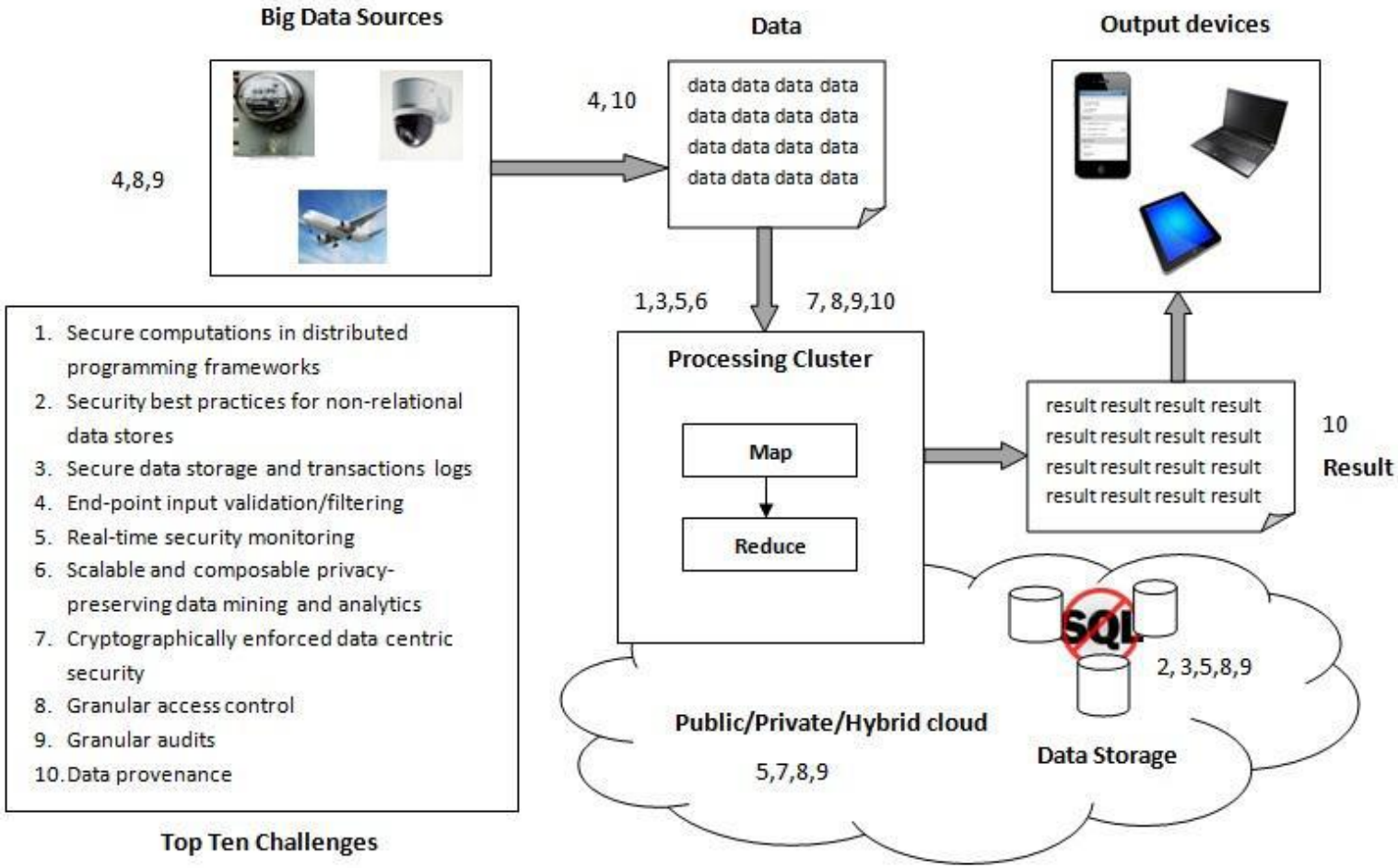


- The Trusted Connector features the secure container management layer *trust|me* as an alternative to Docker.
- trust|me basic mechanisms are similar to Docker (namespaces, cgroups and chroot)
- trust|me was developed as a security architecture including secure boot, platform integrity measurements, and a hardened kernel.

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



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

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:

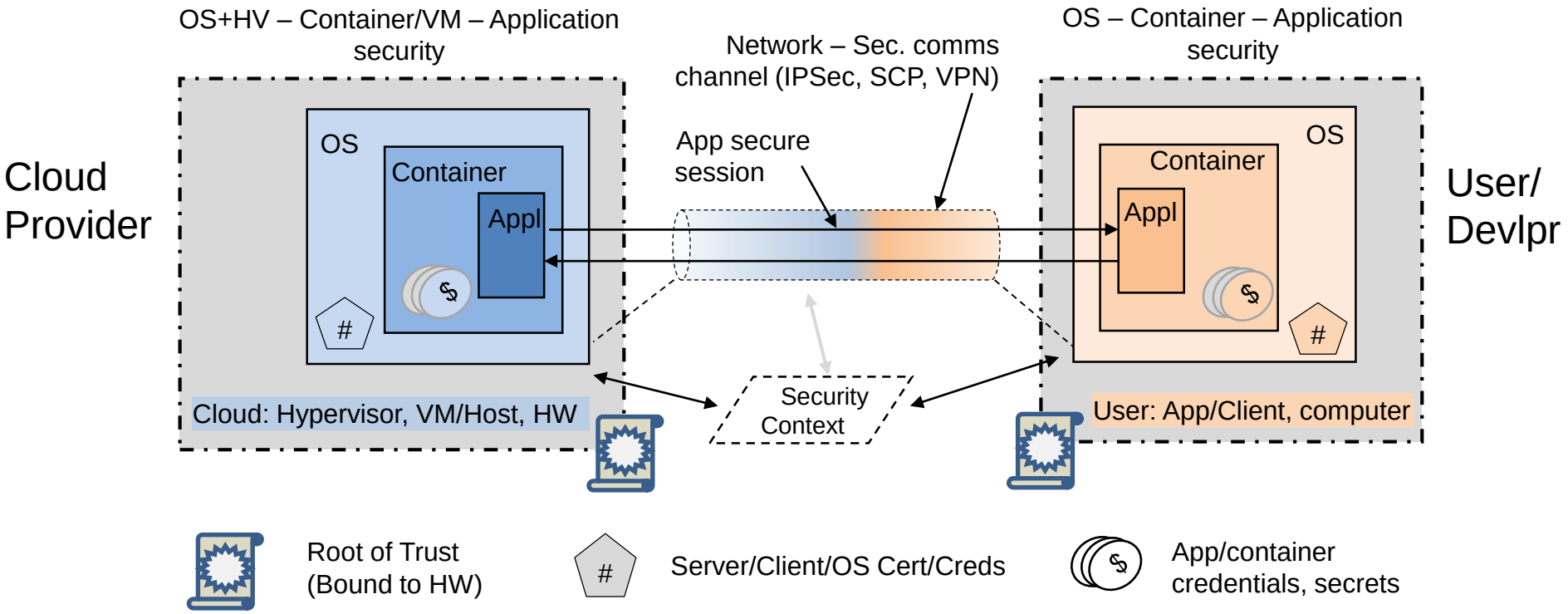
A. Infrastructure security
- TT01. Secure computations in distributed programming frameworks
- TT03. Secure data storage and transactions logs
- TT04. End-point input validation/filtering
- TT05. Real-time security/compliance monitoring

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***

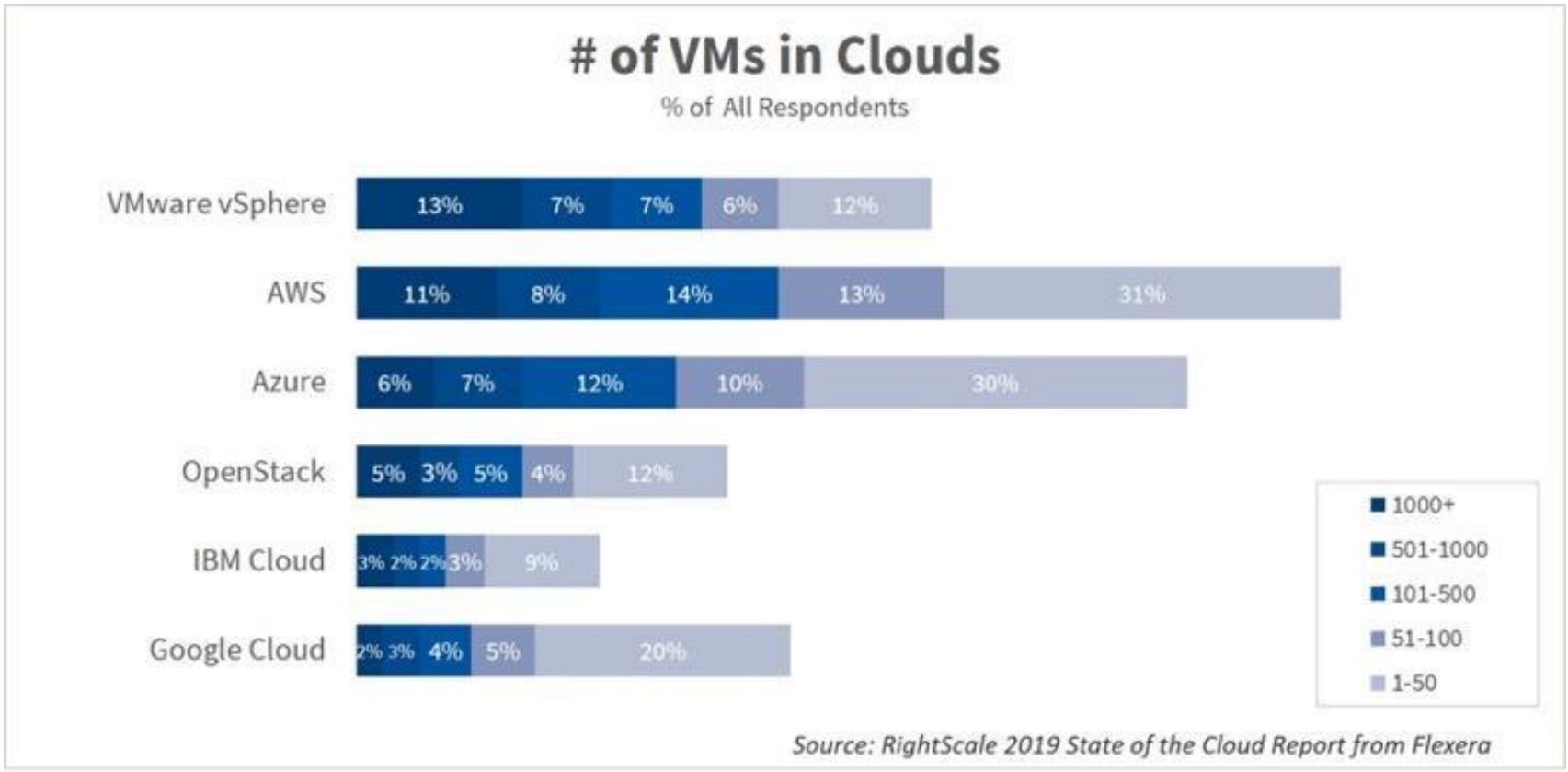
D. Data Management
- TT09. Granular audits
- TT10. Data provenance

Cloud, OS, Network and Applications Trust Layers



- 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 Facts and Observations: AWS vs Azure



- Microsoft Azure is fastest growing cloud: now 85% of AWS (compare 70% in 2018)
- Quite popular in Netherlands