



## APC2018 Panel

# Technological foundation of GDPR: Technologies, practices and challenges

### Panel members

Yuri Demchenko (moderator), University of Amsterdam  
Cees de Laat, System and Network Engineering, University of Amsterdam  
Matthijs Koot, Secura BV  
Marcel Schaefer, SIT Fraunhofer  
Christian Winter, SIT Fraunhofer  
Anna Krasnova, Ernst & Young

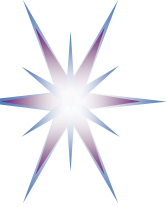


APC2018 Panel  
(Panel of GDPR Skeptics)  
7 October 2018

Technological foundation of GDPR:  
Technologies, practices, challenges, feasibility

Panel members

Yuri Demchenko (moderator), University of Amsterdam  
Cees de Laat, System and Network Engineering, University of Amsterdam  
Matthijs Koot, Secura BV  
Marcel Schaefer, SIT Fraunhofer  
Christian Winter, SIT Fraunhofer  
Anna Krasnova, Ernst & Young



# Panel: Technological foundation of GDPR: Technologies, practices and challenges

- Most of modern online and social media applications and platforms have been developed without
  - primary focus on personal data protection and
  - enforcement of strong ethical norms present in real world and human relations.
- GDPR imposes new-old technology challenges
  - No clear commonly accepted view on for existing and emerging technologies
  - Privacy by design declared but no technical approach proposed
- Close discussion and cooperation between technical experts, policy makers and legal experts, and may require changes in all involved domains.
- Involving audience into discussion



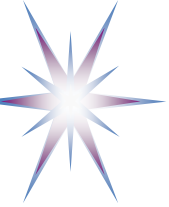
# Panel Discussion Topics

- Trusted data processing platforms and implementation problems, in particular, when using modern Big Data Analytics platforms and emerging AI tools
- What can blockchain offer for data protection and policy enforcement?
- What data need to be protected and what data protection is challenging?
- Importance of Data and Digital literacy in effective data protection. Ethical code of conduct for future IT professionals
- European projects and initiatives on data protection technologies
- Recent (big) privacy breaches: technological aspects analysis and observations



# Track 10 Sessions 1 and 2 - Overview

- GDPR implementation (full/literate) provides challenges for current technology of Big Data and modern Data Analysis methods
  - In particular, with the current Big Data and Analytics technologies
  - GDPR2.0 to come
- Privacy by Design
  - Privacy Design Strategies by Jaap-Henk Hoepman (2013)
- Blockchain and privacy
  - Many illusions and frictions with GDPR (by Chantal Bompezzi)
  - Not designed for privacy
- Dialog between ICT and users/citizens
  - Literacy for citizens and understanding by IT “crowd”
    - SamenBeter by Winfried Tilanus - <https://www.samenbeter.org/>
  - EU Report Digital Competences for Citizens (DigComp, 2017)



# Panel Members

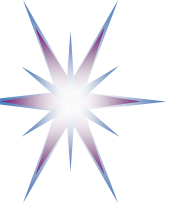
- Yuri Demchenko (moderator), University of Amsterdam
- Cees de Laat, System and Network Engineering, University of Amsterdam
- Matthijs Koot, Secura BV
- Christian Winter, SIT Fraunhofer
- Marcel Schaefer, SIT Fraunhofer
- Anna Krasnova, Ernst & Young



# Introduction to Panel

## “Technological foundation of GDPR”

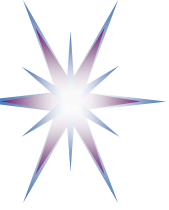
- Track 10 Sessions 1 and 2 – Overview
- Cloud and Big Data security and compliance
- GDPR and technological challenges
  - Different approaches in Europe and US, US-EU Privacy shield



# Technical Introduction to Panel

---

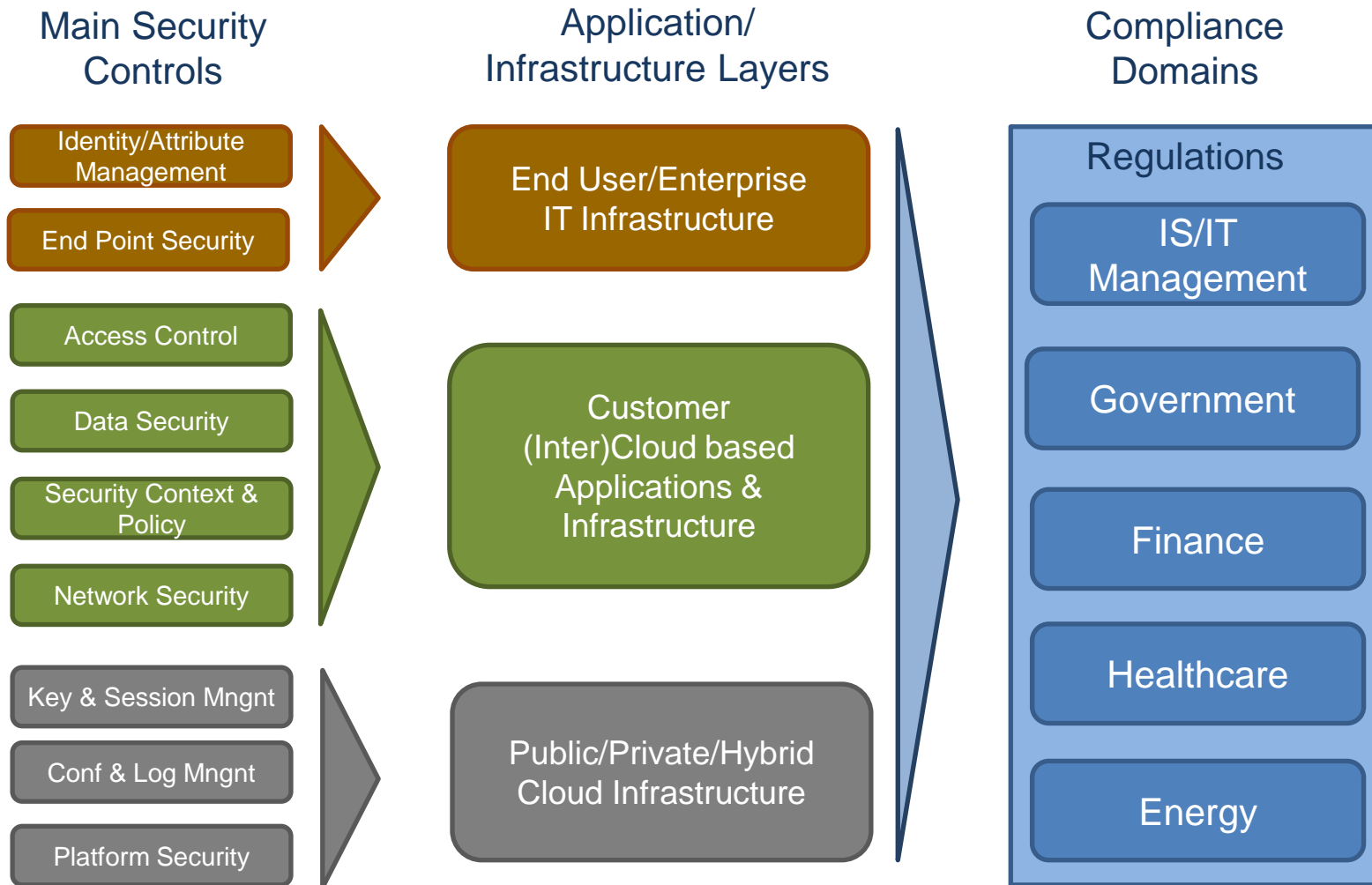


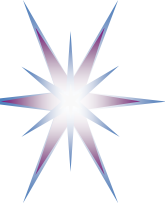


# Cloud Compliance and Big Data

- Use and adopting cloud is unavoidable for modern and future technologies
- Compliance standards, Security Controls
- CSA GRC Stack: Governance, Risk Management and Compliance

# Mapping Compliance and Cloud Infrastructure Components





# 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

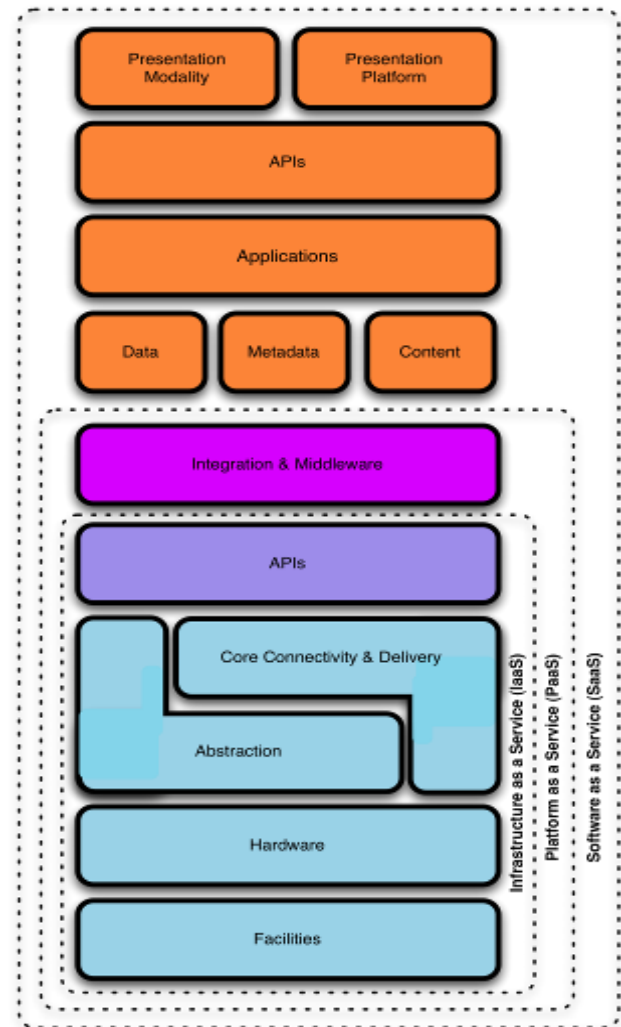
1. Governance and Enterprise Risk Management
2. Legal Issues: Contracts and Electronic Discovery
3. Compliance and Audit
4. Information Management and Data Security
5. Portability and Interoperability

## 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

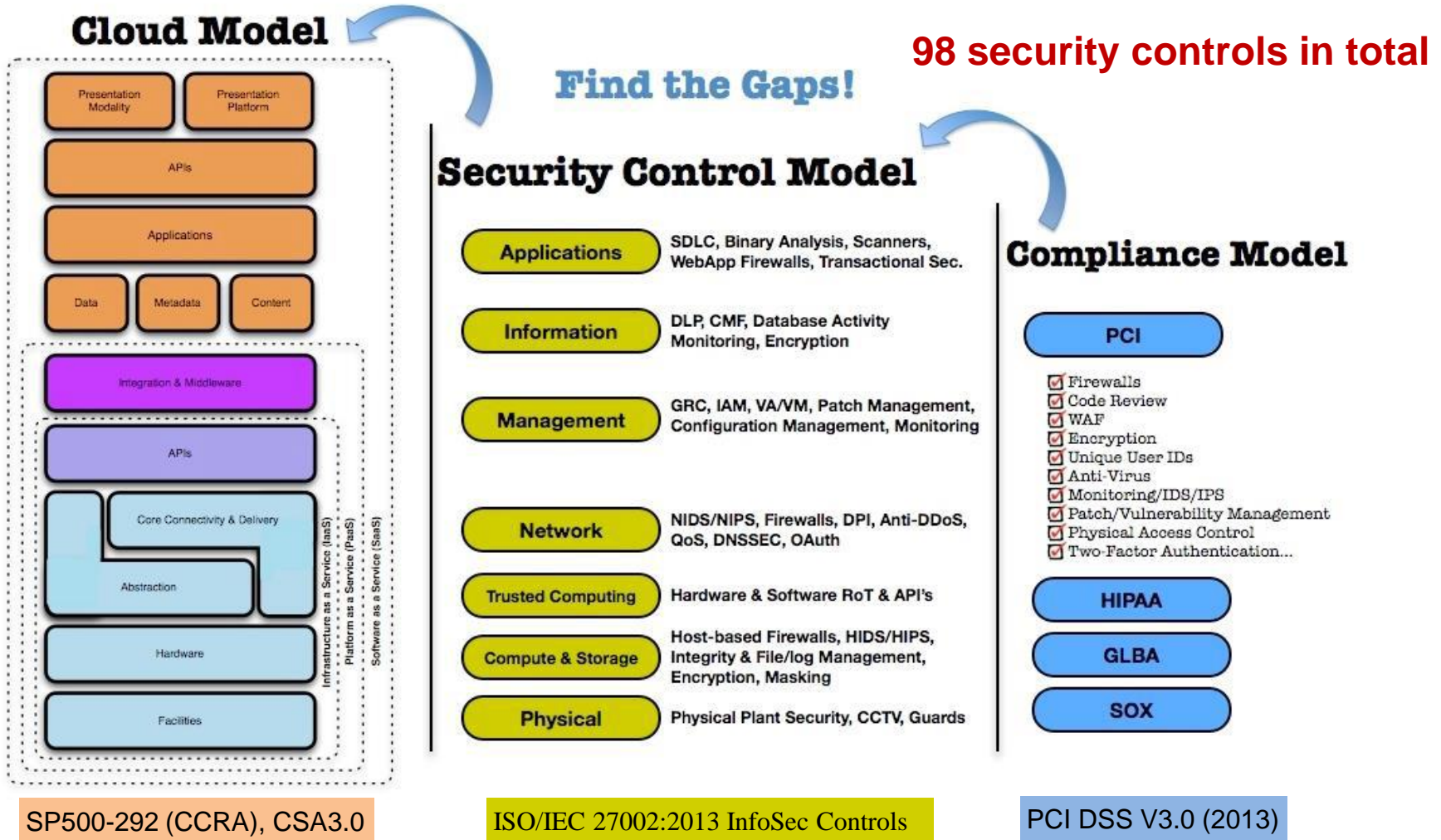
**98 security controls in total**

CSA3.0 Cloud Services Model



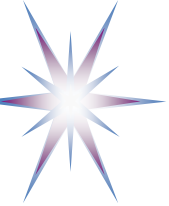


# CSA3.0: Mapping the Cloud Model to the Security Control & Compliance

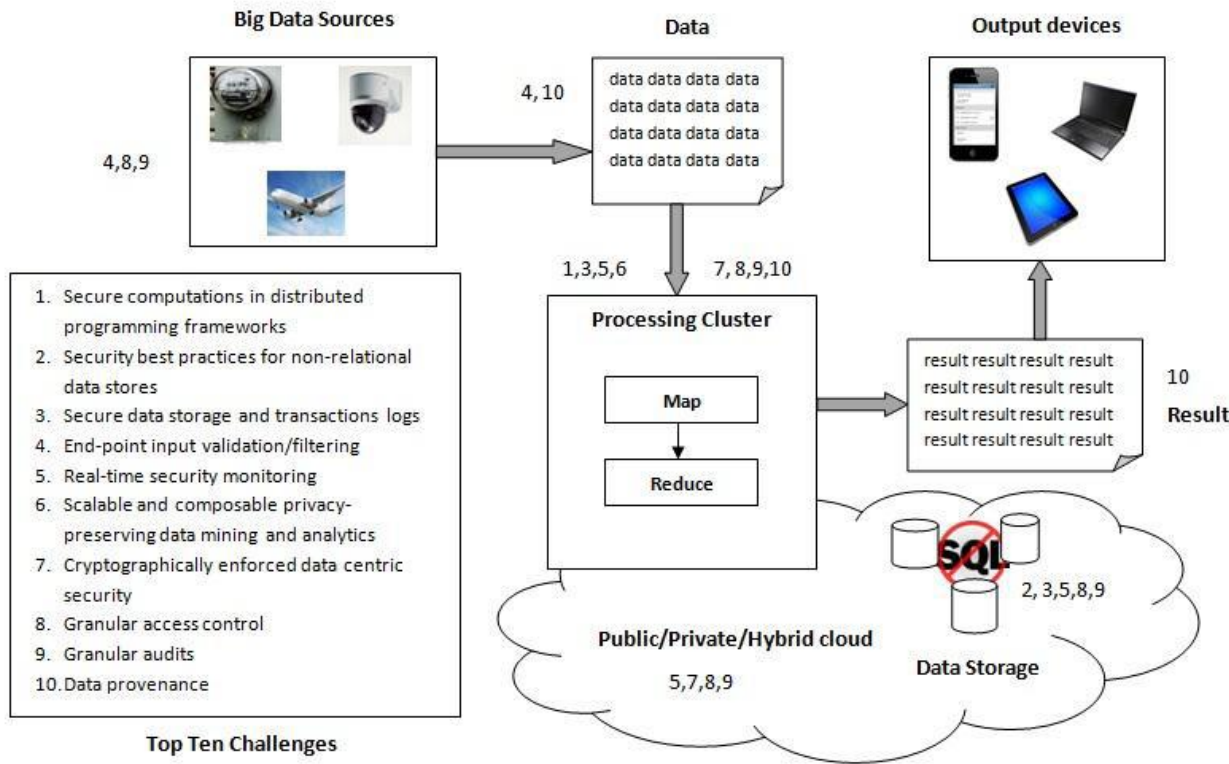


[ref] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2013)

<https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/>



# CSA Top Ten Big Data Security and Privacy Challenges (2013)

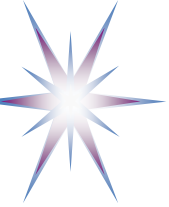


A. Infrastructure security  
 B. Access control and policy

**C. Data Privacy and Confidentiality**  
*TT06. Scalable and composable privacy-preserving data mining and analytics*  
*TT07 Cryptographically enforced data centric security*

**D. Data Management**

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](https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf)



# 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/>

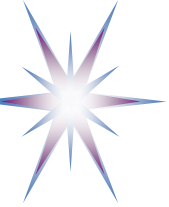


# Case study: Certification/Compliance by Microsoft Azure

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/>

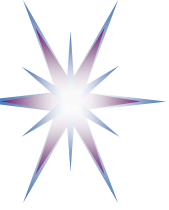


# A Complete Cloud Security Governance, Risk, and Compliance (GRC) Stack

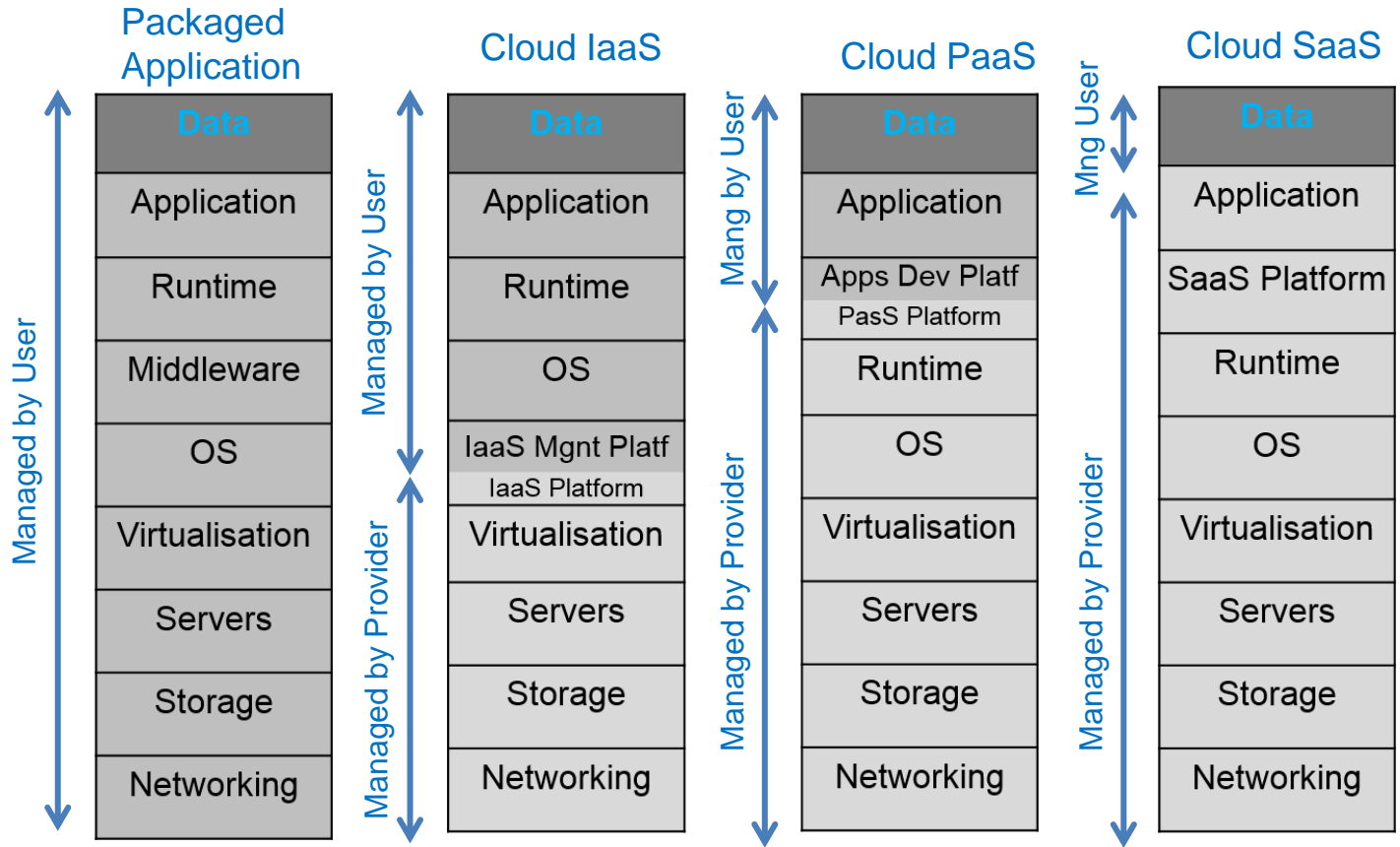
<https://cloudsecurityalliance.org/research/grc-stack/>

| Delivering  | ← Stack Pack →  | Description   |
|---|---|---|
| Continuous monitoring ... with a purpose                      |    | <b>Cloud Trust Protocol (CTP)</b> <ul style="list-style-type: none"><li>• Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers</li></ul>   |
| Claims, offers, and the basis for auditing service delivery   |    | <ul style="list-style-type: none"><li>• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments</li></ul>   |
| Pre-audit checklists and questionnaires to inventory controls |   | <b>Consensus Assessments Initiative (CAI)</b> <ul style="list-style-type: none"><li>• Industry-accepted ways to document what security controls exist</li></ul>   |
| The recommended foundations for controls                      |  | <b>Cloud Control Matrix (CCM)</b> <ul style="list-style-type: none"><li>• Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider</li></ul> |





# Responsibilities Split in IaaS, PaaS, SaaS

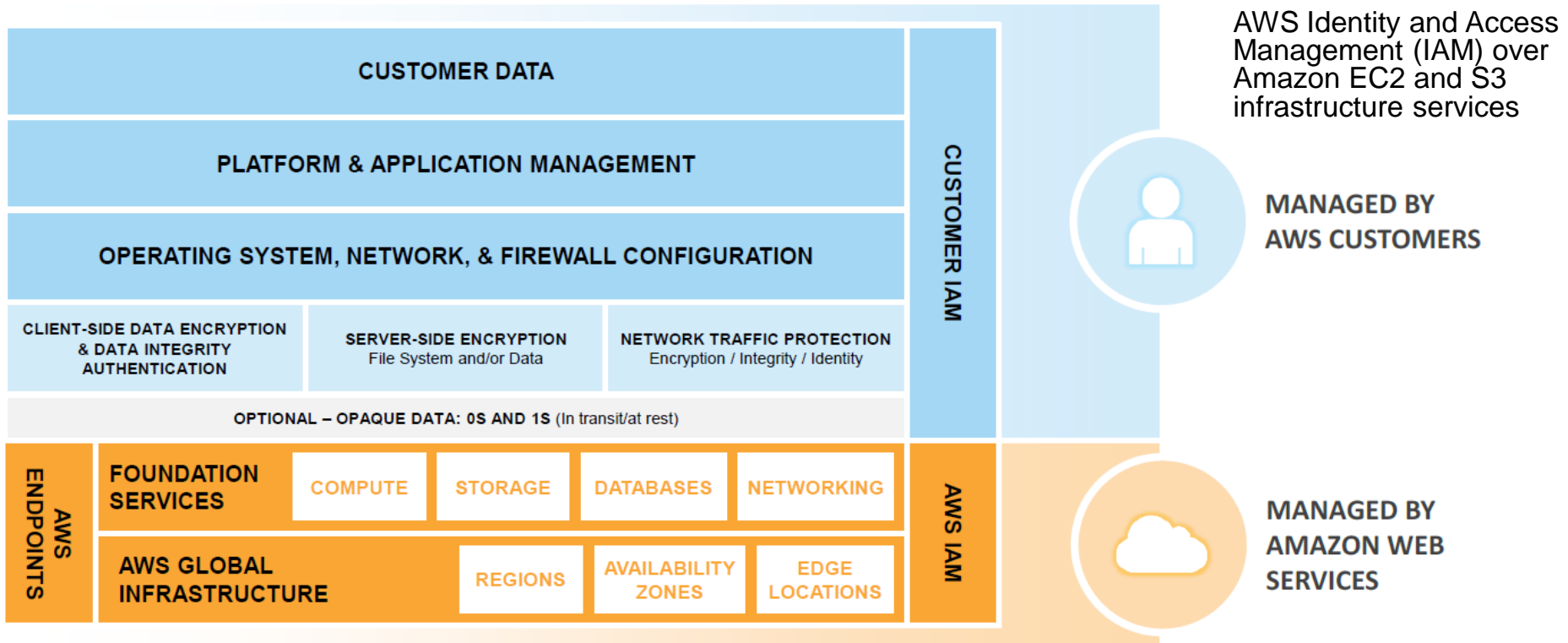


Security management responsibilities split between Customer and Provider for IaaS, PaaS, SaaS service models

- Updating firmware and software for platform and for customer managed components
- Firewall 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



# 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](http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf)



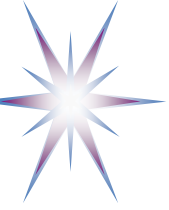
# Adopting Public Cloud – Security Practices

- **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.**
  - 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.



# Data Protection Regulations

- EU General Data Protection Regulation (GDPR)
- Attitude to Data Protection (EU study) – EU vs US
  - EU – U.S. Privacy Shield



# Attitude to Data Protection (EU study 2015)

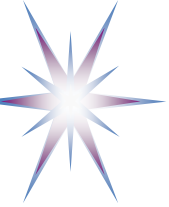
*Special Eurobarometer 431 - Data protection, June 2015*

[http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs\\_431\\_sum\\_en.pdf](http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf)

- A large majority of people (71%) still say that providing personal information is an increasing part of modern life and accept that there is no alternative other than to provide it if they want to obtain products or services
- Over half of Europeans who use the Internet use an online social network at least once a week. This proportion is similar for using messaging or chat sites.
- A large majority of Europeans (69%) would like to give their explicit approval before the collection and processing of their personal data
- More than six out of ten respondents say that they do not trust landline or mobile phone companies and internet service providers (62%) or online businesses (63%).
- 67% find it important to be able to transfer personal data to a new online service provider ('data portability').

Trust in internet services:

- 81% of Europeans feel that they do not have complete control over their personal data online
- Only 24% of Europeans have trust in online businesses such as search engines, social networking sites and e-mail services.



# White House report “Big Data: Seizing Opportunities, preserving values” (2014)

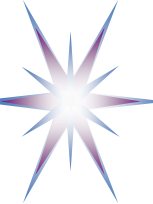
- The White House report ‘Big Data: Seizing Opportunities, preserving values’ published in May 2014.
  - The report is the result of the 90-day study commissioned by the President of the United States to examine how big data will transform the way people live and work and how big data will alter the relationships between government, citizens, businesses and consumers.
- Data security and privacy challenges in Cloud Computing and big data have been a focus of numerous study groups initiated by different governmental bodies that produced several valuable reports.
  - Wide implementation of Cloud Computing provided a basis for developing big data technologies and data-centric and data-driven applications that in their own turn facilitate cloud technologies development.
- ***The main approach in developing recommendations was to protect privacy while not hindering/restricting development of new technology for the benefit of the whole society.***
  - ***The report expresses the opinion that despite widely discussed needs for personal control of the collected e-commerce and social data, the practical use of such control is impractical due to the unmanageable volume of information and its variety. Instead, the advertisement companies and other organisational users of the personally***



# EU – U.S. Privacy Shield



- EU-U.S. Privacy Shield: stronger protection for transatlantic data flows
  - Adopted *12 July 2016*. Repeals **former Safe Harbor Framework**
  - [http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm)
- *The new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers.*
- The new arrangement includes:
  - **strong data protection obligations on companies receiving personal data from the EU**
  - **safeguards on U.S. government access to data;**
  - effective protection and redress for individuals;
  - annual joint review to monitor the implementation.
- What will it mean in practice for American companies
  - Self-certify annually that they meet the requirements.
  - Display privacy policy on their website.
  - Reply promptly to any complaints.
  - If handling human resources data: Cooperate and comply with European Data Protection Authorities.



# GDPR main principles and key changes

- One simple technologically neutral and future-proof set of rules across the EU
  - Helps building trust in the online environment (that is global, distributed, opaque)
- Everyone has the right to the protection of personal data
  - Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose.
  - Person or organisation which collect and manage personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.
  - Consent is requested in a clear affirmative way
- Privacy impact and requirements
  - Right to be forgotten (RTBF) and right for explanation
- Data portability: right to obtain data and relocate to new provider/location
- Recommendation to establish a position responsible for compliance
- Privacy by-design principle for services and infrastructure





# GDPR: Technological challenges

- Regulation, legal enforcement is not enough
  - Not all are law abiding citizens
- All privacy policies, measures must be technologically enforced
- Data protection and security during all data handling phases  
**collection – transfer – store – processing - delivery**
- Protection and security of all components of the data handling ecosystem:
  - Infrastructure – software – management – operation – development
  - People: user – developers - operators
- Big Data and Cloud =>



# Big Data and Clouds

- Current technology development stage:
  - Post – Big Data and post – Cloud
  - == Cloud and Big Data are mainstream technologies and common platform
- Role of Big technology firms (superstar)
  - Technology drivers and innovators
  - Huge concentration of the technology power
- Emergence of Agile Data Driven Enterprise (ADDE) model
  - Digitalisation of all processes and extensive use of Data Science and Analytics (DSA)
  - Data bring competitive advantage and monopoly



# GDPR and Data Science and Analytics

- GDPR requirements create challenges for designing and operating modern DSA based services
  - Data processing and profiling
  - Right to explanation
  - Right to be forgotten
  - Bias and discrimination
- Brings new requirements to Machine Learning and Data Analytics methods and tools
  - ML and DA algorithms are based on statistical algorithms
  - New testing and compliance verification procedures to be developed



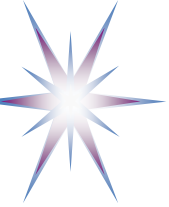
# Data Management and Governance

- Underestimated area of the (mature) enterprise IT infrastructure
- Data Management Body of Knowledge (DMBOK) by DAMA (Data Management Association)
- Data Management Maturity (DMM) model by CMMI Institute (Capability Maturity Model Integration)
- Industry adopted best practices, addressing:
  - Data Quality, Data Provenance, Data Security
  - Data Infrastructure



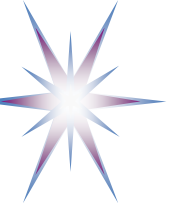
# Summary and discussion

- Cloud compliance provides a basis for wider cloud services adoption and enterprise-inter-cloud integration.
  - How much is it known for specialists and wider public?
- Compliance is supported by numerous standards, legislations, 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
- Data Protection and Privacy in cloud is regulated by numerous group of standards and regulatory documents
  - European General Data Protection Regulation (GDPR) provides common framework for all EU Member States
  - EU-U.S. Privacy Shield is a new framework for cross-Atlantic cooperation



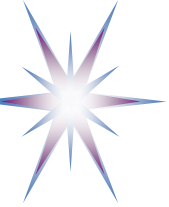
# Panel Discussion Topics

- Trusted data processing platforms and implementation problems, in particular, when using modern Big Data Analytics platforms and emerging AI tools
- What can blockchain offer for data protection and policy enforcement
- What data need to be protected and what data protection is challenging
- Importance of Data and Digital literacy in effective data protection. Ethical code of conduct for future IT professionals
- European projects and initiatives on data protection technologies
- Recent (big) privacy breaches: technological aspects analysis and observations



# Panel Questions and notes

---



# Examples Recent Privacy breaches and technology role

- Facebook
- Twitter
- Sony
- Russian Intelligence Service
  - Boshirov vs Bashirov :-)





# Panel Discussion Summary

- Panel of GDPR and Privacy skeptics
- GDPR2.0
- ICT vs citizen literacy
  - DigComp?
- Boshirov vs Bashirov :-)