



Cloud Security Strategies

Fabio Gianotti , Head of Cyber Security and Enterprise Security Systems

London, 14 October 2015

UNICREDIT AT A GLANCE

- Employees: more than **146.600**
- Branches: **8.403**
- Banking operations in **17** countries
- International network spanning: ~ **50** countries
- Global player in asset management: **€221** bn in managed assets
- Market leader in Central and Eastern Europe leveraging on the region's structural strengths



A COMPLEXITY TO BE MANAGED

The approach to ICT Security Governance follows different paths

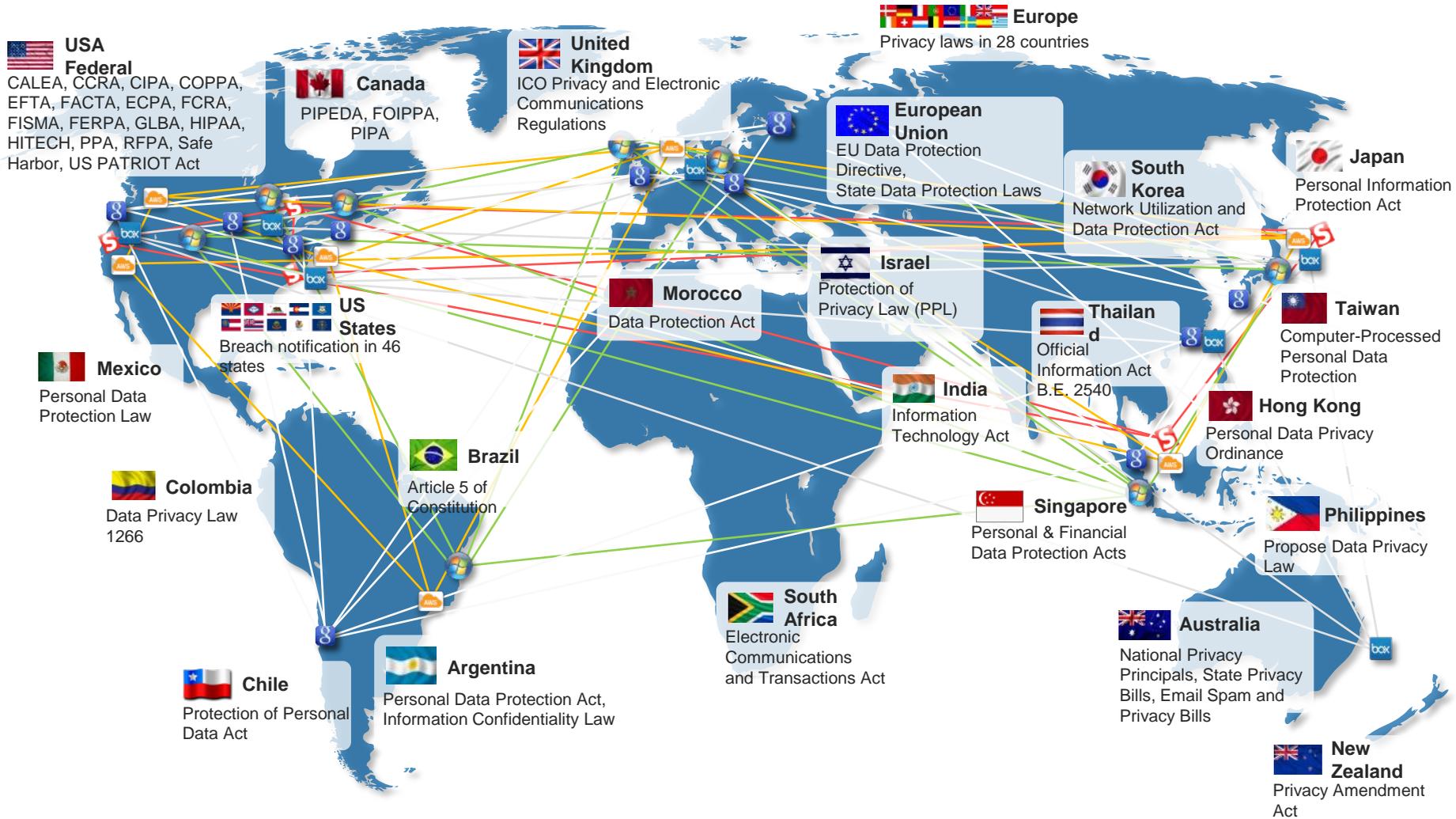
- UniCredit landscape is complex
- Different country regulations
- Different approaches to cloud adoption due to high-number and the geographical distribution of UniCredit Data Centers
- Cloud adoption strategy for Data Centers consolidation framework, and Business Enabler
- Strong ICT Security governance is both mandatory and strongly recommended



Last but not least :

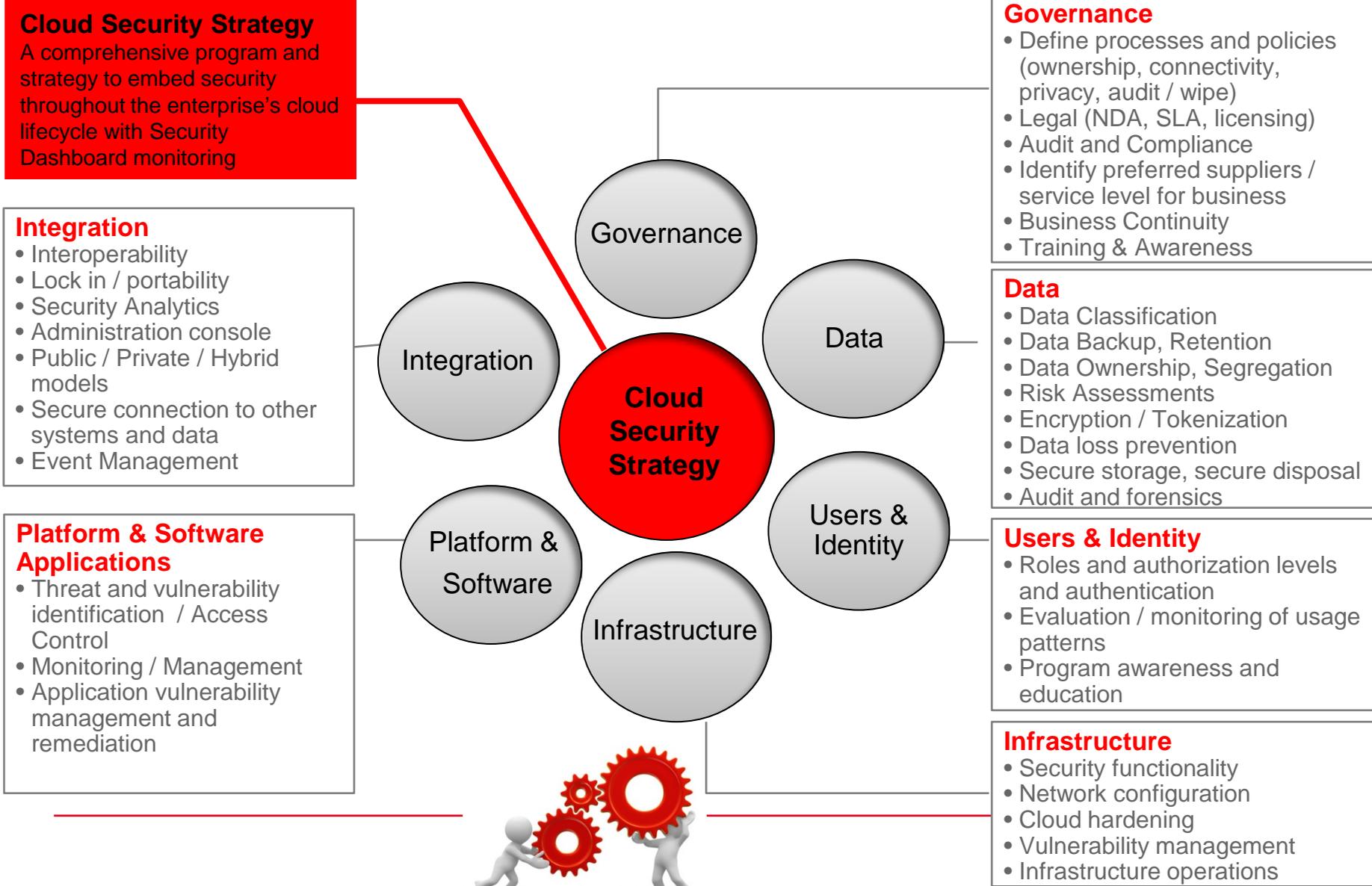
Judgment of European Court of Justice in CASE C-362/14 declaring the Commission's US Safe Harbor Decision invalid....**any Ideas from ENISA team?**

WHERE CLOUD DATA ARE LOCATED AND WHICH LAW IS APPLIED



SEVERAL COMPONENTS TO BE ADDRESSED

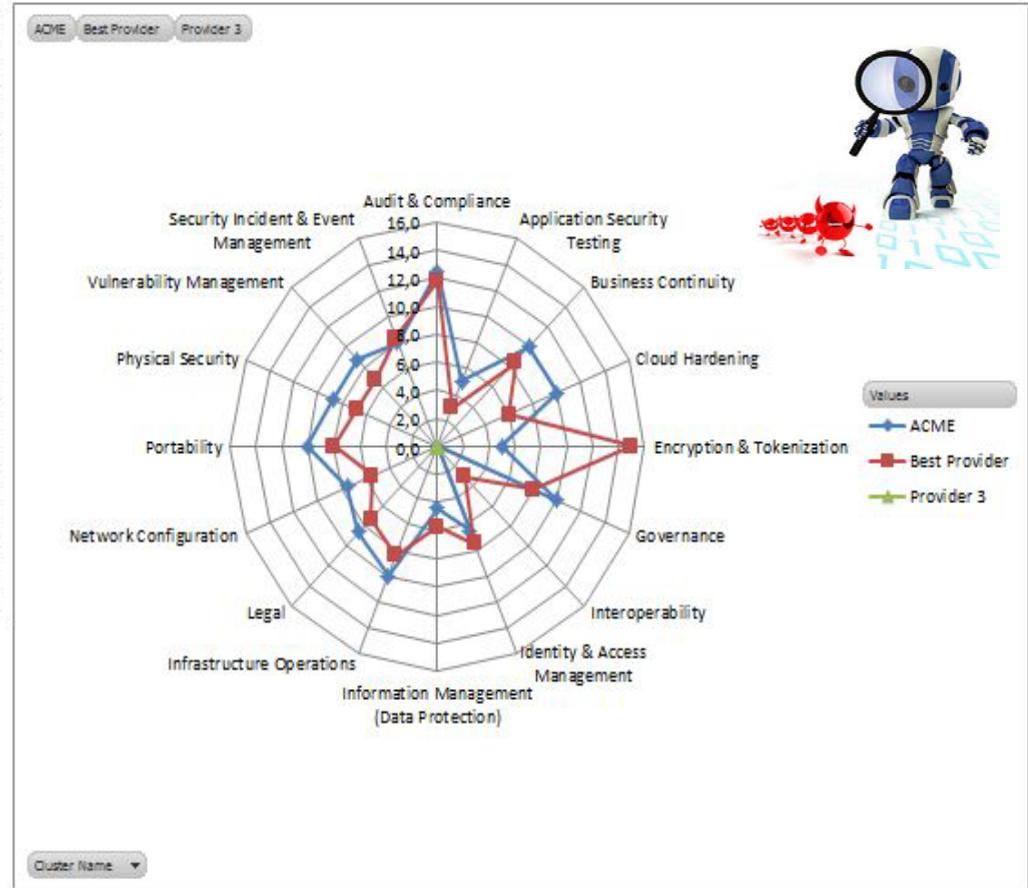
(in order to set a comprehensive Cloud security strategy)



UNICREDIT CLOUD SECURITY EVALUATION DASHBOARD

Summary of scoring results

Clusters	ACME	Best Provider	Provider 3
Audit & Compliance	12,5	11,8	0,0
Application Security Testing	5,0	3,0	0,0
Business Continuity	10,0	8,5	0,0
Cloud Hardening	10,0	6,0	0,0
Encryption & Tokenization	5,0	15,0	0,0
Governance	10,0	8,0	0,0
Interoperability	0,0	3,0	0,0
Identity & Access Management	6,5	7,5	0,0
Information Management (Data Protection)	4,4	5,8	0,0
Infrastructure Operations	10,0	8,4	0,0
Legal	8,6	7,3	0,0
Network Configuration	7,5	5,5	0,0
Portability	10,0	8,0	0,0
Physical Security	8,8	6,8	0,0
Vulnerability Management	8,8	6,8	0,0
Security Incident & Event Management	8,0	8,4	0,0
Total score	125,0	119,7	0,0

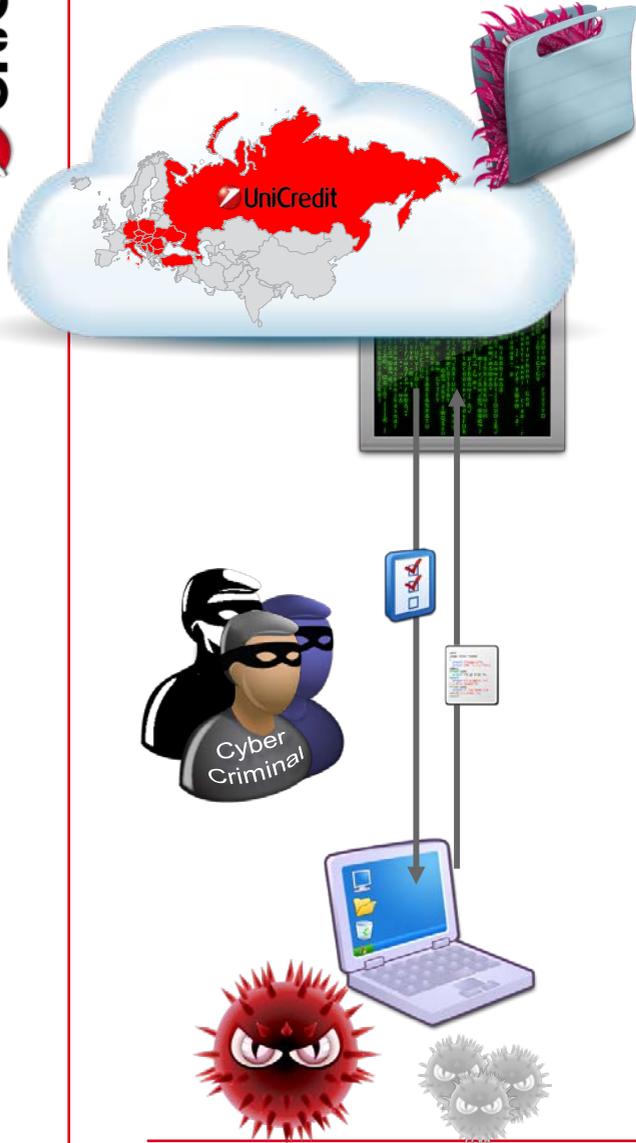


IS THERE ANY DIFFERENCE BETWEEN DATA AND THEIR APPLICATIONS IN THE CLOUD?

- Yes, the law is applied to the data, not to the application
- If you can encrypt the data, then the cloud provider has no access to the data
This might change how responsibilities are allocated from a compliance point of view according to the countries where your business is



CLOUD READY PROGRAM



- Cloud Ready overview declines the Group CIO Global and Group CIO ICT Security cloud strategy and feasibility, in order to design a sustainable and common UniCredit **Service Platform/ Framework**.
- Cloud computing is a new way of delivering computing & services resources, not a **new technology**. Computing services ranging from data storage and process to software on demand to launch new time-to-market business proposition in UniCredit multichannel perspective.
- The massive concentrations of resources and data could represent a more attractive target to **attackers**, but cloud-based defenses can be more robust, scalable and cost-effective in terms of IT security perspective.
- It is important to note that cloud computing can refer to several different service types, including Application/Software as a Service (**SaaS**), Platform as a Service (**PaaS**), and Infrastructure as a Service (**IaaS**).
Lastly API rest exposure, for B to B and B to C customers services.

FINAL TAKE-AWAYS

- Cloud benefits in terms of elasticity, scalability, on-demand computing power – growing list of providers
- Companies must be structured (or re-structured) in order to deal with a new generation of risk evaluation, and address the best cloud strategic and omni-comprehensive approach (data protection, application security, network security, encryption , file sharing, local and global regulation, compliance, log management, identity management, KPI & SLA, etc), in order to deploy a strong and sustainable security governance.
- Companies must raise the bar on ongoing security activities, while addressing at least three key-points to the respective cloud provider:
 - Setting the minimum security level expected
 - Managing the increasing complexity with different and new monitoring points
 - Putting on the table technical skills, more and more sophisticated with a holistic view
- Bridging the gap between requirements, risks and skills

THANK YOU!