Cloud Computing: A European Perspective

Rolf von Roessing CISA, CGEIT, CISM
International Vice President, ISACA

Overview

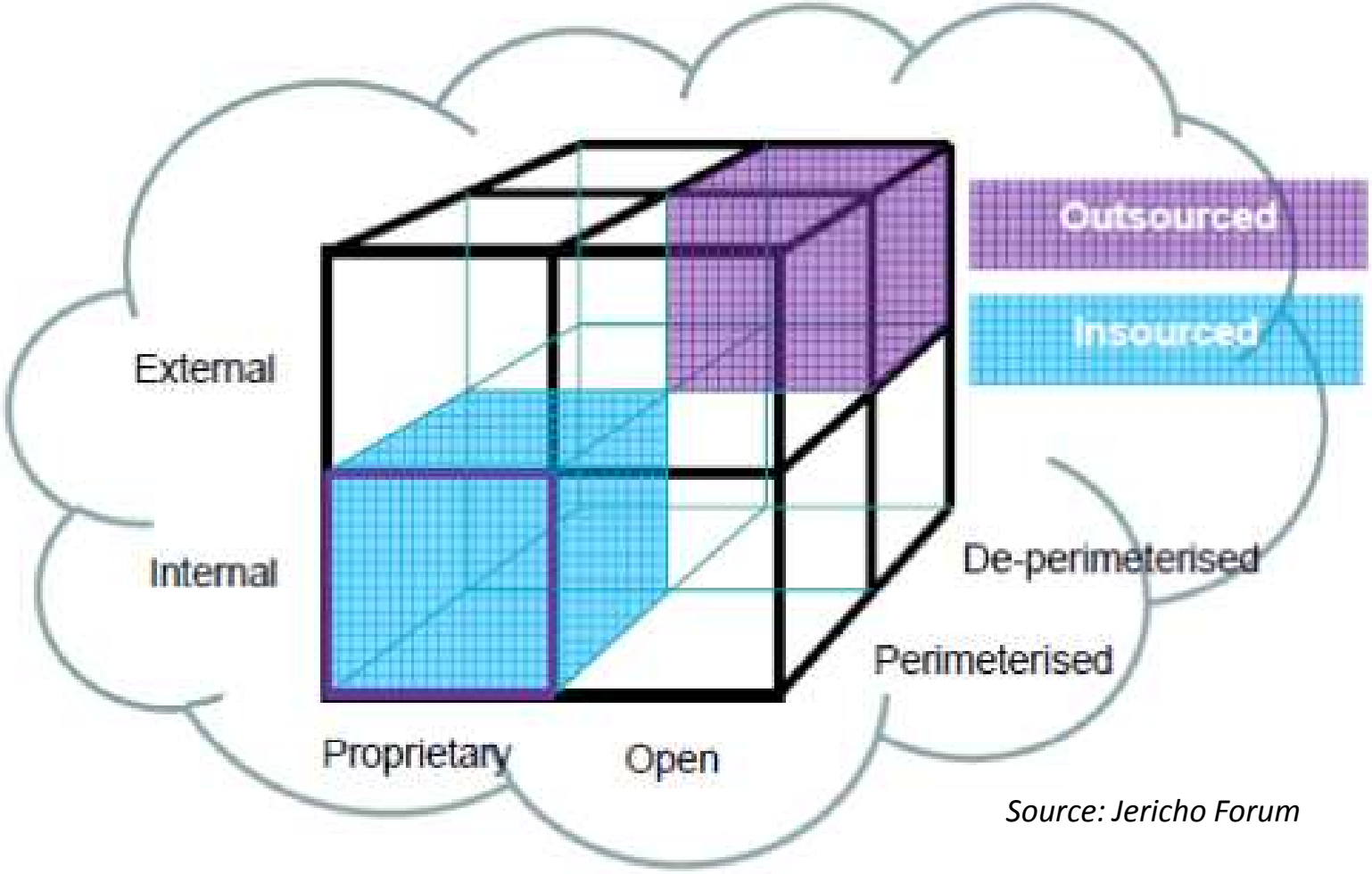
- Cloud Universe – Definitions
- Cloud Risks in Europe
- Governance, Risk and Compliance (GRC) Issues
- European Union Perspective
  - Research Agenda
  - GRC Recommendations
  - Regulatory Initiatives
- Selected National Approaches in the EU
- Conclusions and Outlook

ISACA®
Serving IT Governance Professionals

Cloud Computing – A European Perspective

CLOUD UNIVERSE - DEFINITIONS

The Cloud Universe



Source: Jericho Forum

ISACA®
Serving IT Governance Professionals

Cloud Cube Dimensions and Layers

- Internal vs. External – delineate the physical boundaries of the cloud under review
- Proprietary vs. Open – determine ownership of technology, services, interfaces and other components
- Perimeterised vs. De-Perimeterised – trace your corporate boundaries (structural / logical), for instance DMZ / firewalling: may be wider than physical
- Layer(s) at which the cloud exists – Process, Software (SaaS), Platform (PaaS), Infrastructure (IaaS)

- Insourced vs. Outsourced – control of resources, contracts

Source: based on Cloud Cube Model (Jericho)

ISACA®
Serving IT Governance Professionals

Social Networks as Part of the Cloud

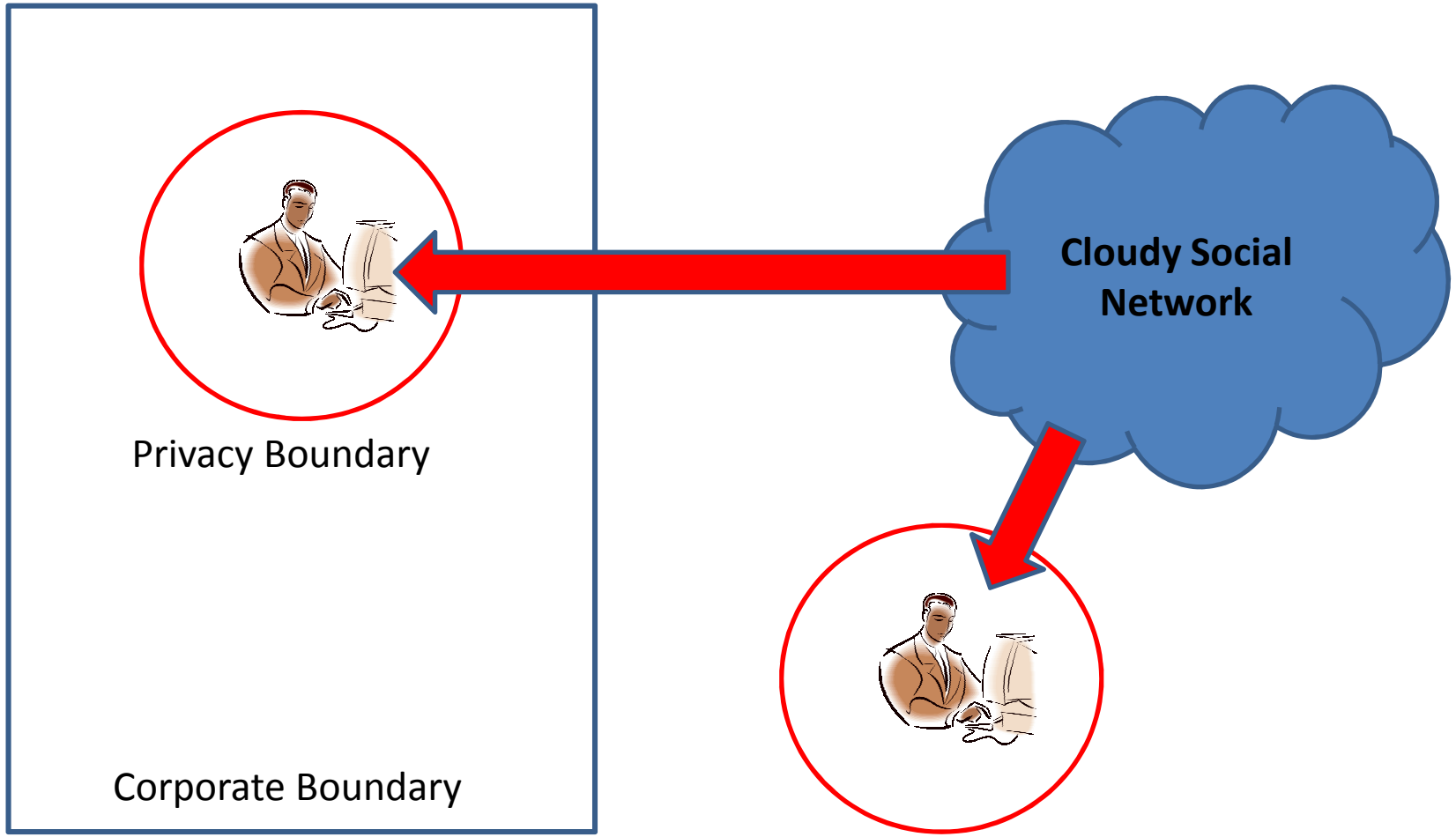
- Social Networks have rapidly become an area of concern throughout Europe – therefore included in this presentation
- Practical areas of concern: Facebook controversy, employment / recruitment practices, GPS-based tracking of minors etc.

- Typically external, de-perimeterised, outsourced
- Process or software layer, sometimes platform layer

- Social networks are user-centric: they tunnel through the corporate paradigm
- Link between social network users and their corporate background is organisational, not technical
- Corporate use of social networks must be bottom-up (by definition)
- Social networks are encapsulated by a Privacy boundary that is drawn around the individual user
- Network operators have introduced far-reaching terms and conditions that may be in breach of European privacy regulations

ISACA®
Serving IT Governance Professionals

User, Corporation, and Social Network



Cloud Computing – A European Perspective

CLOUD RISKS IN EUROPE

Key Risks in Cloud Computing

- User privileges – access, bypassing the border etc.
- Regulatory compliance – key internal controls, financial controls etc.
- Data location – physical and logical
- Data segregation – data at rest, data flow, encryption etc.
- Availability and DR – capacity and recovery capabilities, dimensioning of platforms and infrastructure, etc.
- Audit and investigative support – logging, audit trails, evidence, chain of custody etc.
- Long-term viability – what to do about 10 yr retention (or longer)

Source: Gartner

ISACA®
Serving IT Governance Professionals

More Key Risks

- Contracting risk – SLA design, strategic dependencies, exit scenarios, etc.
- User privacy risk – protective rights may be prohibitive to audit AND regulators, ie contradictory points of law (also consider employee duty of care)
- Reputational and societal risk – Process as a Service, and social networks, evoke spontaeous phenomena such as virtual flash mobs etc.
- Reverse user privacy risk – targeted identity theft, defamatory activity, libel / slander, stalking etc. (also consider employer duty of care)

Strategic European Risks

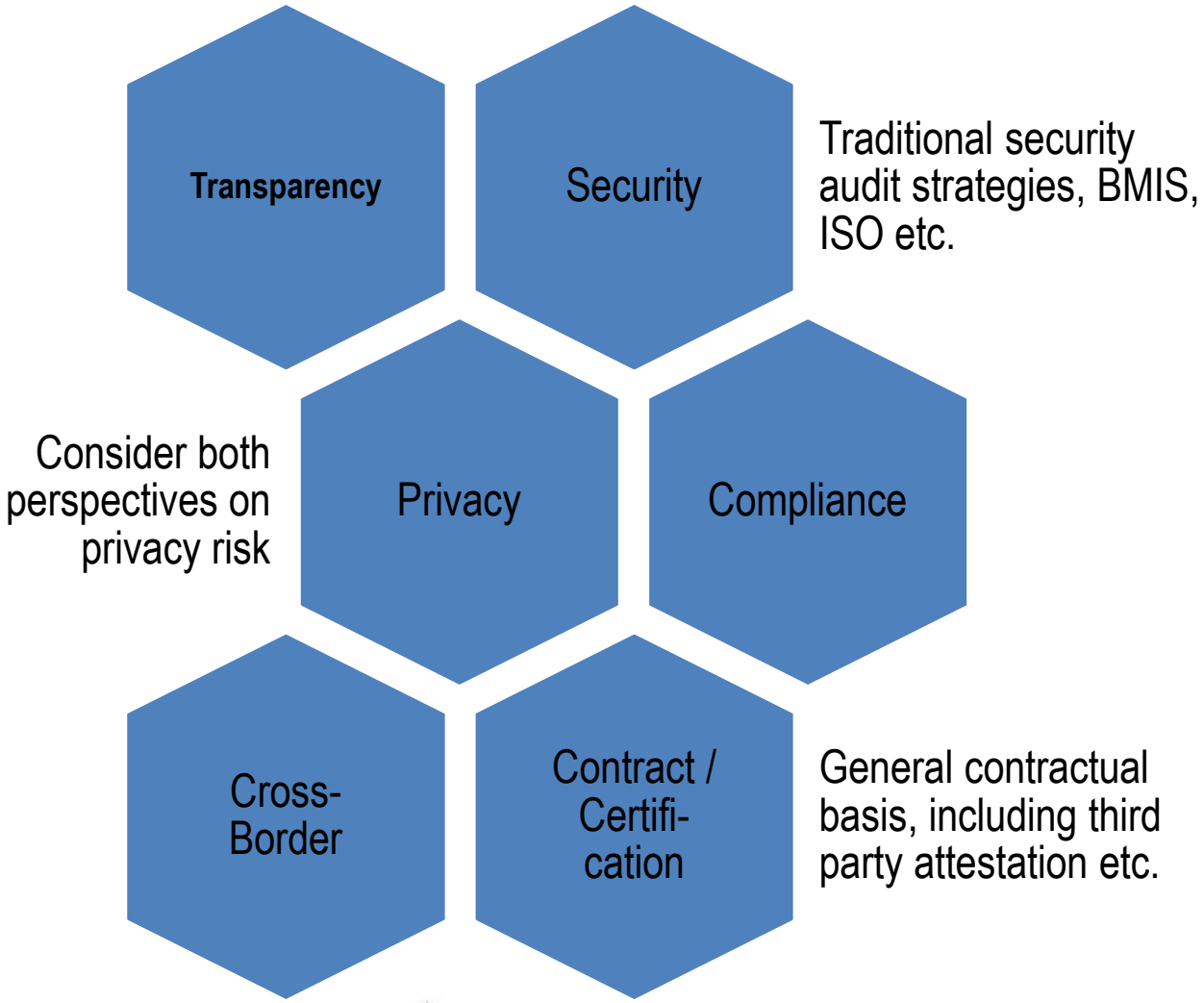
- Sourcing dependency (lock-in): technical dominance of non-EU commercial providers
- Cross-border: loss of control over data and infrastructure situated outside the Union
- Cyber crime: decentralised attack and crime vectors from outside the Union
- Data availability: service and platform continuity for critical infrastructures
- Alignment: integration of clouds with existing GRC provisions across the member states

ISACA®
Serving IT Governance Professionals

Cloud Computing – A European Perspective

GOVERNANCE, RISK AND COMPLIANCE (GRC) ISSUES

GRC Issues



ISACA®
Serving IT Governance Professionals

GRC Issues

- Transparency: Structure, Quality of Service, suppliers and supply chains, liability
- Security: Outlying services, degree of control, alignment with corporate and national ISMS, critical infrastructures
- Privacy: EU and national laws, safe harbor, binding corporate rules (BCR), data location issues, encryption and archival
- Compliance: adjusting cloud GRC to internal corporate compliance provisions, eg SOx, operational risk etc.
- Cross-border: multiple suppliers / vendors, agile data, data mappings, data management, binding corporate rules
- Contract / Certification: rights to audit, contractual language vs technology, existing certifications (eg ISO 27001), existing regulatory reports

Cloud Computing – A European Perspective

EUROPEAN UNION PERSPECTIVE

Research Agenda

- EU Framework Programme 7 (FP7):
  - The Future of Cloud Computing, Report (2010)
  - January 2010 Symposium, including an interesting EU / Japan comparative perspective
- 2011 FP7 Work Programme under way
- European Network Information Security Agency (ENISA):
  - Official EU agency conducting surveys and research in cloud computing, specifically security
  - Cloud Computing Security Risk Assessment (2009)
  - Cloud Computing Small and Medium sized Enterprise (SME) Report (2009)

GRC Recommendations

- Governance: growing number of informal calls for better governance (from industry) since 2009
  - See for instance Helmbrecht (2010), further Proceedings of Octopus Conference (2010)
- Risk: growing risk and some notable incidents
  - See for instance EU Parliamentary Resolution (June 2010)
- Compliance: heterogeneous approaches across EU:
  - ENISA: Cloud Computing Information Assurance Framework (2009)
  - France: national federation of clouds (?)
  - Germany: generic regulatory approach, privacy-driven
- Emergence of a growing consultancy sector, many vendor-centric recommendations

ISACA®
Serving IT Governance Professionals

Regulatory Initiatives

- Most regulatory activity is indirect
- Provisions such as SOx, 8th EU Directive (EuroSOx), Privacy laws etc. influence cloud computing
- Employment practices are a significant driver that is shaping public cloud security
- While there appears to be a common goal to regulate, this is difficult across 27 member states
- Best practice / self-regulation vs. Codification
- Several sectors (eg Finance, Health) are subject to more stringent regulation

Cloud Computing – A European Perspective

SELECTED NATIONAL APPROACHES IN THE EU

Example: France

- Planned national infrastructure (federation of clouds)
- Independence vis a vis US / international cloud structures
- National agencies or institutions
- Substantial budget allocated

- French plans are widely seen as difficult to implement
- It is not clear if any national structure will be competitive in the international arena

Example: Germany

- Two National Plans:
  - Critical Infrastructures, including some strategic clouds
  - Standardisation, specifically BSI 100 series, across all federal agencies
- Close alignment with State Privacy Officers
- Adaptation of national privacy laws
- Alignment with EU initiatives on critical infrastructures and security

Cloud Computing – A European Perspective

CONCLUSIONS AND OUTLOOK

Conclusions

- Cloud computing is a dominant theme throughout the EU
- There is a defined research agenda at Union level, both in the technical and in the societal fields
- Best practices are forming, but this will require some more work
- At this point, there is no definitive regulation or definitive governance over cloud computing
- Many GRC issues persist, sometimes addressed by non-governmental bodies or Union agencies
- National thinking on cloud GRC is still heterogeneous

ISACA®
Serving IT Governance Professionals

Outlook

- Regulatory initiatives at EU level may start in the near future
- Internationally recognised frameworks such as COBIT and BMIS are applicable
- Standardisation and best practice are slowly converging
- New challenges are arising from privacy and social networks, as the latter are becoming a mass movement
- At national and Union levels, individual (personal) protection in public clouds is an important issue
- Corporate and national protection of critical infrastructures are extended to cloud computing
- Cyber crime grows in importance, particularly at the corporate and industry sector level

ISACA®
Serving IT Governance Professionals

Background Materials

- The sources quoted and some important background materials are supplied together with this presentation
- All sources quoted represent the opinion of the respective author(s)

Thank you very much indeed for your kind attention.
Your questions and comments are highly appreciated.

Rolf can be contacted at:

FORFA AG Holding

Forfa AG Holding
Andhauser Str. 62
8572 Berg / Thurgau
Switzerland

rvr@scmltd.com
Skype: rvrscm

ISACA®
Serving IT Governance Professionals