ENISA-ANACOM Workshop on Risk and Innovation

HOW DOES RISK AFFECT FINANCIAL SERVICES?

DEBATE: PROPORTIONALITY OF INNOVATION | ENTREPRENEURSHIP | RISK

Establishing and Maintaining a Sound 27K ISMS Compliant Control Environment in the face of the migration of legacy services to Cloud Computing

MARIANO ARNAIZ | DIRECTOR IT, CESCE

22 January 2010

enisa European Network and Information Security Agency

GRUPO CESCE
Gestión Integral del Riesgo Comercial

Index

HOW DOES (IT) RISK AFFECT FINANCIAL SERVICES?

Financial Services companies are extraordinarily sensitive to risks that arise from the rapid evolutionary changes in IT.

*It is paramount for CIOs and CSO's of financial companies to establish and maintain a Sound I**SO 27001 Information Security and ISO 20000 Service Management Compliant Control Environment** in the face of the migration of legacy services to cloud computing.*

As CIO's are faced with the compelling argument of getting far more IT computing resources for much less, ***many security concerns arise due to the fact that organizational assets are in the custody of a very immature environment that can't provide the level of risk mitigating control that financial organizations need***. The CIO / CSO need an approach for obtaining assurance that the controls needed are indeed readily available and effective.

Synopsis II

The ***ISO 27001*** establishes three forms of risk treatment:

- Acceptance of the Risk
- Mitigation through Controls in a under adequate authority in the cororate domain
- Transfer of the risk responsibility through administrative and legal prescription *(e.g. Service Level Agreement)*.

The line between treatment through mitigation or transfer is determined by establishing if the cloud can in deed provide a sound control environment.

The problem is determining how and where cloud security administration can provide adequate controls for the data asset owner.

The owner's accountability, especially with regards to compliance requirements, is about when the transfer of responsibility provides an adequate level of assurance.

The importance of Standards for Financial Institutions

In evaluating the many options for network security solutions, it is essential to understand and consider the role of security standards for financial institutions.

The growth in distributed computing and the ensuing increase in exposure to risk events with direct effects on the confidentiality integrity or availability of data assets or business processes has led to regulations and in some cases legislation that establish legal requirements for network and data security.

The various ISO network security standards, including the ***27001 Information Security Management, ISO 20000 IT Service Management and the British Standard 25999 for Business Continuity planning*** have undergone extensive peer review and represent the strongest security design thinking available for financial institutions.

The International Bank of Settlements Basel II agreement also specifies policies for containing and mitigating operational risk.

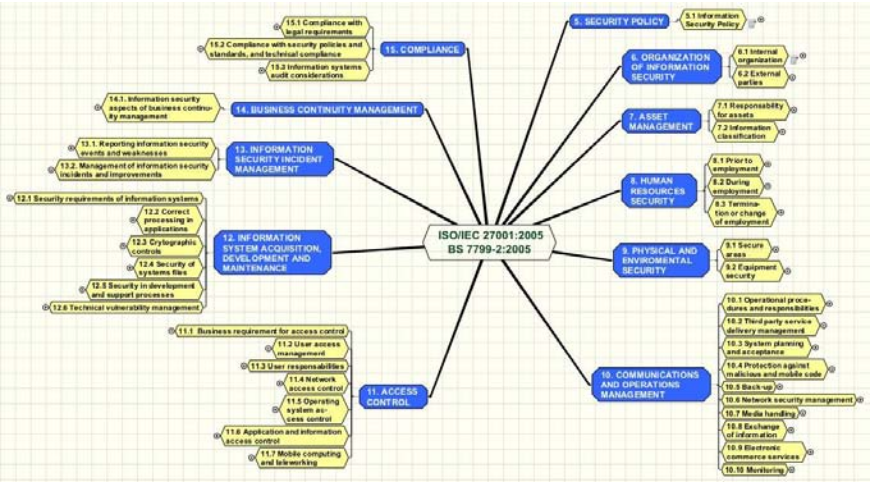
Sound Control Environment

The principal IT and Network Security goal when taking advantage of cloud resources is to create **a sound control environment** that supports ISO 27001 and ISO 20000 prescribed controls for business and addresses IT risks effectively.

Through a sound IT-control architecture; strong policies; and the use of technology solutions capable of managing, maintaining, and reporting on the status of compliance, organizations can reduce the human and monetary resources required for compliance.

ISO 27001

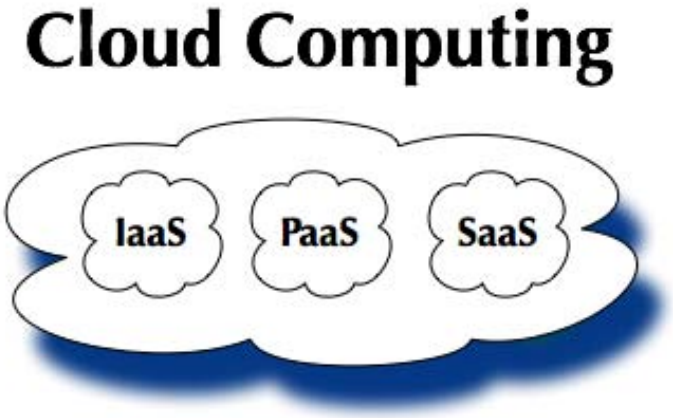
Information Security Management System



enisa European Network and Information Security Agency

GRUPO CESCE Gestión Integral del Riesgo Comercial

Cloud Computing Scenario



Cloud computing is Internet-"cloud" based development and use of computer technology. In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them.

Cloud computing describes a new supplement, consumption and delivery model for IT services based on Internet, and it typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.

Compelling Benefits

Despite the important security and privacy risks issues, Cloud Computing has many compelling benefits that financial corporation and other organizations are certain to want to take advantage of:

- Reduced Cost
  - Cloud technology is paid incrementally, saving organizations money.
- Increased Storage
  - Organizations can store more data than on private computer systems.
- Highly Automated
  - No longer do IT personnel need to worry about keeping software up to date.
- Flexibility
  - Cloud computing offers much more flexibility than past computing methods.
- More Mobility
  - Employees can access information wherever they are, rather than having to remain at their desks.

Compelling Benefits II

- Scalability
  - IT departments that anticipate an enormous uptick in user load need not scramble to secure additional hardware and software with cloud computing.
- Easy Implementation
  - Without the need to purchase hardware, software licenses or implementation services, a company can get its cloud-computing arrangement off the ground in record time at fraction of the cost of an on-premise solution.
- Skilled Practitioners
  - When a particular technology becomes popular, a number of vendors become available and therefore more skilled practitioners come into the market.

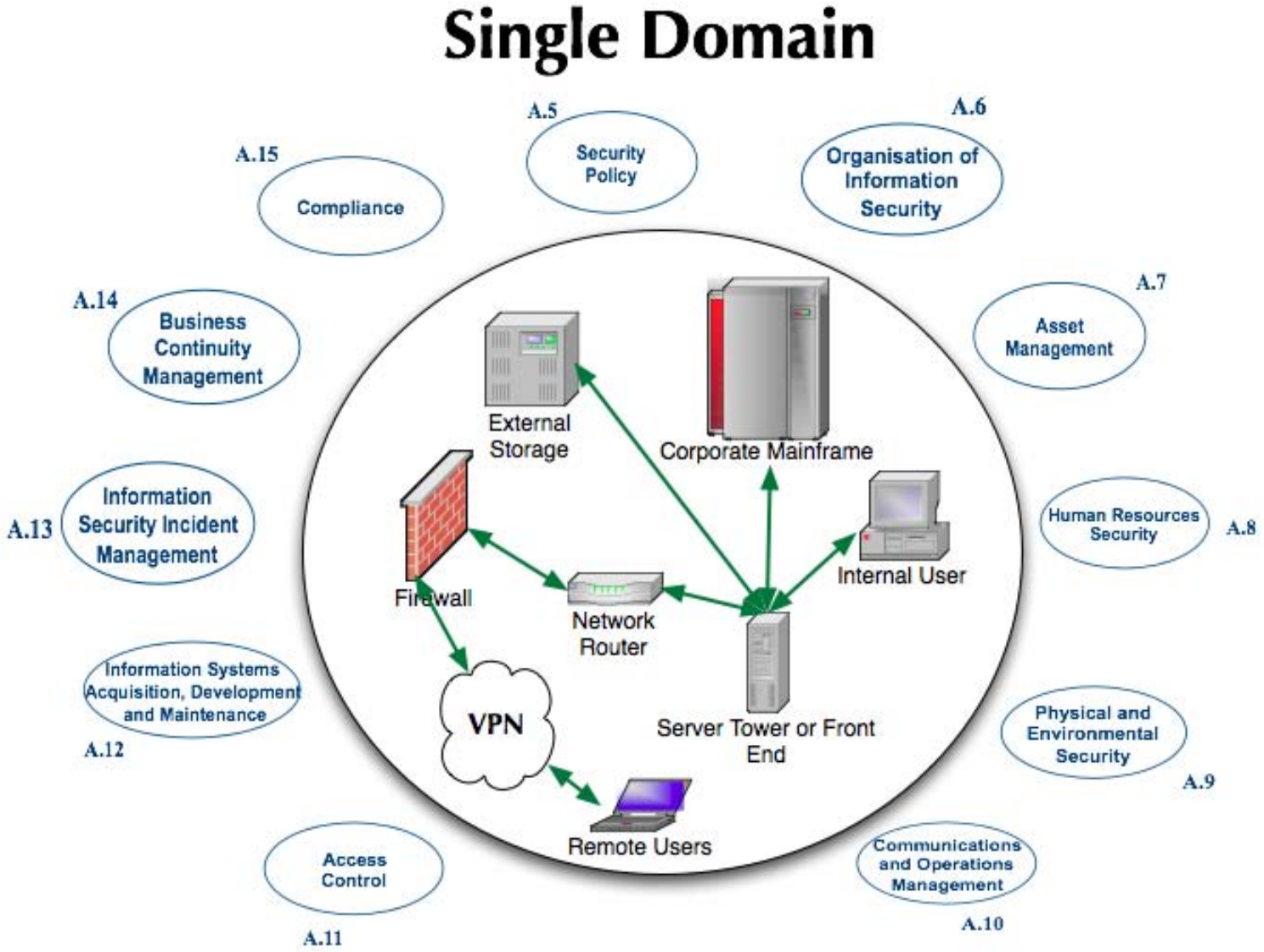
Security Concerns with Cloud Based Services

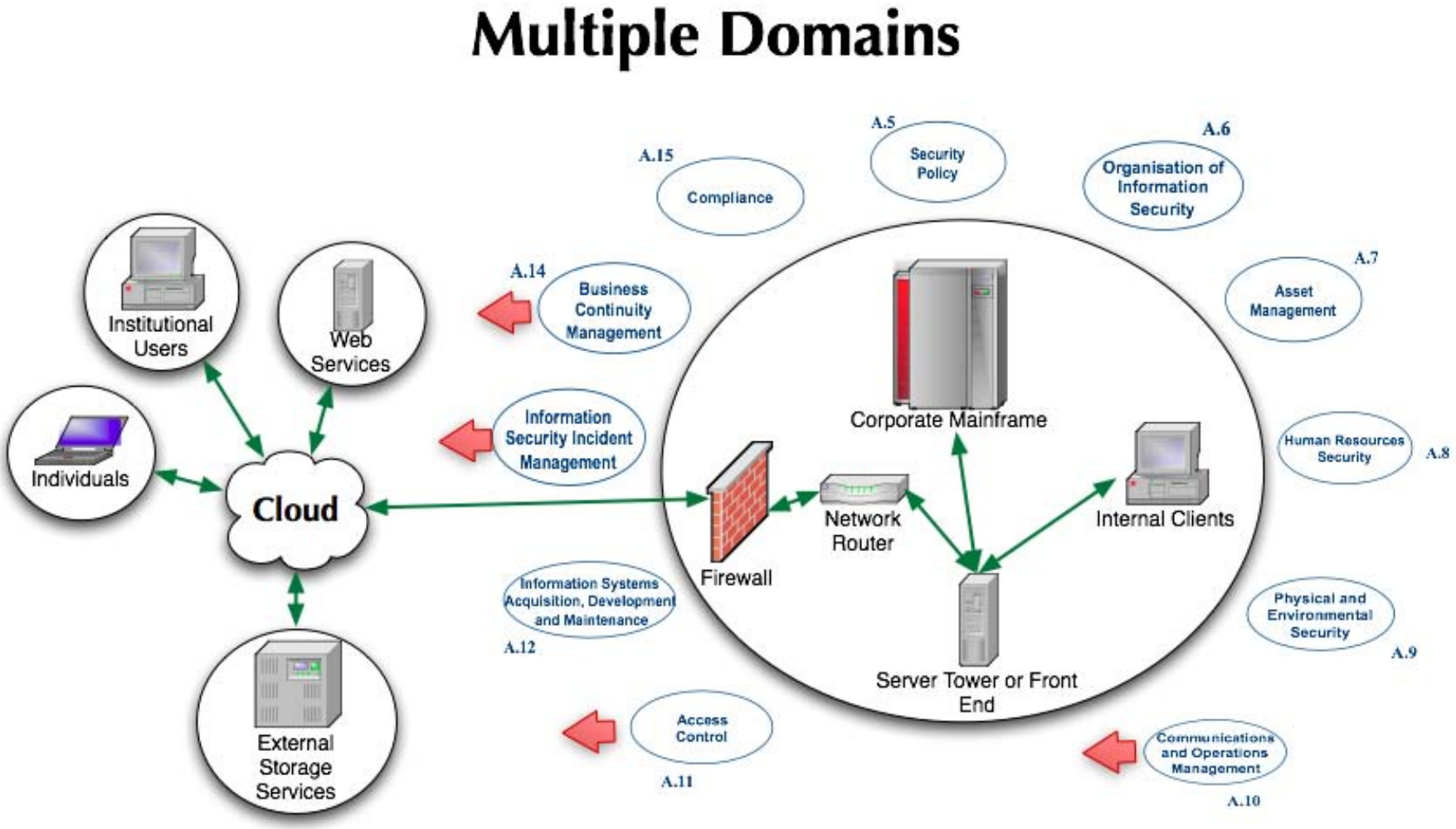
- Privileged user access.
  - Sensitive data processed outside the single domain brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.
- Regulatory compliance
  - Customers are ultimately responsible or accountable for the security and integrity of their own data, even when there has been a transfer of responsibility to service provider.
- Data location
  - When corporate a corporation uses a cloud-based service the data owners probably won't know exactly where their data is hosted or stored.
- Data segregation
  - Data in the cloud is almost always in a shared environment alongside data from other customers. Segregation should go beyond encryption.

•Security Concerns with Cloud Based Services II

- •Business Continuity and Recovery
  - •A cloud-service provider needs to have a viable business continuity plan for data and services in case of a disaster.
- •Incidence Investigative Support
  - •Investigating inappropriate and/or illegal activity may be impossible in cloud computing.
- •Long-term viability
  - •Ideally, your cloud-service provider needs to provide assurances for long term viability and assurances for what happens to corporate clients data assets in the case of business failure or acquisition.

Risks and Loss of Control




Multiple Domains
A.5
Security Policy
A.6
Organisation of Information Security
A.15
Compliance
A.7
Asset Management
A.14
Business Continuity Management
Institutional Users
Web Services
Individuals
Cloud
Information Security Incident Management
Corporate Mainframe
Human Resources Security
A.8
Network Router
Internal Clients
Firewall
Information Systems Acquisition, Development and Maintenance
A.12
Physical and Environmental Security
A.9
Server Tower or Front End
External Storage Services
Access Control
A.11
Communications and Operations Management
A.10

Management Level

The ISO 27001 and ISO 20000 have specific prescriptions for transferring risk once a formal risk analysis has been carried out. Here are some potential measures that should be negotiated with the service provider:

- The cloud-services must have a clear mandate for assuming the risks and provide formulas for mitigation.
- Any legal compliance issues regarding the handling or location of data assets must be clearly defined.
- All matters regarding availability should be defined in accordance with clearly described provisions for service levels, and service continuity.
- Access rights must be defined and monitored
- Data Assets must be shown to be properly segregated from other client's data with the use of encryption, and well defined administrative procedures.

General References

- MASTER FP7 Project
  - http://www.master-fp7.eu/
- Jericho Forum
  - http://www.opengroup.org/jericho
- Security in a Cloud Computing Environment
  - http://cloudsecurity.org/

Michael Hall
CISSP, BSI Registered Auditor
Partner, Forbes Sinclair Inc

Discussion