Self-assessment of security in cloud deployment

Pinja Koskinen & Vesa Simola

(2019)

Don’t we already have enough of these standards and criterion?

- Ease of use combined with the flexibility of different cloud delivery models has led to significant increases in the numbers of applications running on cloud platforms.
- Applications running on cloud have same requirements for security as traditionally hosted ones.

But doesn’t cloud just make it easier to meet the security requirements?

- Cloud services have radically different approaches on distribution of responsibilities, technical dependencies and requirements for life-cycle management.
- Both the customer and cloud service provider have to be compliant.

Self-assessment sheet to the rescue

- Aims for straightforward, check-list like approach to evaluate the security posture and maturity.
- 17 Questions based on literature review of national criterion, literature and best practices.
- Written for Traficom and NCSC-FI

What kind of issues are highlighted?

- Processes and management: Importance of topics such as RTO, RPO, change management and how these are handled on both sides of the customer – service provider relationship.
- Technical requirements: Sufficiently redundant connectivity, segregation of duties, data redundancy and encryption.
- Physical security: Service provider is responsible of this, but how is this handled?

Key findings 1/2

- Not much literature available that is directly aimed at auditing cloud security.
- Literature and best practices from other disciplines of IT or even completely different industries were applied to cloud context.
- All in all, over 15 questions to investigate internally or with the service provider were found.

Key findings 2/2

- Encryption and connectivity are more challenging.
- Classical change management and IT governance still applies but it is more difficult to implement in cloud as services can be created more easily, decommissioning is still nightmare if not planned properly.
- Cloud provides easy to deploy security features, but they need to be properly activated.
- Regulation and locality are increasingly important.

Few words about the thesis work itself

- As an after thought, it would have made things easier if we would have started way sooner.
- First version was a complete mess, but it made it bit easier to understand some of logic behind getting the thesis more into shape.
- In the end, we wrote the whole thing quite quickly once we decided to put our mind to it.