Impact of Critical Infrastructure Requirements on Service Migration Guidelines to the Cloud

Christian Wagner, Aleksandar Hudic,
Silia Maksuti, Markus Tauber
Austrian Institute of Technology
Vienna, Austria
{christian.wagner, aleksandar.hudic,
maksuti.silia.fl@ait.ac.at, markus.tauber}@ait.ac.at

Frank Pallas
Karlsruhe Institute of Technology
Karlsruhe, Germany
frank.pallas@kit.edu

***Abstract*—A high level of information security in critical infrastructure IT systems and services has to be preserved when migrating their IT services to the cloud. Often various legislative and security constraints have to be met in line with best practice guidelines and international standards to perform the migration. To support the critical infrastructure providers in migrating their services to the cloud we are developing a process based migration guideline for critical infrastructure providers focusing on information security. First of all we investigate, via questionnaires, how the importance of individual security topics covered in such guidelines differentiates between industry stakeholders and critical infrastructure providers. This supports the selection of relevant security topics and the considered guidelines and standards, which we survey in search for common relevant security topics. Subsequently we present the analysis of the above-mentioned security requirements and how they affect a here developed taxonomy for a process-based security guideline. Furthermore we present potential service migration use cases and how our methodology would affect the migration of secure critical infrastructure services.**

***Index Terms*—survey analysis; security requirements; critical infrastructure; industry; security guideline, cloud migration**

I. INTRODUCTION

Enterprises recognized the cloud paradigm as an opportunistic business strategy to remain competitiveness, meeting business objectives, increasing performance and reducing costs [1], [2]. The utilization of services across a layered distributed architecture, that is the very nature of cloud computing [3], offers tremendous advantages over a traditional computing paradigm [4]. Cost reduction is one of the main benefits which affect both cloud provider and cloud customer [4]. Therefore, migration of services from expensive enterprise IT infrastructures to the cloud became a prominent and cost-efficient solution [5], [6], [7]. Although, the migration into the cloud offers various benefits [8], [9] primarily in terms of finances, often it is the case that services that are intended to be "cloudified" (i.e. migrated to cloud) are not designed for distributed computing. Thus, additional steps that include detailed analysis and setting up guidelines for migrating services are required [10], [11], [12].

Some of the proclaimed benefits make the cloud also attractive to organizations with high protection requirements, such as critical infrastructures (e.g. telecommunication organizations, the electric power industry, healthcare services, or agriculture companies). However, when considering such a scenario for critical infrastructure services, the potential consequences of a malfunction are of major significance, leading to such systems and services typically being subject to strict regulations in matters of security. Therefore, appropriate measures for maintaining and accomplishing intended information security levels are required from a critical infrastructure providers' perspective. IT systems and services used for managing critical infrastructures require a large amount of resources, and hence critical infrastructure providers often host their own infrastructure or may join resources with other similar organizations. In any case multi-tenant and multi-layer issues apply in these scenarios in a similar way as for common IT businesses.

978-1-4673-8103-1/15/$31.00 © 2015 IEEE

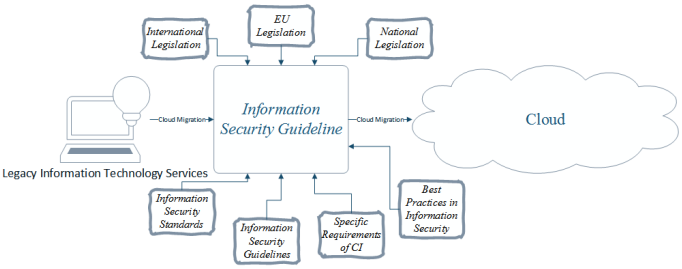

Fig. 1. Information Security Guideline Overview - Topics which determine a cloudification process

In this paper we present our approach in constructing an information security guideline, in form of a life cycle, for the cloud migration phase of critical infrastructure IT services (Figure 1). In our research we have first investigated the differences in security requirements between industry, and critical infrastructure providers by means of questionnaires. With the obtained information from the analysis of the returned questionnaires as well as an extensive literature analysis we develop a taxonomy which we set in relation to relevant best practice guidelines. Hence our main contributions are threefold:

- Analysis of differences in information security requirements of critical infrastructure providers and industrial stakeholders with respect to cloud computing.
- Survey of standards and guideline topics, related to the identified requirements and a taxonomy in order to

represent the results.
- An approach for a process-based information security guideline, including - in the survey- identified process-steps, for the migration of critical infrastructure services to the cloud.

The remainder of this paper is as follows: We evaluate related work in section II. In section III the survey methods and the results of an information security requirements survey among industry and critical infrastructure providers are presented. In section IV the survey results are applied to a taxonomy imbedded in a process-based cloudification life cycle. We present a conclusion and outline of future work in section V.

II. RELATED WORK

In this section we discuss the recent security challenges, methodologies, guidelines and standards with respect to cloud services with high security requirements.

A. Critical infrastructure Security challenges

Despite the attractive economical and performance benefits lack of security (e.g. lack of transparency, data privacy, trust, data lock-In, data loss) still remains the main obstacle for migrating services in to the cloud. This is especially emphasized when taking in to the account services with high security requirements such as critical infrastructure services. Hence, the analysis of security issues in cloud attracted broad research interest [13], [14], [15], [16], [17], [18], [19], [20], [21], [13]. However, majority of the research community concluded that the current security methods and techniques in cloud are not mature enough to reliably support hosting services in cloud. Nevertheless, solutions for migrating enterprise services to the cloud are emerging constantly [10], [11], [6], [12], [5], [7].

Younis et. al. [21] based on their detailed security analysis for various critical infrastructure providers, outlined major security issues in the cloud that hinder the migration of critical infrastructure services. Alcaraz and Zeadally in their survey [13] highlighted the vital role of critical infrastructures in modern society. However, they elaborated security challenges of critical infrastructure assets are mainly focusing on the industrial control systems (SCADA). In addition, authors evaluate the compliance of critical control systems towards standards, recommendations and guidelines.

B. Migration Concepts and Methodologies

Khajeh et. al elaborated in their work [11], [6] the migration of enterprise IT services to the cloud in context of financial and socio-technical enterprise issues which should be considered during migration. In addition, the authors elaborate the decision making process for service migration with two following tools: cost modeling, and benefits and risk assessment. Kaisler and Money investigated in their work [10] the compatibility of the service migration approach with the cloud computing paradigm by addressing various issues(acquisition, implementation, security, usage reporting, valuation and legislative). Fehling et. al. advocate in their work [12] best practices for addressing service migration challenges in context of migration patterns demonstrated on a web based application. Sun and Li perform effort estimation on infrastructure level by using tool for that automatically migrates configuration of workload from physical platform to visualized platform. in their systematic literature review Jamshidi et. al. [7] identify and systemically analyze existing research on legacy software migration to the cloud. The outcome of the research identified the importance of a comprehensive migration framework, which would taxonomically classify and compare various studies for cloud service migration. Paudel et. al. [22] analyzed how mitigation options for identified open security issues for critical infrastructures in the cloud point to individual aspects of standards and guidelines.

C. Standards and guidelines

ENISA generalizes security issues of cloud computing from Critical Information Infrastructure Protection (CIIP) perspective [23]. Additionally, authors discuss the risk assessment and security measures related with CIIP. Although our work is closely related with the work from ENISA, we are more focused on outlining open issues of hosting critical infrastructure services in the cloud.

The National Institute of Standards and Technology (NIST) published the framework for improving Critical Infrastructure Cybersecurity[24]. The framework provides a set of guidelines for developing individual organizational profiles, by aligning cybersecurity activities with business requirements, risk tolerances and resources.

We have identified in the related work that there is some existing work which addresses the service migration methodologies and processes in a generic way. There is also a part of the research community which elaborate on security issues and requirements referred to cloud computing. Furthermore, there are international standards and guidelines available to deal with the protection of critical infrastructure providers. However, there is no uniform solution that addresses the above mentioned challenges, critical infrastructure protection, and secure service migration to cloud environments.

III. INFORMATION SECURITY REQUIREMENTS ANALYSIS

A. Research methodology

To highlight and analyze the differences between industry and critical infrastructure providers information security requirements we performed an extensive survey among industry and academic experts. Thus, we distributed the questionnaire at various events with a cloud computing focus. Furthermore, to acquire the results from broader audience of professionals we also offered an online version of our questionnaire. Finally, we acquired 111 participants (72 via events and 39 online). Answers from academia, where listed, are only used as control sample.

1) Normalization of the results: For most of the questions in the questionnaire, survey participants could rank their opinion according to their importance (i.e. not at all important, slightly important, important, fairly important, very important, and no opinion).

For the analysis of the survey we chose the following normalization formula:

$$\frac{actualrepliesperansweroption}{samplesizeperdomain} \times 100 \times weight \quad (1)$$

In addition the weight values, shown in Table I, were used calculating the normalized output in the above mentioned equation.

TABLE I
WEIGHTING SCALE

Answer Option	Weight
No Opinion	$\log_{10}$ 1
Not at all important	$\log_{10}$ 1
Slightly important	$\log_{10}$ 2
Important	$\log_{10}$ 3
Fairly important	$\log_{10}$ 4
Very important	$\log_{10}$ 5

In the nomenclature of the possible answers the results presented in this survey analysis therefore have the following meaning:

TABLE II
MEANING OF NORMALIZED IMPORTANCE

Range	Meaning
0 % - 43 %	Slightly important
44 % - 68 %	Important
69 % - 86 %	Fairly important
87 % - 100 %	Very important

B. Evaluation of survey results

In the analysis of the provided questionnaire, we show the importance of the NIST cloud characteristics for the industry and critical infrastructure providers and their security needs for these characteristics. We in particular consider the aspect of the geolocation of cloud providers. Furthermore we indicate that the importance of information security for the cloudification of various exemplary IT service for the respective domains. Based on a pre-selected list of security controls, we analyze their importance for the industry and critical infrastructure providers. This is a starting point for the creation of the taxonomy for the process-based information security guideline (chapter IV).

The results of this survey analysis address the following questions:

- Which typical information security requirements (availability, integrity, confidentiality, auditing) are most relevant for critical infrastructure providers for applying cloud computing business models to their IT services?
- Which security controls related to cloud computing environments do critical infrastructure providers consider as important for IT service cloudification?
- How do the findings of this survey analysis influence the taxonomy for a cloud migration guideline for critical infrastructure providers?

Within the following six paragraphs we summarize and justify the most relevant outputs of our survey.

1) Company affiliation of survey respondents: In order for being able to make differentiated statements the survey participants were asked to specify their company affiliation. Out of all 111 respondents

- 31 individuals (28 %) have stated to be affiliated to organization type academia,
- 46 (41 %) to industry,
- 23 individuals (21 %) to critical infrastructure provider, and
- 11 (10 %) to another, undefined organization type.

2) Importance of the geolocation of the cloud provider and relevance of individual cloud computing characteristics: In the survey, besides the elicitation of security requirements of industry and critical infrastructure providers, the respondents were asked some general questions about 1) the importance of the NIST cloud computing characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service) , and 2) the importance of the geolocation of the cloud provider.

With respect to economic espionage, the location of the cloud provider and the data center is very often proclaimed as an important topic [25]. Furthermore, location is also highly relevant from the legal/regulatory perspective, particularly including European data protection law. Our analysis (Figure 2) shows that geolocation is in fact an important element for critical infrastructure providers when selecting cloud providers (12 % higher compared to the industry domain). The total values are: 78 % importance for critical infrastructure domain, 66 % for industry, and 67 % for academia (the control sample).

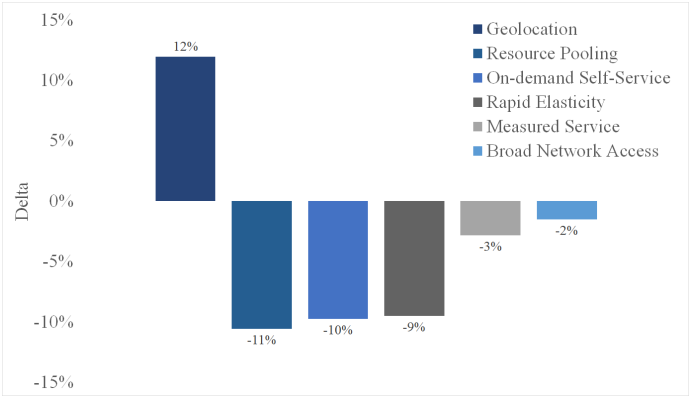

Fig. 2. Values show that regarding the here presented comparison of interest in NIST cloud characteristics of critical infrastructure providers with industry stakeholders, only geolocation is significantly more important for critical infrastructure providers (based on our importance metric).

With respect to the NIST cloud computing characteristics the delta values (Figure 2) show that broad network access is the most important cloud characteristic for critical infrastructure providers, whereas the resource pooling possibilities cloud computing offers are not as relevant. In general, the industry sector and also critical infrastructure providers perceive cloud computing as fairly important (85 % on average - total value) for their businesses.

3) Information security requirements analysis: Critical infrastructures are at the fundament of today's societies as a consequence, failures and breakdowns may lead to serious repercussions. Hence it is important that software that is operated in the field of critical infrastructures is designed and built in a secure manner. The same concerns apply if the IT services are operated in cloud environments. In addition, we analyze the opinions regarding certain security attributes (availability, confidentiality, integrity, and auditing) for diverse IT services in a cloud environment as well as for generic cloud characteristics.

In general we found out that: (1) Information security is generally recognized as a very important matter by critical infrastructure providers. (2) Auditing is not perceived as important as availability, confidentiality, or integrity.

4) Security requirements for IT services: The following four common IT services were chosen for the security requirements elicitation:

- customer web platform
- enterprise management software (e.g. SAP)
- industrial control system / SCADA
- IT infrastructure (e.g. DNS, mail)

Our analysis shows that for the two sectors industry and critical infrastructure providers the smallest differences in information security requirements are for confidentiality and availability. The biggest difference was observed for integrity. Here the members of the industrial sector reported a higher-than-average need for security. In general the industry sector shows slightly higher information security needs than the critical infrastructure providers, as highlighted in Figure 3.

5) Security requirements for generic cloud computing characteristics: In this section the common NIST cloud characteristics on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service are evaluated for their required level of security for the two domains examined. Here the same results as determined in the previous investigation on the security requirements for IT services apply: In general the industry sector shows higher security needs than critical infrastructure providers (Figure 4). The highest requirements are specified for on-demand self-service.

6) Information security topics for a cloud migration guideline: The field information security consists of many controls that could be considered for hardening IT services. The relevance of several information security controls (risk assessment, incident response, SLA management, architectural patterns, service life cycle, socio-technical issues, autonomic security management, forensic and auditing, international standards) was asked for in the survey, shown in Figure 5. The outcome is again comparable with other questions from the survey, where

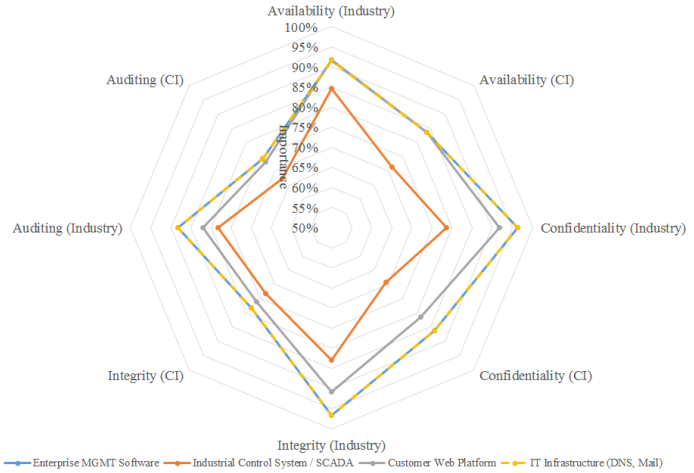

Fig. 3. Net chart of critical infrastructure providers' information security requirements for IT services compared to the industry domain. The industry sector in comparison generally has higher requirements.

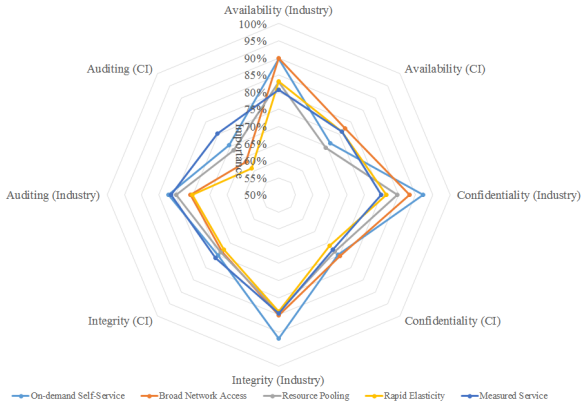

Fig. 4. Net chart of critical infrastructure providers' information security requirements for cloud computing characteristics compared to the industry domain. The industry sector in comparison generally has higher requirements.

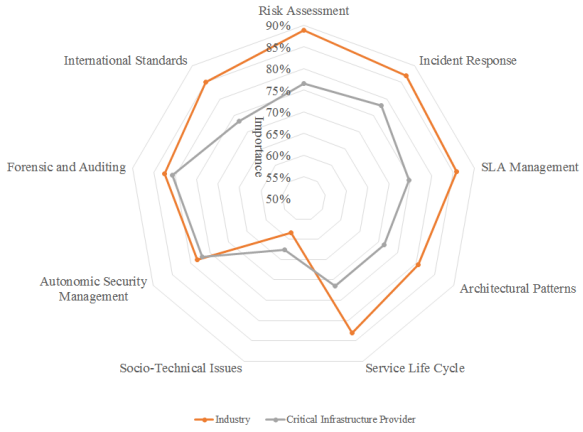

Fig. 5. Importance of information security topics for a cloud migration guideline.

the industry sector generally has a higher need for security as the critical infrastructure providers. Only socio-technical issues are slightly more important to critical infrastructure providers than to industry.

IV. PROCESS-BASED INFORMATION SECURITY MIGRATION GUIDELINE

In this section we, first of all, introduce an extensive set of security controls, which is based on the security topics that we addressed in our questionnaire (Chapter III). We use these security controls to build our taxonomy and use it for evaluating security related guidelines. Finally, based on the evaluation outcome we conclude and propose a process-based guideline(model) for secure service migration towards the Cloud environments.

A. Secure cloud migration taxonomy

The questionnaire results presented in Section III are used as a foundation for building the taxonomy that we present in this section. In our questionnaire we based the security related topics on the initial analysis of the security related aspects within the SECCRIT project[1] with respect to critical infrastructures. Within our taxonomy we now cover a more extensive set of security related topics. This extensive list of topics can be seen in Table III, where we have cross checked these topics with the state of the art security guidelines to investigate how and whether they are being addressed by each one of them.

The taxonomy depicted in Table III includes 34 security controls used for evaluating guidelines, by investigating how they address secure service migration in cloud based environments. Although, each individual security control covers a separate security dimension we use them in our taxonomy to answer the following:

1) *Is the security control enumerated and defined within the observed guideline?*
   Within this question the following security controls are covered: security requirements, privacy requirements, security architecture design, security risk assessment, threat management, vulnerability management, security testing, secure life cycle phases plan, development of security controls, data locality, incident handling, environment hardening, operational enablement, maturity levels, case studies, application migration.
2) *Is the security control implemented in a form of a process?*
   Within this question the following security controls are covered: security requirements, privacy requirements, security and privacy training, security risk assessment, threat management, security testing, regular improvement of security process artifacts, security life cycle phase plan, continuous monitoring of system and services, security planing for the project, integration of proposed concepts in established environments, privacy impact assessment, security accreditation/certification, information disposal, establishing trust strategies, data locality, legal compliance, incident handling, maturity levels, disaster recovery, consideration of security aspects in data migration, application migration.
3) *Does the security control involve architecture or conceptual design?*
   Within this question the following security controls are covered: security architecture design, secure planing for the project, disaster recovery, application migration.

In Table III we detail our results of the analysis of guidelines that support or address migration of services towards Cloud-based environments.
Although being addressed by 60% of guidelines[26], [27], [28], [29], [30], [24] the first two controls, security and privacy requirements, are unfortunately either enumerating a narrow set of requirements or referencing a third party set. Most of the evaluated guidelines[26], [27], [30], [24] provide adequate approaches for increasing awareness for security and privacy in form of a training to support the enumerated requirements. However, only [26], [30], [24] provide concrete steps for accomplishing this requirement. Next security control is the security architecture design where we investigated the proposed architectural solutions and entailing processes, which were supported only by 50% of the guidelines[26], [27], [28], [30], [31] that we addressed. Whereby from these 50% only [26], [28] provide a generic solutions. Furthermore, security risk assessment was addressed by the majority of the evaluated guidelines where only 10% of the guidelines [32] have not included or considered it as relevant. However, only the following from the above mentioned guidelines detail the risk assessment approach [26], [27], [29], [24], others provide only a generic solutions. Although, threat management and vulnerability management are essential for implementing risk assessment, only 40% of guidelines[26], [29], [30], [24] support threat management whereas 50% of guidelines[26], [27], [30], [31], [24] support vulnerability assessment. In case of threat management only ENISA [29] is providing a generic solutions, whereas in case of vulnerabilities only NIST cyber security framework[24] is focusing only on generic solutions. Consideration of security practices during the development phase are unfortunately supported by only 20% of evaluated guidelines[26], [31] focusing on generic solutions, where as performing security tests was covered by only 50% of guidelines[26], [27], [29], [30], [31] most of them providing a detailed approach for tests handling. Improvement of security related processes is a continuous requirement which was supported by 50% of guidelines[26], [27], [31], [24], [33]. Formulating structured life-cycle phases for performing certain actions or tasks was embraced by 50% of the guidelines[26], [27], [30], [31], [34]. Processes for delivering continuity in terms of monitoring systems or services was defined by 60% of evaluated guidelines[26], [27], [28], [29], [24], [33]. Furthermore, only 50% of evaluated guidelines[26], [27], [28], [30], [33] implement security planning as process. The evaluation

[1]SECCRIT project, https://www.seccrit.eu

shows that only CSA[31] advises in their guideline how to integrate the proposed concepts.

The assessment of privacy concerns was covered by the minority, only 30% of guidelines[26], [27], [28]. We investigated whether the guidelines support development of security related controls but unfortunately it was addressed only by only 40% of evaluated guidelines. The NIST SP800-64[27] was the only guideline interested in accreditation or certification processes and information service disposal. Suggesting processes or models related with establishing trust was a topic addressed only by 20% of guidelines[27], [34] where Microsoft[34] proposed a solution on a use case scenario for their Windows Azure. A very important security control which was also considered in our Section III-B is geographical location of the data addressed by only 30% of guidelines[28], [33], [34].

Legislative requirements were one of a most referred points which were addressed through compliance and legislative requirements from 70% of guidelines[27], [28], [29], [30], [31], [33], [34]. However, due to the area-specific and often nationally bound nature of legal requirements, it cannot be expected from these guidelines to provide universal and sufficient guidance here. Solutions for handling incidents was proposed by 60% of guidelines[26], [27], [28], [29], [31], [24]. The Software Assurance Maturity Model (SAMM)[30] was the only guideline concerned with hardening and operational enablement. Only 20% of guidelines[32], [30] proposed and define maturity levels in their work. The Software Assurance Maturity Model (SAMM)[30] and Microsoft [34] supported their guidelines with a use case. Disaster recovery solutions and concepts were proposed from 40% of the guidelines[27], [32], [34], [30]. Consideration of security aspects during migration is only addressed by 30% of the guidelines[33], [31], [32]. Finally, only 30% of the guidelines[33], [34], [32] address and propose application migration concepts or processes which are tightly related with the technology the guideline was made for.

The results from our detailed evaluation show that Microsoft SDL[26], NIST SP 800-64 [27], and Software Assurance Maturity Model [30] are the guidelines that fulfill most of the security related controls, Table III Coverage of security controls per guideline, that we used in our taxonomy. Not all of the controls have been covered by at least one of the guidelines. Therefore, we propose a comprehensive solution for handling such a scenario in the following section.

B. Secure cloud migration life cycle

To use such a taxonomy in an effective way, it should be incorporated into a process that gives attention to the information security aspects of *cloudification*.

According to our literature review there is currently no security development life cycle that explicitly takes into account a cloud migration scenario. We therefore propose a novel approach for a Cloudification Security Development Life cycle (CloudSDLv1) of IT services which we base on common security development life cycles [26], [27], [30]. Our approach for CloudSDLv1 is shown in Figure 6. It is built around the security requirements relevant to the *cloudified* product.

We consider the following use cases for CloudSDLv1:

- Software development for cloud environment from scratch.
- Software migration from legacy system to cloud (adoption for cloud).
- Software migration from private to public cloud and vice versa.

CloudSDLv1 comprises five phases:

1) Analysis: In this phase a decision is made upon which service or which part of a service is to be migrated to cloud. The IT service that is to be *cloudified* is analyzed for cloud fitness and the initial set of security requirements is specified. Ideally, if security requirements for the IT service already exist they have to be taken into account and if needed adopted to the new circumstances. In particular, this should also include security requirements indirectly resulting from the *cloudification* of a certain service. For example, this might refer to novel needs for providing credible digital evidence on the providers' security-related conduct for the potential case of legal conflicts or to cloud-specific requirements from data protection law. In this phase we also suggest to analyze which implications the *cloudification* of the IT service has on the organization and the business. Any implications on information security have also to be converted into security requirements.

2) Design: In the design phase the software architecture for the to-be-migrated IT service is constructed on the basis of the security requirements specified in the analysis phase. If necessary refinements to the security requirements are made.

3) Implementation: Based on the design the software is implemented. If necessary refinements to the security requirements are made. Additionally in this phase the organization is, where necessary, prepared for the use of the *cloudified* IT service.

4) Verification: In the verification phase the software is tested against the specified security requirements. Also the readiness of the organization for the *cloudified* IT service is verified.

5) Deployment: In this final phase of the CloudSDLv1 the IT service is deployed on the cloud environment, taking into account the security requirements related to platform configuration.

V. Conclusion

In this paper we have show that the major difference in importance of information security topics between industrial stakeholders and critical infrastructure provider is geolocation. This means that storing data within the same legal domain is more important for critical infrastructure provider than for industrial stakeholder, other than that interests are aligned. We have used this information to survey existing industrial and critical infrastructure guidelines to update our initial set of security controls and fed this into a proposal for a cloudification guideline for critical infrastructure providers. We present a novel approach for a process-based information security guideline. The presented taxonomy together with

TABLE III
STANDARDS AND GUIDELINES FOR MIGRATING CRITICAL INFRASTRUCTURE SERVICES TO TAXONOMY

SECURITY CONTROLS	Microsoft: Security development lifecycle	NIST SP800-64: Security Considerations in the System Development Life Cycle	NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing	ENISA: A CIIP perspective on cloud computing services	OPENSAMM: A guide to building security into software development	CSA: Security guidance for critical areas of focus in cloud computing	NIST: Framework for Improving Critical Infrastructure Cybersecurity	Migrating your Existing Applications to the AWS Cloud	Moving Applications to the Cloud on Microsoft Azure	Cloud migration research: A systematic review	Control implemented in Percentage of Guidelines
Security Requirements	x	x	x	x	x		x				60%
Privacy Requirements	x	x	x	x	x		x				60%
Security& Privacy Training	x	x			x		x				40%
Security Architectural Design	x	x	x		x	x					50%
Security Risk Assessment	x	x	x	x	x	x	x	x	x		90%
Threat Management	x			x	x		x				40%
Vulnerability Management	x	x			x	x	x				50%
Secure Coding Practices	x					x					20%
Security Testing	x	x		x	x	x					50%
Regular Improvement of Security Process Artefacts	x	x				x	x	x			50%
Security Life Cycle Phases Plan	x	x			x	x			x		50%
Continuous monitoring of systems and services	x	x	x	x			x	x			60%
Security Planning for the Project	x	x	x		x			x			50%
Integration of proposed Concepts in Established Environments						x					10%
Privacy Impact Assessment	x	x	x								30%
Development of Security Controls		x				x	x	x			40%
Security Accreditation/Certification		x									10%
Information Disposal		x									10%
Establish trust strategies			x						x		20%
Data locality			x					x	x		30%
Legal compliance		x	x	x	x	x		x	x		70%
Incident Handling	x	x	x	x		x	x				60%
Environment Hardening					x						10%
Operational Enablememt					x						10%
Maturity Levels					x					x	20%
Case Studies					x				x		20%
Disaster Recovery		x				x	x			x	40%
Consideration of Security Aspects in Data Migration						x		x		x	30%
Application Migration								x	x	x	30%
Coverage of Security Controls:	**52%**	**62%**	**38%**	**28%**	**52%**	**48%**	**38%**	**31%**	**24%**	**14%**	

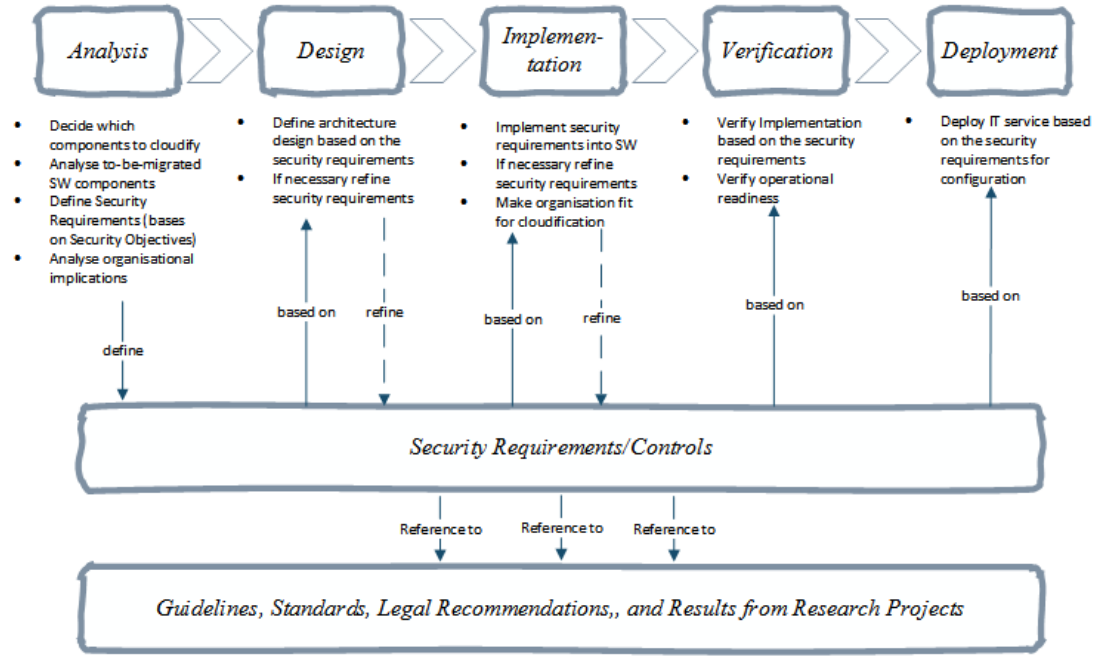

Fig. 6. Process-based information security guideline for cloud migration

the proposed *cloudification* security development life cycle (CloudSDLv1) will support critical infrastructure providers in migrating their legacy IT services to the cloud. Based on this work our next steps will be a) an extension of the presented taxonomy towards research results of the EU FP7 research project SECCRIT, and b) empirical evaluation of our taxonomy and CloudSDLv1 in a real world scenario.

ACKNOWLEDGEMENTS

The research presented in this paper has been funded by the European Union (H2020 project PRISMACLOUD, Grant No. 644962 and FP7 project SECCRIT, Grant No. 312758).

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X08001957

[2] R. Buyya, "Market-Oriented Cloud Computing: Vision, Hype, and Reality of Delivering Computing As the 5th Utility," in *Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, ser. CCGRID '09. Washington, DC, USA: IEEE Computer Society, 2009. [Online]. Available: http://dx.doi.org/10.1109/CCGRID.2009.97

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology*, vol. 53, no. 6, p. 50, 2009.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[5] K. Sun and Y. Li, "Effort Estimation in Cloud Migration Process," in *Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on*, March 2013, pp. 84–91.

[6] A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, and P. Teregowda, "Decision Support Tools for Cloud Migration in the Enterprise," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, July 2011, Service migration, pp. 541–548.

[7] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud Migration Research: A Systematic Review," *Cloud Computing, IEEE Transactions on*, vol. 1, no. 2, pp. 142–157, July 2013.

[8] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of internet services and applications*, vol. 1, no. 1, pp. 7–18, 2010.

[9] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, April 2010, pp. 27–33.

[10] S. Kaisler and W. Money, "Service Migration in a Cloud Architecture," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, Jan 2011, Service migration, pp. 1–10.

[11] A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, "Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, July 2010, Service migration, pp. 450–457.

[12] C. Fehling, F. Leymann, S. Ruehl, M. Rudek, and S. Verclas, "Service Migration Patterns – Decision Support and Best Practices for the Migration of Existing Service-Based Applications to Cloud Environments," in *Service-Oriented Computing and Applications (SOCA), 2013 IEEE 6th International Conference on*, Dec 2013, Service migration, pp. 9–16.

[13] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *International Journal of Critical Infrastructure Protection*, no. 0, pp. –, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548214000791

[14] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804510001281

[15] B. Kandukuri, V. Paturi, and A. Rakshit, "Cloud Security Issues," in *Services Computing, 2009. SCC '09. IEEE International Conference on*, Sept 2009, Security, pp. 517–520.

[16] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X10002554

[17] R. Piggin, "Are industrial control systems ready for the cloud?" *International Journal of Critical Infrastructure Protection*, no. 0, pp. –, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548214000821

[18] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol. 1, March 2012, Security, pp. 647–651.

[19] M. Jensen, J. Schwenk, N. Gruschka, and L. Iacono, "On Technical Security Issues in Cloud Computing," in *Cloud Computing, 2009. CLOUD '09. IEEE International Conference on*, Sept 2009, Security, pp. 109–116.

[20] M. Nanavati, P. Colp, B. Aiello, and A. Warfield, "Cloud Security: A Gathering Storm," *Commun. ACM*, vol. 57, no. 5, pp. 70–79, May 2014. [Online]. Available: http://doi.acm.org/10.1145/2593686

[21] M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: A survey," *Liverpool John Moores University, United Kingdom, Tech. Rep*, 2013.

[22] S. Paudel, M. Tauber, C. Wagner, A. Hudic, and W.-K. Ng, "Categorization of standards, guidelines and tools for secure system design for critical infrastructure it in the cloud," in *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on*, Dec 2014, pp. 956–963.

[23] M. Dekker, "Critical Cloud Computing:CIIP Perspective on Cloud Computing," 2013, [Online; accessed 19-July-2013].

[24] N. I. of Standards, T. (NIST), and U. S. of America, "Framework for improving critical infrastructure cybersecurity," 2014.

[25] J. Morin, J. Aubert, and B. Gateau, "Towards cloud computing SLA risk management: issues and challenges," in *System Science (HICSS), 2012 45th Hawaii International Conference on*. IEEE, 2012, pp. 5509–5514.

[26] M. Howard and S. Lipner, *The security development lifecycle*. O'Reilly Media, Incorporated, 2009.

[27] R. Kissel, K. M. Stine, M. A. Scholl, H. Rossman, J. Fahlsing, and J. Gulick, "SP 800-64 Security Considerations in the System Development Life Cycle," 2008.

[28] W. Jansen, T. Grance *et al.*, "Guidelines on security and privacy in public cloud computing," *NIST special publication*, vol. 800, p. 144, 2011.

[29] M. Dekker, "Critical Cloud Computing-A CIIP perspective on cloud computing services," *white paper, December*, 2012.

[30] P. Chandra, "The Software Assurance Maturity Model - A guide to building security into software development," 2009.

[31] CSA, "Security guidance for critical areas of focus in cloud computing," *Cloud Security Alliance*, 2011.

[32] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: a systematic review," *Cloud Computing, IEEE Transactions on*, vol. 1, no. 2, pp. 142–157, 2013.

[33] J. Varia, "Migrating your existing applications to the aws cloud," *A Phase-driven Approach to Cloud Migration*, 2010.

[34] D. Betts, A. Homer, A. Jezierski, M. Narumoto, and H. Zhang, "Moving applications to the cloud on microsoft azure," *MSDN Library*, 2012.