Leveraging the Potential of Cloud Security Service Level Agreements through Standards

Jesus Luna, Neeraj Suri, Michaela Iorga and Anil Karmel

***Abstract*: Despite the undisputed advantages of Cloud computing, customers (in particular small and medium enterprises – SMEs) are still in need of "meaningful" understanding of the security and risk management changes that the Cloud entails, in order to assess if this new computing paradigm is "good enough" for their security requirements. This article presents a fresh view on this problem by surveying and analyzing, from the standardization and risk assessment perspective, the specification of security in Cloud Service-Level Agreements (secSLA) as a promising approach to empower customers in assessing and understanding Cloud security. Apart from analyzing the proposed risk-based approach and surveying the relevant landscape, this paper presents a real-world scenario to support our advocacy of creation and adoption of secSLAs as enablers for negotiating, assessing, and monitoring the achieved security levels in Cloud services.**

***Keywords:* Cloud, metrics, risk management, security assessment, SLA, standards.**

I. Introduction

The varied functional and economic benefits of the Cloud are substantial. However, security assurance and transparency remain as significant open issues to enable the customer's trust in Cloud Service Providers (CSPs). Both of these issues become even more complex to manage when we consider the growing number of CSPs offering diverse Cloud-enabled services (from virtual machines and storage, to transactional databases), and new architectures leveraging the services of more than one CSP (e.g., the Cloud supply chain shown in Figure 1). The latter setup is typically referred to as a Multi-Cloud System (MCS) [11] and it opens unique challenges of inter-Cloud interfaces, issues of consistent access controls and many other complex but necessary issues.

As state of practice, a commonly utilized approach by CSPs has relied on the adoption of security certifications based on standardized "controls frameworks" (e.g., ISO/IEC 27002 [2] or the upcoming 27017 [4]) to provide customers a reasonable degree of security assurance and transparency. Many CSPs are increasingly adopting Cloud-specific security controls frameworks such as the Cloud Security Alliance's Cloud Control Matrix (CSA CCM, www.cloudsecurityalliance.org/cm.html) and National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 [3]. Based on well-known standards, most of these security control frameworks allow for interoperability between CSPs, hence easing the deployment of MCS.

However, in order to provide Cloud[1] assurance and transparency, the actual use of security control frameworks has proven rather limited in practice. Over the implementation of their security controls framework, the CSP can only assume the type of data a customer will generate and use; the CSP is not aware of the additional security requirements or the tailored security controls deemed necessary to protect the customer's data. Conversely, customers can typically only obtain a coarse view of the CSP's security policies and implemented mechanisms. Such limitations are problematic for deploying advanced features such as monitoring and end-to-end security assurance in MCS.

Work supported in part by EC SPECS.

J. Luna is with the Cloud Security Alliance (Europe), Scotland, U.K and at TU-Darmstadt, Hochschulstr. 10, 64289 Darmstadt, Germany; email: jluna@cloudsecurityalliance.org . Phone: +49 6151 4291707
N. Suri is with TU-Darmstadt, Hochschulstr. 10, 64289 Darmstadt, Germany; email:suri|@cs.tu-darmstadt.de , Phone: +49 6151 16-3513
M. Iorga is with National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899-1070, U.S.A; email: michaela.iorga@nist.gov . Phone: +1 301-975-843A.
A. Karmel is with C2 Labs, One Freedom Square 11951, Reston, VA 20190. U.S.A; email: akarmel@c2labs.com , Phone: +1 703-251-4492

[1] Henceforth, Cloud will refer to both single-CSP systems and MCS.

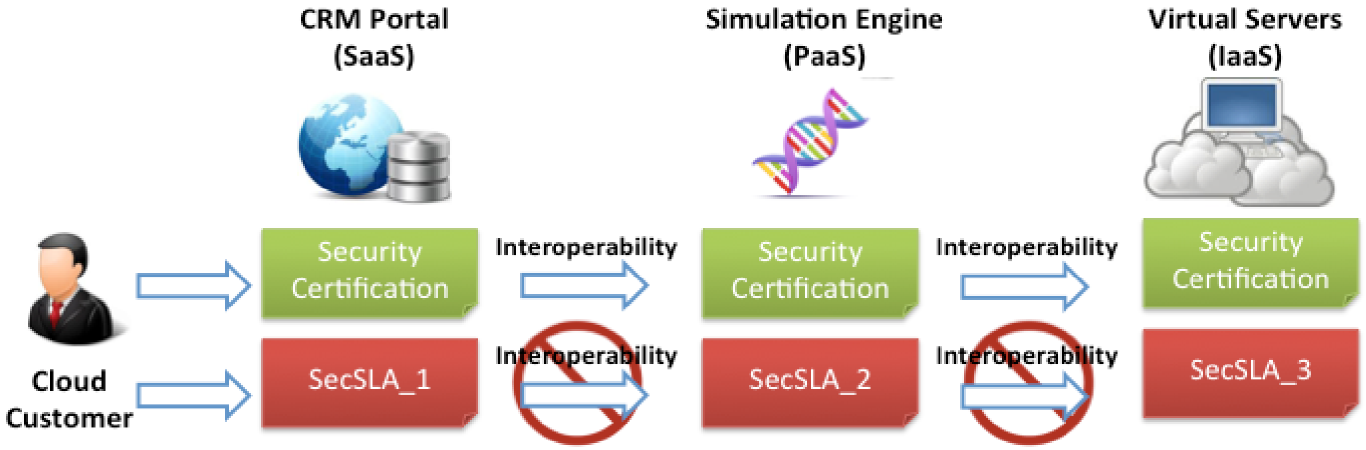


Figure 1. Standardized Security Control Frameworks and Non-standardized secSLAs in a MCS Cloud Supply Chain

Thus the customers crucially require mechanisms (and also tools) that can enable them to understand and assess what "good-enough security" [1] means, and especially the new challenges in risk assessment/management (e.g., continuous assessment, and risk composition in MCS) that the Cloud entails. In this context, and as also highlighted by the European Commission's Cloud Computing strategy (ec.europa.eu/digital-agenda/node/10565), the use of contracts and Service Level Agreements (SLAs) become key components driving Cloud services. According to the ETSI Cloud Standards Coordination group [13], SLAs should facilitate Cloud customers in understanding (i) the claims behind the Cloud service, and (ii) relate such claims to their own requirements. A recent report from NIST [8] and also the European Commission[2] considers SLAs as the dominant means for CSPs to establish their credibility, attract or retain Cloud customers since they will be used as a mechanism for service differentiation. These reports suggest the use of Cloud SLAs to develop better assessments and perform informed customer decisions, and ultimately improve trust and transparency between Cloud stakeholders.

In order to better leverage the benefits of Cloud SLAs from a security perspective, multiple stakeholders in the Cloud community (e.g., the European Network and Information Security Agency -ENISA[3]-, ISO/IEC [5], NIST, and the European Commission) have identified that specifying security parameters in Service-Level Agreements (termed as *secSLA* in this article) is useful to establish common semantics to provide and manage security assurance both for CSPs, and Cloud customers. As discussed in Section II, Cloud secSLAs allow a CSP to describe implemented security controls, associated metrics, and committed CSP values for those metrics. From a customer perspective, secSLAs allow for a more transparent view of the security levels offered by the CSP, while at the same time provide information to monitor the fulfillment of the customer's security expectations. Unfortunately, the lack of relevant Cloud (security) SLA standards is a barrier for its adoption.

Using the standardization perspective, this article surveys and analyzes the challenges of the specification and usage of Cloud secSLA. In order to scope our analysis, this paper departs from the classical notion of risk management framework~~s~~ (RMF) advocated by relevant working groups at ISO/IEC, the European Commission, NIST, and the Cloud Security Alliance. Instead, we combine the result of traditional RMF with security metrics techniques to develop the secSLA elements and framework that allow their assessment and continuous monitoring. Furthermore, by analyzing the standardization landscape and presenting a real-world use case of US Department of Energy's YOURcloud (energy.gov/sites/prod/files/IT%20Modernization%20Strategy_0.pdf), we support the creation of common vocabularies, metrics, and frameworks for the management of Cloud secSLAs.

Our vision aims to benefit both assurance and transparency by motivating the use of standardized secSLAs to create customer-centric approaches/tools for negotiating, assessing, and measuring security over the Cloud supply chain.

Paper Structure:

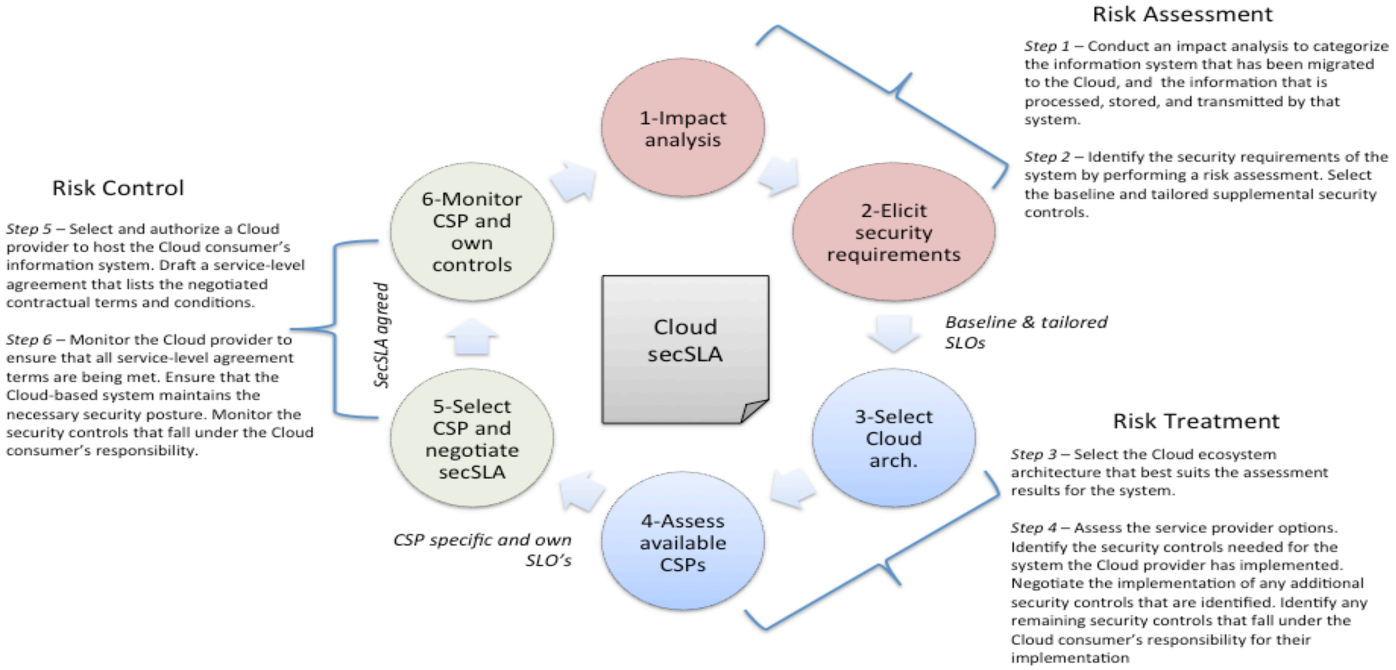
This article is organized as follows: Section II introduces the concepts of secSLA through risk management activities. Section III analyses the standardization landscape related to Cloud secSLAs. A real-world use case related to the usage/benefits of standards for Cloud secSLAs is presented in Section IV.

II. Good-enough Cloud Security through Service-Level Agreements

Sandhu [1] introduced the concept of *good-enough security* driven by the principle of "everything should be made as secure as necessary, but not securer." The classical PDCA approaches (Plan-Do-Check-Act [2]) are increasingly being

[2] Please refer to "Cloud Computing Service Level Agreements: Exploitation of Research Results," European Commission, Tech. Rep., 2013.

[3] ENISA's report "Survey and analysis of security parameters in Cloud SLAs across the European public sector."



Step 1 – Conduct an impact analysis to categorize the information system that has been migrated to the Cloud, and the information that is processed, stored, and transmitted by that system.

Step 2 – Identify the security requirements of the system by performing a risk assessment. Select the baseline and tailored supplemental security controls.

Step 3 – Select the Cloud ecosystem architecture that best suits the assessment results for the system.

Step 4 – Assess the service provider options. Identify the security controls needed for the system the Cloud provider has implemented. Negotiate the implementation of any additional security controls that are identified. Identify any remaining security controls that fall under the Cloud consumer's responsibility for their implementation

Step 5 – Select and authorize a Cloud provider to host the Cloud consumer's information system. Draft a service-level agreement that lists the negotiated contractual terms and conditions.

Step 6 – Monitor the Cloud provider to ensure that all service-level agreement terms are being met. Ensure that the Cloud-based system maintains the necessary security posture. Monitor the security controls that fall under the Cloud consumer's responsibility.

Figure 2. Cloud secSLA development within a standardized Risk Management Framework

considered by SMEs for assessing and managing their IT risk and security exposure following adoption of Cloud services. Consequently we explore, from a standardization perspective, the synergies across risk management frameworks and secSLAs as a means to achieve "good-enough security" in the Cloud.

A. Cloud secSLAs: A "Risky Business"

Organizations targeting Cloud secSLA as a means to implement good-enough security typically start with an introspective view that identifies both the assets to protect, and the (probabilistic) risks to consider when migrating to the Cloud (cf., NIST SP 800-30 [6] and ENISA's report[4]). The NIST *Guide for Applying the Risk Management Framework to Federal Information Systems* (RMF) [15] provides a structured process that integrates information security and risk management activities into the system development life cycle. The selected Cloud delivery model (public, private, hybrid, community) and the service type (SaaS, PaaS, IaaS), in association with security controls selected for the ecosystem, need to be chosen such that the system preserves its security requirements. Therefore, a systematic risk management cycle helps ensure that the residual risk is minimal, and that the deployed Cloud system achieves a security level that is at least equivalent to the one offered by an on-premise (non-Cloud) technology architecture or solution. Conversely, the use of an MCS has an impact on the distribution of security responsibilities among the Cloud actors part of the supply chain, as related to the security conservation principle [14].

Despite the variety of approaches in Cloud risk management [15], the challenges associated with MCS (cf., Figure 1) and also secSLAs from a risk management perspective have only recently resulted in new approaches. The key elements for the successful adoption of a Cloud solution based on secSLAs are the Cloud consumer understanding of the (a) Cloud-specific characteristics, (b) the architectural components for each Cloud service type and deployment model, (c) along with each Cloud actor's precise role in orchestrating a secure ecosystem. The Cloud customer's confidence in accepting the risk from using Cloud services depends on how much trust they place in the entities orchestrating the Cloud ecosystem. The risk management process ensures that issues are identified and mitigated early in the investment cycle and followed by periodic reviews. As Cloud customers and the other Cloud actors involved in securely orchestrating a Cloud ecosystem (cf., Figure 1) have varying degrees of control over Cloud-based IT resources, they need to share the responsibility of implementing and monitoring the security requirements.

Furthermore, it is essential for the Cloud consumers' business -critical processes to identify Cloud-specific risk-adjusted security controls. Cloud consumers need to leverage their contractual agreements to hold the Cloud providers (and Cloud brokers, when applicable) accountable for the implementation of the security controls. They also need to assess the correct implementation and continuously monitor all identified security controls. Draft NIST SP 800-173, *Cloud-Adapted Risk Management Framework (CRMF)* [7], is a key approach addressing the elements of a successful Cloud risk management strategy to enable the usage of secSLAs. CRMF was first highlighted in NIST SP 500-299 [14] as a cyclically executed process composed of a set of coordinated activities for overseeing and controlling risks. This set of activities consists of the following tasks:

[4] Please refer to ENISA's report "Cloud Computing Benefits, risks and recommendations for information security."

- Risk Assessment
- Risk Treatment
- Risk Control

These tasks collectively target the enhancement of security through secSLAs, which goes beyond the capabilities offered by widely used security control frameworks. CRMF provides a consumer-centric approach following the original RMF, identifying the six steps shown in Figure 2.

A risk-based approach to managing information systems is an holistic activity that should be integrated into every aspect of the organization, from planning and system development life cycle processes (Steps 1 – 2 in Figure 2) to security controls allocation (Steps 3 – 5). The resulting set of security controls (baseline, tailored controls, controls inherited from providers and under customer's direct implementation and management) lead gradually to the creation of the secSLA in the CRMF's Step 5, as explained next. The recently published ENISA report on security frameworks for Governmental Clouds[5] (GovClouds) highlights the real-world applicability of the process described in this section. The GovClouds analyzed by this report have adopted a similar risk-based approach to elicit the security controls that offer the security level that is adequate for their operation. Furthermore, ENISA's report shows how selected security controls are the basis to develop the GovCloud's (security) SLAs.

B. *Deriving secSLA from CRMF-elicited security controls*

The key element of a Cloud secSLA, and possibly the most notable difference to a control framework, is specifying the Service-Level Objectives (SLOs). The ISO/IEC standard on Cloud SLA [5] defines SLO as "the objectives concerning Cloud services that are recommended to consider by a Cloud customer in order to assess and make informed decisions about the CSP." Typically a SLO is assessed through *metrics* (either quantitative or qualitative), where the SLO metrics are used to set the boundaries and margins of errors CSPs have to abide by (along with their limitations). In the rest of this section is presented an approach to define "good-enough" security SLOs for the Cloud supply chain.

Considering the advocated familiarity of practitioners with security controls frameworks, the EC's Cloud Select Industry Group on Service-Level Agreements C-SIG SLA (ec.europa.eu/digital-agenda/en/cloud-select-industry-group-service-level-agreements) proposed an approach that iteratively refines individual controls into *measurable* security SLOs. The elicited SLOs metrics are subsequently mapped to a conceptual model (such as the one proposed by the members of the NIST Public RATAX Working Group [8]). Figure 3 shows an example of the presented refinement approach. CSA is currently composing a catalog[6] of Cloud security metrics to support this process.

For a MCS scenario (cf., Figure 1), the described process also needs consider the dependencies between Cloud services in the supply chain. Thus, it does not suffice to understand how the part of the service under the *front CSP* control affects its own customers, but also how the sub-services contribute to the overall offered Cloud secSLA. Hence, there is a distinct need for *aggregation of security metrics guaranteed by single Cloud services in order to get values for a composition (MCS)*. Recent academic works have proposed initial approaches to solve the secSLA aggregation problem utilizing multi-criteria decision based techniques[7].

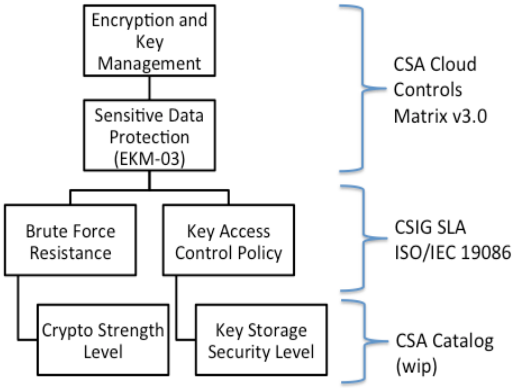

Encryption and Key Management
Sensitive Data Protection (EKM-03)
Brute Force Resistance
Key Access Control Policy
Crypto Strength Level
Key Storage Security Level
CSA Cloud Controls Matrix v3.0
CSIG SLA ISO/IEC 19086
CSA Catalog (wip)

Figure 3. Refining Security Controls into SLO and Metrics

The security SLOs developed by the Cloud customer can become the actual "security requirements" to communicate to the CSP before acquiring the Cloud service. These SLOs provide a *common semantic* that both customers and providers can use to *negotiate* the Cloud secSLA (cf., Section IV).

The EC SPECS project (Secure Provisioning of Cloud Services based on SLA Management, specs-project.eu/) is investigating this topic to propose a customer-centric framework to manage Cloud security based on secSLAs. The framework is composed of techniques (e.g., security evaluation) and tools (e.g., machine readable secSLA specification, security dashboards) to enable the negotiation, monitoring, and enforcement of Cloud secSLAs. Apart from SPECS, EU projects such as A4Cloud (www.a4cloud.eu/), SLA@SOI (sla-at-soi.eu/), Contrail (contrail-project.eu/) and OPTIMIS (www.optimis-project.eu/) have devoted significant efforts to develop Cloud SLAs with a subset of common elements and metrics that can be also applicable to secSLAs. These projects study the challenges associated to the use of Cloud SLAs from both technical and legal perspectives, as in the case of A4Cloud. The European Commission recently published a detailed analysis of the relationship between EU research results and Cloud SLAs[8]. The working groups such as CSIG SLA have followed similar approaches to elicit SLOs and metrics as presented in a recent report [10]. Section III further presents and analyzes the standardization landscape related with Cloud secSLA.

[5] Please refer to http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds

[6] The security metrics catalog is still under development, but interested readers can contact the corresponding author for obtaining access.

[7] A. Taha, R. Trapero, J. Luna and N. Suri, "AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security". In Proc. of IEEE Trust, Security and Privacy in Computing and Communications. 2014.

[8] Please refer to Footnote #2.

The next section discusses Steps 5 – 6 in Figure 2, related to the secSLA monitoring.

C. *Risk control through Cloud secSLA.*

Once a Cloud secSLA is built and agreed with the CSP, the customer now has a mechanism to monitor the fulfillment of the requested SLOs. This is the essence of the *risk control* stage in CRMF. In theory, after the mechanisms for monitoring Cloud secSLAs are in place, it is possible to assess both the fulfillment of agreed security SLOs and also potential deviations from expected values (i.e., SLA violations). Intuitively these violations can be managed by the CSP through actions ranging from changes to the current secSLA, to termination of the agreed Cloud service.

Despite the apparent feasibility of this control/monitoring approach, to the best of our knowledge, there are very few efforts exploring this area. One of the recent developments in the area of continuous monitoring is CSA's CTP: Cloud Trust Protocol (cloudsecurityalliance.org/research/ctp/) builds an open API to enable Cloud customers to query CSPs about the security level of their services. A key design choice that has shaped CTP is the focus on the monitoring of security metrics (secSLAs), rather than the monitoring of security controls.

As mentioned in Section I, a barrier limiting the development of such secSLA monitoring solutions arises from the lack of Cloud standards associated with SLAs, SLOs, and metrics/measurements. Standards such as ISO/IEC 19086 [5] could become the enabler for possible solutions. The following section presents the relevant secSLA standardization landscape.

III. The Road to Standardization

The activities to standardize secSLAs are mostly included on the (few) initiatives targeting the overall standardization of Cloud SLAs. This section elaborates the need for standards in the field of Cloud (security) SLAs and analyzes the standardization landscape.

A. *Why standards for Cloud security SLAs?*

While secSLAs form key components defining security elements in a Cloud ecosystem, they are arguably the least understood Cloud attributes given the complex language and terms of service from both a technical and legal perspective. This is exacerbated by the lack of standard frameworks and vocabularies, along with a paucity of metrics/measurements associated with SLOs.

As input for this paper, at the SecureCloud2014 conference we conducted a survey on SLA usage and needs among 200 Cloud customers/CSPs *(80% from the private sector, 15% from the public sector)*. The two top reasons why Cloud SLAs are important were *(1)* being able "to better understand the level of security and data protection offered by the CSP" (41%), and *(2)* "to monitor the CSP's performance and security levels" (35%).

Furthermore, the key issues needed to make Cloud SLAs "more usable" for Cloud customers highlighted: *(1)* the need for "clear SLO metrics and measurements" (66%); *(2)* "making the SLAs easy to understand for different audiences" (62%); *(3)* "having common/standardized vocabularies" (58%); and *(4)* "clear notions of/maturity of SLAs for Security" (52%). These responses constitute empirical indicators of the need to develop standards.

It is worth noting that the European Cloud Computing Strategy (ECCS) calls for the identification and development of standardized solutions for contract terms (including SLAs), to increase consumer trust and encourage wider adoption of Cloud services.

B. *Analyzing the current standardization landscape.*

Standardization bodies (e.g., ISO/IEC) and best-practices organizations (e.g., CSA) are currently devoting several efforts to the study of Cloud SLAs. While not specifically focused on security, this is an aspect that has proved very challenging (cf., Section II). In general, a major activity in relevant Standards Development Organizations (SDOs) focuses on the definition of common vocabularies, taxonomies, metrics/measurements, and techniques to negotiate and specify them in machine-readable languages (e.g., based on WS-Agreement).

The initial report on Cloud secSLA was published by ENISA (cf., Section I), analyzing the use of security parameters in (EC public sector) Cloud SLAs. ETSI also highlights the need for standardized and measurable SLAs for the Cloud's supply chain, even though ETSI does not elaborate on any particular proposal [13].

A key Cloud SLA standardization activity is being carried out by ISO/IEC JTC 1/SC38 on "19086 - Information Technology (Cloud Computing) Service-Level Agreement (SLA) Framework and Terminology" [5]. This prospective standard will be divided in four parts as:

1. The definition of a standardized framework for Cloud SLAs including both a vocabulary and comprehensive catalogue of commonly used SLOs.
2. The definition of Cloud SLA-related metrics.
3. Core requirements for implementation.
4. Security and privacy in Cloud SLAs[9].

From the set of ISO/IEC 19086 standards, Part 4 represents a major achievement in the area of Cloud secSLAs, where approaches associated with the specification and the usage of secSLAs are expected to be discussed (cf., Section II). This upcoming standard acknowledges the importance of developing common SLOs and metrics for security SLAs. Ongoing efforts that may become a foundation for ISO/IEC 19086 Part 4 are presented next.

NIST SP 800-173 (draft) [7] defines the types of boundaries of different trust levels or architectural considerations that consumers need to identify and secure. These boundaries and the security control sets outlined by them are supporting the identification and development of the security SLA/SLO terms, and associated monitoring (continuous diagnostic and

[9] At the time of writing, the draft ISO/IEC 19086 Part 4 was not yet released.

mitigation) during operations. This is also relevant for Cloud secSLAs is NIST SP 800-174 (draft) [9], which targets the identification of security controls from [3] applicable in a Cloud ecosystem for each security capability leveraged in NIST SP 500 -299, *Cloud Computing Security Reference Architecture* (SRA) [14]. The final goal is to identify which specific security controls from the SP 800-53 R4 catalog actually apply to components of the architecture, in order to focus the elicitation of relevant security SLOs.

The ECCS has identified three key actions to improve the uptake of Cloud computing in the EU. One action is directly related to Cloud SLAs leading to the creation of the C-SIG SLA working group. The C-SIG SLA group has already released initial customer guidance on Cloud SLAs [12] containing a list of relevant SLOs (including security related). C-SIG SLA also published a set of Cloud SLA standardization guidelines (including a common vocabulary and indicative list of security SLOs) [10] that will become part of the EC feedback to ISO/IEC 19086 Part 4. Finally the CSA, through its Service-Level Agreements/Cloud Trust working groups, is focusing on the definition of security SLOs, metrics, and techniques to reason about them. For these purposes, CSA is developing an online repository of security metrics definitions (cf., Section III.B) to contribute to ISO/IEC 19086. Part 4

IV. Case Study: (DOE)'s YOURcloud

This section presents a real-world use case showing the usage of Cloud secSLAs, and the benefits of standards in this area. The U.S. DoE's National Nuclear Security Administration (NNSA) is responsible for the safety, security, and reliability of the U.S. Nuclear Weapons Stockpile. Given the nature of its work and the autonomous nature of its national labs and plants, the department required a Cloud architecture that respected site autonomy, leveraged the power and scale the Cloud had to offer, and effectively managed the security of its systems. These design principles led the department to DOE's YOURcloud (cf., Figure 4), a MCS approach powered by a secSLA-driven Cloud service broker able to implement realistic levels of security automation.

In order to provide Cloud services within YOURcloud, prospective CSPs must go through an accreditation scheme that guarantees a baseline security level (i.e., a minimum secSLA) through the system. Customer organizations that are members of DOE's YOURcloud authorize target CSPs for use by their home organization. Organization-level secSLAs associated to baseline security levels, are manually agreed and contractually enforced by NNSA with each CSP. As presented in Section II, YOURCloud's secSLAs contain security controls and associated SLOs related to the offered Cloud services (e.g., virtualization security for IaaS). Despite security controls are based on standardized frameworks adopted by accredited CSPs, the related SLOs (and metrics) were developed for the sole purposes of YOURCloud. The lack of standards in the area of secSLA, indirectly results on cumbersome tailoring efforts for CSPs willing to be accredited by YOURCloud.

The YOURcloud Service Broker allows organizational users to login to a self-service portal to provision servers and on-premise and off-premise services, which are owned and managed by the requestor. Based on the sensitivity of the data, the user is presented a list of (accredited) CSPs able to provide the requested security level in the form of a Cloud secSLA (equivalent to Steps 1 – 4 in Figure 2). As shown in Figure 4, once the user selects the CSP that makes the most sense to them based on their cost and security requirements (elicited after a risk assessment process), Cloud services are automatically provisioned within YOURCloud's secure enterprise "enclaves" (i.e., security domains) with specific secSLAs. As mentioned before, these secSLAs fulfill a minimum security baseline (as defined by the accreditation process), but can over-provision it in order to grant the user's requirements.

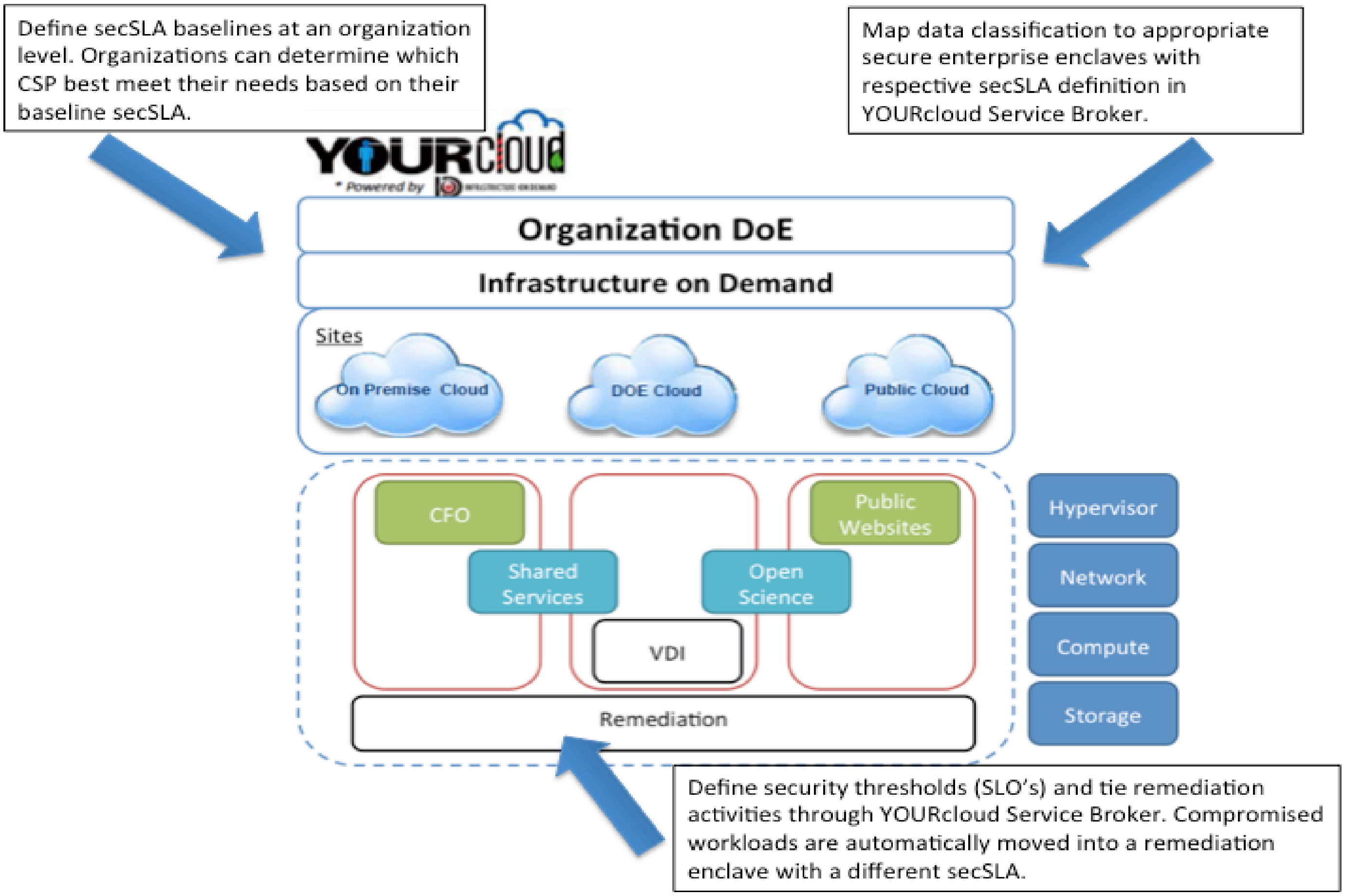
Systems within this secure MCS are subject to continuous monitoring by both the Cloud customer and the CSP based on their predefined roles and responsibilities, and agreed secSLAs. If a system is found by continuous monitoring to be compromised or vulnerable, it is moved by the Cloud broker to a *remediation enclave* off the production network (with a different secSLA) for the problem to be rectified before the system is moved back into its source enclave. This process is compliant with Steps 5 – 6 in Figure 2.

In YOURcloud, the use of Cloud secSLAs facilitates the automation of tasks within the security life cycle (in particular monitoring and remediation). However, due to the lack of established standards related to Cloud secSLAs (in particular metrics), security thresholds (SLOs) are predefined by each organization's continuous monitoring team and instrumented by the YOURcloud Service Broker.

The adoption of standards like ISO/IEC 19086 (cf., Section III) would result in reduced security management overhead (commonly accepted and metrics), increased usability (standardized vocabularies), and higher levels of automation on the accreditation and monitoring processes (through machine readable secSLAs) within YOURCloud.

V. Conclusions

The benefits related to the specification of standardized security elements in Cloud SLA are clear, in particular, for (prospective) SMEs planning their migration to the Cloud and also for existing customer/CSPs looking for higher levels of automation and usability (e.g., YOURcloud). Beyond the use of security control frameworks and as confirmed by the CSA's secSLA survey (cf., Section III.A), the usage of secSLA seems to be the missing piece on the Cloud Customer's security assurance and transparency puzzle. For these reasons, standardized Cloud secSLAs should become part of the more general SLAs/Master Service Agreements signed between the CSP and its customers.


Define secSLA baselines at an organization level. Organizations can determine which CSP best meet their needs based on their baseline secSLA.

Map data classification to appropriate secure enterprise enclaves with respective secSLA definition in YOURcloud Service Broker.

Define security thresholds (SLO's) and tie remediation activities through YOURcloud Service Broker. Compromised workloads are automatically moved into a remediation enclave with a different secSLA.

Figure 4. DOE YOURcloud: Leveraging SecSLA's and standards

Despite being work in progress, the standards discussed on this paper are also establishing the basis to leverage the full potential of Cloud secSLAs. In particular we refer to ISO/IEC 19086 series of standards, which are developing the vocabulary (Part 1), metrics (Part 2 and Part 4) and core requirements (Part 3) associated to Cloud secSLAs.

However, the analysis presented in this paper acknowledges that prior to any meaningful standardization the Cloud community should invest efforts in the empirical validation of the security SLOs and metrics being discussed in standardization bodies. In particular we refer to evaluate their feasibility in real-world scenarios, and assess their usage for advanced functionalities (e.g., machine-readable representations and automated negotiation). An entire research agenda should be developed by Cloud stakeholders to guarantee the creation of standards and best practices reflecting Cloud secSLA elements that are feasible to deploy.

Alongside development of the presented standards, there is active development by industry, academia and policy makers on three major topics related to Cloud secSLAs.

Firstly, standardization bodies and policy makers are devoting efforts to analyze the benefits (economic, technical, usability) of secSLAs with respect to "traditional" security certifications. The recent C-SIG SLA report [10] is one of the first outcomes related to this topic.

Second, both the academic community[10] and research projects such as EU funded SPECS are targeting the development of user-centric tools (e.g., decision-making dashboards) based on emerging Cloud SLA standards.

Finally, researchers are taking the first steps to use Cloud secSLAs as mechanisms to model end-to-end security levels in MCS. This is a novel approach were more empirical validation and qualitative evaluations are needed, despite the fact that NIST[11] and the ETSI CSC report [13] already highlighted security composition as one of the main challenges in this field.

References

[1] R. Sandhu, "Good-enough security: toward a pragmatic business-driven discipline." In IEEE Internet Computing. Vol. 7, No. 1, pp. 66-68. 2003.

[2] "Information Technology, Security Techniques, Code of Practice for Information Security Management," ISO/IEC 27002, 2014.

[10] J. Luna, R. Langenberg and N. Suri, "Benchmarking Cloud Security Level Agreements Using Quantitative Policy Trees," in Proc. of ACM Cloud Computing Security Workshop. 2012.

[11] "Directions in Security Metrics Research." NIST IR-7564, NIST, 2010.

[3] "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP-800-53 rev. 4, 2013.

[4] "Information technology -- Security techniques –Guidelines on information security controls for the use of Cloud computing services based on ISO/IEC 27002," ISO/IEC CD 27017, 2014.

[5] "Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework and Terminology." ISO/IEC WD 19086, 2014.

[6] "Risk Management Guide for Information Technology Systems," NIST SP 800–30, 2002.

[7] "Cloud-adapted Risk Management Framework", Draft NIST SP 800-173, 2014.

[8] "Cloud Computing: Cloud Service Metrics Description," NIST Public RATAX WG, WG draft document. 2014.

[9] "Security and Privacy Controls for Cloud-based Federal Information Systems," Draft NIST SP 800-174, 2014.

[10] "Cloud Service Level Agreement Standardization Guidelines," European Commission - Cloud Select Industry Group (C-SIG), Brussels, 2014.

[11] M. Singhal, S. Chandrasekhar, G. Ahn, E. Bertino, R. Krishnan, R. Sandhu and G. Tingjian, "Collaboration in Multi-Cloud Systems: Framework and Security Issues", IEEE Computer, Vol 46, No 2, pp. 76-84. 2013.

[12] "Cloud service provisions: Draft suggestions for common terms of service and SLAs for Cloud service contracts," European Commission - DG Communications Networks, Content & Technology. 2014.

[13] "ETSI Cloud Standards Coordination Final Report," European Telecommunications Standards Institute, November 2013.

[14] "NIST Cloud Computing Security Reference Architecture," NIST SP 500-299 (draft), 2013.

[15] "Guide for Applying the Risk Management Framework to Federal Information Systems," NIST SP 800-37, 2010.

Jesus Luna is the Research Director of the Cloud Security Alliance (Europe). Since 2003, Jesus is also affiliated with the Dept of CS at TU Darmstadt, Germany.

Neeraj Suri received his Ph.D. from the University of Massachusetts at Amherst. He holds the TUD Chair Professorship at TU Darmstadt, Germany.

Michaela Iorga serves as the senior security technical lead for the NIST Cloud Computing where she joined in 2008.

Anil Karmel is founder and CEO of C2 Labs Inc. Karmel was Deputy Chief Technology Officer for the National Nuclear Security Administration (NNSA).