Using a Capability Oriented Methodology to Build Your Cloud Ecosystem

Michaela Iorga
National Institute of Standards and Technology (NIST)

Karen Scarfone
Scarfone Cybersecurity

//Please send high resolution author photos to be included on the first page of the department.//

The potential benefits of cloud computing span from enabling innovation and establishing a backbone for rapid deployment of applications to improving the availability, security, reliability, scalability, and flexibility of operations. However, while these benefits entice organizations to favor cloud computing for their IT modernization efforts, many organizations are still struggling with identifying the right path forward for making cloud the first option for their information systems.

In our previous "Managing Risk in a Cloud Ecosystem" article [1], we highlighted that the key to successful implementation of a cloud-based information system is a level of transparency into the cloud provider's service. The article also discussed managing the security risks related to the operation and use of cloud-based information systems and pointed out that organizations need to quantify their residual risk and ensure it is at an acceptable level to limit the potential negative impact of compromises, operational disruptions, etc. Furthermore, we described in the article the cloud Provider and Consumer's risk management processes, focusing on the best practice steps a cloud Consumer should follow and the tasks associated with each step.

One of the tasks listed in the previous article is the identification and selection of functional capabilities deemed necessary for the cloud ecosystem that supports the cloud-based information system. Having a comprehensive, accurate, and prioritized list of these capabilities is strongly recommended before researching and evaluating cloud offerings. In the current article, we present a cloud capability oriented methodology for architecting the desired cloud ecosystem. The methodology was first introduced in NIST Special Publication (SP) 500-299, NIST Cloud Computing Security Reference Architecture [2]. This methodology complements the NIST Risk Management Framework discussed in the "Managing Risk in a Cloud Ecosystem" article by providing the capability oriented methodology for completing first task of the step two of the framework. The reader is encouraged to review the above mentioned article.

Cloud Computing Security Reference Architecture (SRA)

Cloud computing changes the emphasis from procuring, maintaining, and operating the necessary IT hardware and related infrastructure to meeting the agency's mission and taking advantage of higher-quality, added-value capabilities and faster services at lower cost to users. However, a cloud computing environment does not inherently provide the same level of security and compliance with US government (USG) mandates as was achieved in the traditional IT model. The ability of an organization acting as a cloud Consumer to comply with business, regulatory, operational, or security requirements in a cloud environment is a direct result of the cloud service and deployment models adopted by the organization, the cloud architecture, and the deployment and management of the resources in the cloud environment.

NIST SP 500-299, *NIST Cloud Computing Security Reference Architecture* (for the sake of brevity, SRA) provides a comprehensive formal model to serve as a security overlay to the architecture described in NIST SP 500-292, *NIST Cloud Computing Reference Architecture* [3], and also describes a methodology for using a comprehensive set of functional capabilities and their associated security components to orchestrate a secure cloud ecosystem. The SRA introduces the concept of a *security component* defined as the set of security controls, policy and procedures that are necessary to be implemented and/or enforced to secure a functional capability. In this way each functional capability has an associated security component.

The orchestration of a cloud ecosystem requires a risk-based approach that follows the Risk Management Framework (RMF) described in NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework*

to Federal Information Systems: A Security Life Cycle Approach [4]. Since multiple cloud Actors can participate in the orchestration of a cloud ecosystem, the Actors may incur different levels of risks depending on the roles they play in the process and the levels of control they have over the layers of the functional stack. Figure 1 depicts the SRA approach, showing on the left side of the graphic how the SRA's formal model was layered over the NIST Cloud Reference Architecture, while the right side of the graphic shows the Cloud Security Alliance's Trusted Cloud Initiative Reference Architecture (TCI RA) [5], later renamed Enterprise Architecture (CSA-EA) [6]. The CSA-EA identifies a comprehensive set of functional capabilities and processes grouped in containers and domains. The graphic indicates that the capabilities were extracted and used in the SRA as the foundation for the methodology of constructing a secure cloud ecosystem that meets the functionality and security needs of the cloud-based information system.

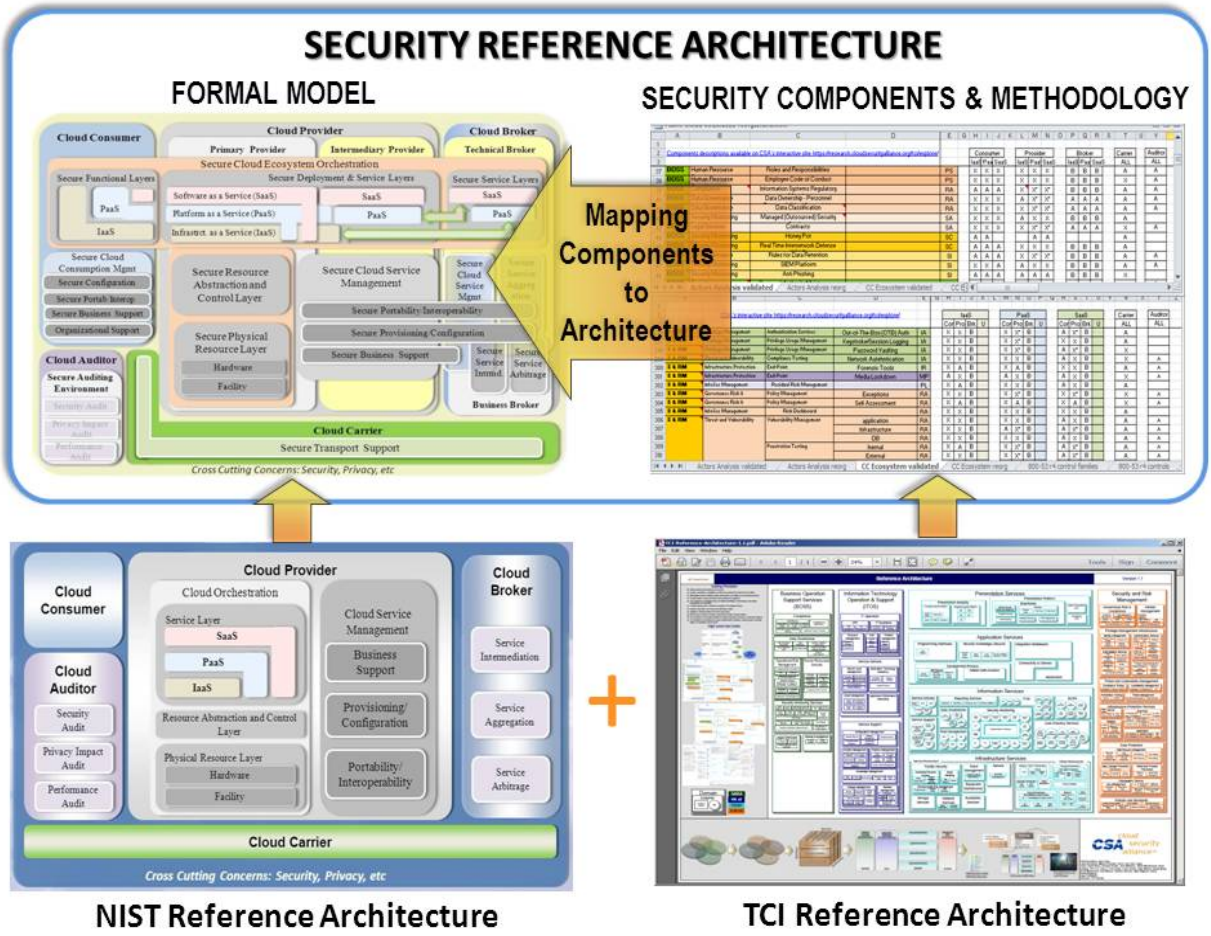

Figure 1: Basis of the NIST Cloud Computing Security Reference Architecture

A Capability Oriented Methodology for Orchestrating a Cloud Ecosystem

The capability oriented methodology for orchestrating a cloud ecosystem aims to demystify the process of describing, identifying, categorizing, analyzing, and selecting cloud-based services for cloud Consumers seeking to adopt such services that address their requirement(s) in the most effective way, and that support their business and mission-critical processes and services in the most secure and efficient manner. This methodology provides a consistent, repeatable process that starts with the analysis of a comprehensive set of functional capabilities. These capabilities, which are leveraged from the CSA-EA, are thought of in NIST SP 500-299 as possible building blocks of a cloud ecosystem.

The SRA introduced in NIST SP 500-299 is not a comprehensive guide to security requirements for all possible instances of cloud type, data, and service model. Rather, the publication provides core concepts, a step by step approach, and supporting information for the decision-making processes for the cloud Actors involved in orchestrating the ecosystem. A cloud Actor can analyze the set of functional capabilities and select the desired ones. For a cloud ecosystem to be secure, each selected functional capability needs to be secure. Accordingly, for each cloud instance[1] and each functional capability and associated security component, the cloud Actors' responsibility to implement and manage the capability was assessed and recorded. The information was recorded using the following codes:

- "X" to indicate that the security component should be implemented by the Actor to secure the Consumer's applications and data.
- "A" to indicate that the security component should be implemented internally, independent of the Consumer's data, for administrative or best practice reasons.
- "B," specific to Business Brokers only, to indicate a security component that is implemented to secure the cloud computing business-oriented service. The marking also emphasizes that the Business Broker only provides business and relationship services, and does not have any contact with the Consumer's data.
- A blank cell, to indicate that the security component cannot be implemented by the particular Actor or is not necessary for securing the cloud Ecosystem.

The markings provide cloud Consumers with a reference they can use to identify the functional capabilities and associated security components that are applicable for a particular cloud service model. The markings also indicate which cloud Actor(s) – Consumer, Provider, or Broker, in most cases – is responsible for a particular security component based on the use case or type of cloud service offered.[2] As indicated by the data sets, there are areas in which the responsibility for a particular security component may reside with multiple Actors. It is important to emphasize that cloud Consumers need to clearly distinguish between the responsibility for identifying and setting security component requirements and for implementing them. As owner of the data, the cloud Consumer is accountable for ensuring that an effective security control environment is in place.

The data collected for a public cloud is aggregated in NIST SP 500-299 for each cloud Actor in two ways:

- An Actor-centric way for each service model, to allow for a better understanding of each cloud Actor's roles and responsibilities for implementing the selected functional capabilities and associated security components. This also indicates how these roles and responsibilities shift among cloud Actors with changes in the service model. The top half of Figure 2 shows an Actor-centric sample. For each cloud Actor, the data collected for each security component and each service model is gathered in one matrix in adjacent columns to highlight the level of control a particular Actor has over the implementation of each security component. It is important to observe how this level increases or diminishes depending upon the service model. This information can assist cloud Consumers when they need to decide which service model best fits their needs in terms of level of control and/or management of particular functional capabilities.
- A service-centric way to facilitate data validation using criteria described in the document as the "Security Conservation Principle". The bottom half of Figure 2 shows a service-centric sample. For each type of service, the data collected for each security component and each cloud Actor is gathered in one matrix in adjacent columns to highlight the shared responsibilities among cloud Actors involved in constructing and securing a cloud Ecosystem of a particular service type.

Readers are encouraged to use the data made available in NIST SP 500-299 to more closely examine the Actor-centric and service-centric aggregations.

[1] A cloud instance is a combination of one of the four cloud deployment models (Public, Private, Hybrid, Community) and cloud service models (IaaS, PaaS, SaaS), as defined in NIST SP 800-145 [7].

[2] Many of the security components are common and should be considered by all cloud Actors (organizations) for implementation in their internal operations as well as in cloud-based service offering operations.

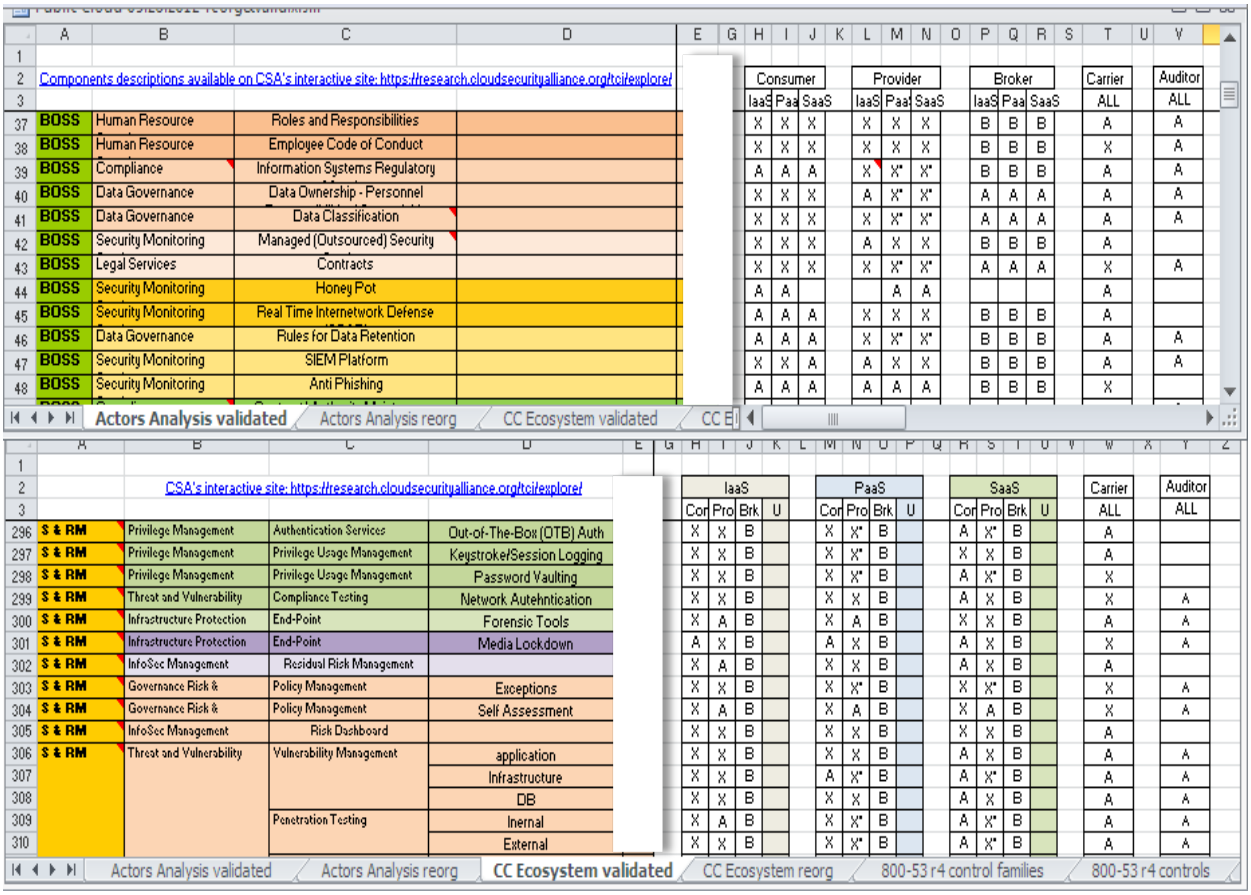

Figure 2: Data aggregation samples for the capability oriented methodology

It is important to note that based on NIST SP 500-292, *NIST Cloud Computing Reference Architecture* definitions of the cloud Carrier, the data collected for this Actor and its security responsibilities do not vary with the service model. This is due to the Carrier's unique role of securing the data in transit between the Consumer and the cloud. All other transport roles and responsibilities within the cloud ecosystem are attributed to the Provider. The data collected for and responsibilities attributed to the cloud Auditor also do not change with the cloud service model, since NIST SP 500-299 only addresses the set of security components necessary to secure the Actor's auditing environment.

Security Index System (SIS)

To build more flexibility into the analysis of the functional capabilities and to facilitate selecting the capabilities deemed necessary for a cloud-based information system, NIST SP 500-299 introduced a *Security Index System* (SIS). Table 1 provides the definitions for each index based upon the adverse effects caused by the loss of confidentiality, integrity, and availability (C/I/A). The definitions leverage those provided by the Committee on National Security Systems (CNSS) in CNSS Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems* [8]. Each index of the system has an associated value that can be interpreted as a priority weight when applied to a functional capability and the associated security component.

Additionally, an Aggregated Security Index (ASI) can be obtained for each functional capability and associated security component by summing the individual Security Indexes of the C/I/A security triad. The ASI can be used to prioritize the implementation of the functional capabilities. When necessary, heat maps of each of the C/I/A triad's security indexes can be used to prioritize the functional capabilities for a particular cloud-based information system.

To obtain an Actor-centric perspective or conduct a more granular evaluation of the security components' implementation priority, each Actor involved in the orchestration of the cloud Ecosystem can apply a logical-conjunction operation (logical "AND") between the Security Index of each C/I/A triad member and a Boolean applicability-value of 0 or 1 (0 for an empty cell or 1 for an X, B, or A cell table, for the service model adopted.

Table 1: Security Index System (SIS)

Security Index Symbol	Security Index Value	Security Index Applicability The Security Index Symbol should be applied to a security component if the loss of a Confidentiality, Integrity, or Availability property associated with the component is expected to cause what adverse effects on the cloud Ecosystem's security posture?
SI0	0	None.
SI1	1	Limited. The loss of a C/I/A property might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
SI2	2	Serious. The loss of a C/I/A property might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational, critical infrastructure, or national security assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals exceeding mission expectations.
SI3	3	Severe. The loss of a C/I/A property might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational, critical infrastructure, or national security assets; (iii) result in major financial loss; or (iv) result in severe harm to individuals exceeding mission expectations
SI4	4	Critical. The loss of a C/I/A property might: (i) generate vulnerabilities in system architecture/design or sabotage or subversion of a system's security functions or critical Security Components, as defined in NIST SP 800-53; (ii) cause a catastrophic loss of mission capability to such an extent and duration that the organization is not able to recover one or more of its system security functions; (iii) result in irrecoverable failure to organizational, critical infrastructure, or jeopardized national security assets; (iv) result in total financial loss; or (v) result in catastrophic harm to individuals exceeding mission expectations.

Conclusion

As organizations increasingly shift their information systems to the cloud, they often struggle to identify and select the functional capabilities that are needed for their cloud ecosystem. Developing a list of all the necessary capabilities, with each capability clearly defined and prioritized to support decision making, is more challenging than it sounds. Organizations also often fail to realize that they must develop a list for each cloud-based information system, because each system has a unique risk profile and thus a unique prioritized list.

To support organizations in functional capability identification, definition, selection, and prioritization, NIST has created SP 500-299, *NIST Cloud Computing Security Reference Architecture*. The Security Reference Architecture, better known as SRA, defines a capability oriented methodology for orchestrating a secure cloud ecosystem through use of functional capabilities. The methodology recognizes that risk may vary for each Actor in a cloud ecosystem, so it takes a risk-based approach that draws from NIST's Risk Management Framework (RMF) and the Cloud

Security Alliance's Enterprise Architecture (CSA-EA). The result of applying the methodology is an aggregated data set that indicate which cloud Actor is primarily responsible for implementing each necessary security component. NIST SP 500-299 also defines a Security Index System (SIS) that is intended for use in prioritizing the implementation of the security components.

When a cloud Actor, especially a cloud Consumer, applies the SRA, that Actor can more easily make well-informed decisions regarding its cloud Ecosystem architectures. The methodology drives the Actor to take into account both the prioritized set of functional capabilities and associated security components resulting from using the SIS, as well as the aggregated data from NIST SP 500-299 that indicates cloud Actors' responsibilities for implementing and integrating the components for each service model.

References

[1] M. Iorga and A. Karmel, "Managing Risk in a Cloud Ecosystem", *IEEE Cloud Computing*, Volume 2, Issue 6, November/December 2015; http://online.qmags.com/CLC1115?sessionID=8106DADDBF00F148FBCD8E4B6&cid=3280150&eid=19702#pg1&mode2.

[2] National Institute of Standards and Technology (NIST), *NIST Cloud Computing Security Reference Architecture* (draft), Special Publication 500-299, 2013; http://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf.

[3] F. Liu et al., *NIST Cloud Computing Reference Architecture,* NIST Special Publication 500-292, 2011; www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

[4] National Institute of Standards and Technology (NIST), Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 2010; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

[5] Cloud Security Alliance, "Trusted Cloud Initiative Reference Architecture Version 1.1", 2011; https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf.

[6] Cloud Security Alliance, "Cloud Security Alliance Enterprise Architecture"; https://research.cloudsecurityalliance.org/tci/

[7] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, 2011; http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[8] Committee on National Security Systems (CNSS), *Security Categorization and Control Selection for National Security Systems,* CNSS Instruction (CNSSI) No. 1253, 2014; https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

Michaela Iorga is Senior Security Technical Lead for Cloud Computing at the National Institute of Standards and Technology. Her current research interests include cloud computing security, forensics and privacy, information assurance, and federated identity and credential management issues in cyberspace. Iorga has a PhD in Engineering from Duke University. Contact her at michaela.iorga@nist.gov.

Karen Scarfone is the Principal Consultant for Scarfone Cybersecurity. Formerly a Senior Computer Scientist at the National Institute of Standards and Technology, she specializes in developing publications that address a wide variety of security topics. She has master's degrees in both computer science and technical writing. Karen can be *reached at karen@scarfonecybersecurity.com.*

Abstract: Organizations often struggle to capture the necessary functional capabilities for each cloud-based solution adopted for their information systems. Identifying, defining, selecting, and prioritizing these functional capabilities and the security components that implement and enforce them is surprisingly challenging. This article explains recent developments by the National Institute of Standards and Technology (NIST) in addressing these challenges. The article focuses on the capability oriented methodology for orchestrating a secure cloud ecosystem proposed as part of the NIST Cloud Computing Security Reference Architecture. The methodology recognizes that risk may vary for cloud Actors within a single ecosystem, so it takes a risk-based approach to functional capabilities. The result is an assessment of which cloud Actor is responsible for implementing each security component and how implementation should be prioritized. A cloud Actor, especially a cloud Consumer, that follows the methodology can more easily make well-informed decisions regarding their cloud ecosystems.

Keywords: cloud, cloud computing, cloud architecture, standards, security, National Institute of Standards and Technology (NIST), risk management, risk management framework, risk assessment *//Please feel free to add to or revise.//*