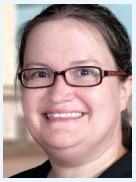
Using a Capability-Oriented Methodology to Build Your Cloud Ecosystem

Michaela Iorga
National Institute of Standards and Technology

Karen Scarfone
Scarfone Cybersecurity



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, although these benefits entice organizations to favor cloud computing for their information technology (IT) modernization efforts, many organizations are still struggling with identifying the right path forward for making cloud the first option for their information systems.

A previous article, "Managing Risk in a Cloud Ecosystem," highlighted that the key to successful implementation of a cloud-based information system is a level of transparency into the cloud provider's service.[1] 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 that it's at an acceptable level to limit the potential negative impact of compromises, operational disruptions, and so on. Furthermore, in that article we described the cloud provider's and cloud 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 these tasks is the identification and selection of functional capabilities deemed necessary for the cloud ecosystem that supports the cloud-based information system.[1] Having a comprehensive, accurate, and prioritized list of these capabilities is strongly recommended before researching and evaluating cloud offerings. Here, we present a cloud capability-oriented methodology for architecting the desired cloud ecosystem. The methodology was first introduced in the National Institute of Standards and Technology (NIST) Special Publication (SP) 500-299, *NIST Cloud Computing Security Reference Architecture* (SRA).[2] This methodology complements the NIST Risk Management Framework[1] by providing the capability-oriented methodology for completing the first task of step two of the framework.

Cloud Computing Security Reference Architecture

Cloud computing changes the emphasis from procuring, maintaining, and operating the necessary IT

2325-6095/16/$33.00 © 2016 IEEE

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 doesn't inherently provide the same level of security and compliance with US government 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 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, policies, and procedures that must 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, they might 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. The left side of the graphic shows how the SRA's formal model was layered over the NIST Cloud Reference Architecture, whereas the right side shows the Cloud Security Alliance's Trusted Cloud Initiative Reference Architecture (https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf), later renamed Enterprise Architecture (CSA-EA; https://research.cloudsecurityalliance.org/tci). 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.

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 requirements most effectively and 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 considered 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 of 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—that is, a combination of one of the four cloud deployment models (public, private, hybrid, or community) and cloud service models (infrastructure as a service, platform as a service, and so on)[5]—and each functional capability and associated security component, the cloud actors' responsibility to implement and manage the capability is assessed and recorded. The information is recorded using the following codes:

- "X" indicates that the actor should implement the security component to secure the consumer's applications and data.

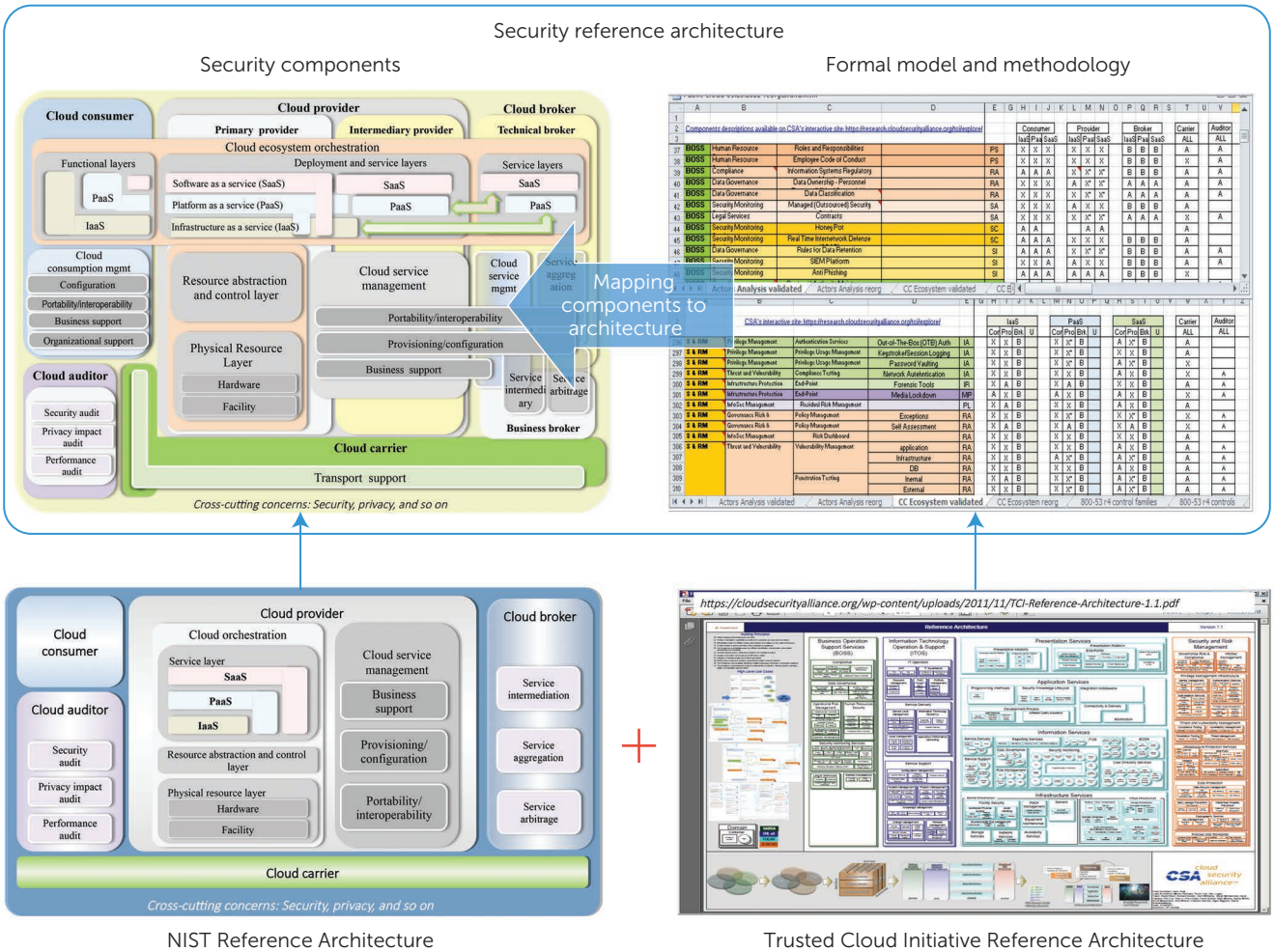
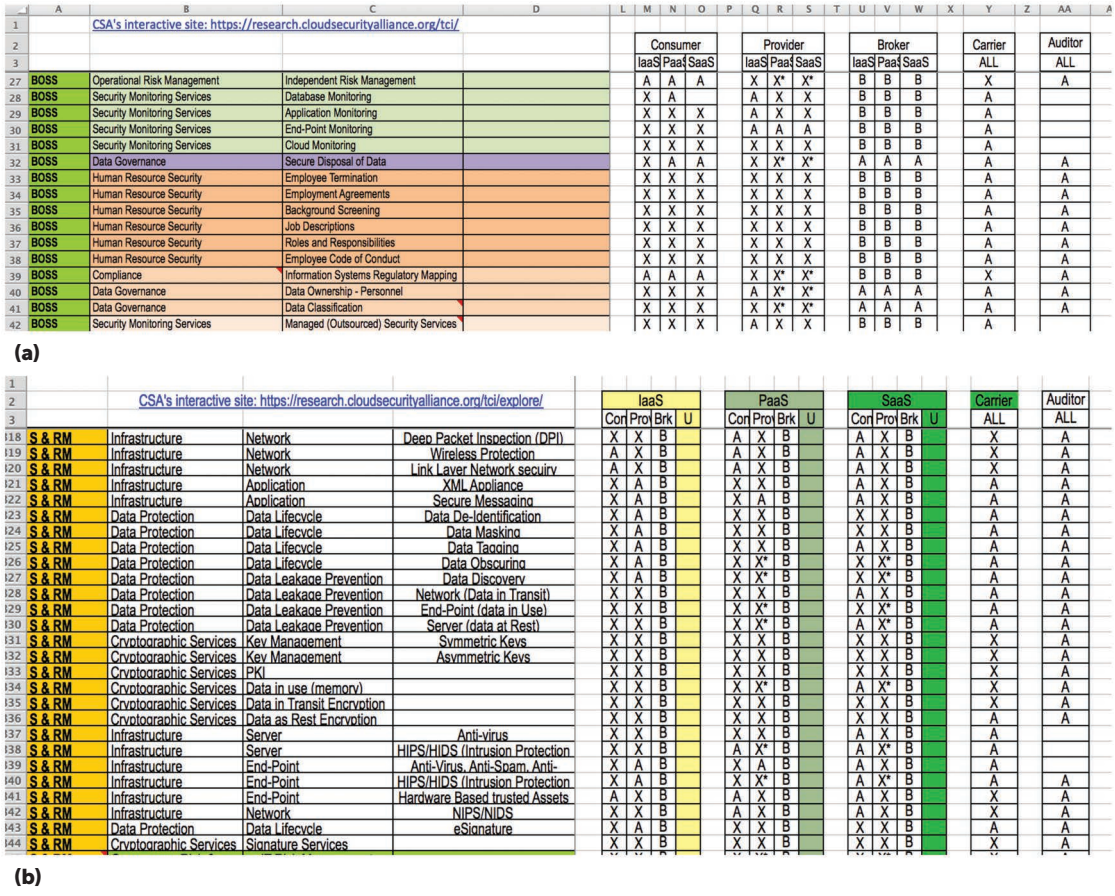


FIGURE 1. Basis of the NIST Cloud Computing Security Reference Architecture.

- "A" indicates that the security component should be implemented internally, independent of the consumer's data, for administrative or best practice reasons.
- "B," which relates to business brokers only, indicates a security component that's implemented to secure the cloud computing business-oriented service. The code also emphasizes that the business broker only provides business and relationship services, and has no contact with the consumer's data.
- A blank cell indicates that the security component can't be implemented by the particular actor or isn't necessary for securing the cloud ecosystem.

The codes 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. They also indicate which cloud actor—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. (Many of the security components are common and should be considered by all cloud actors, or organizations, for implementation in their internal operations as well as in cloud-based service offering operations.) As the datasets indicate, in some areas the responsibility for a particular security component might reside with multiple actors. It's important to emphasize



				Consumer			Provider			Broker			Carrier	Auditor
				IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	ALL	ALL
27	BOSS	Operational Risk Management	Independent Risk Management	A	A	A	X	X*	X*	B	B	B	X	A
28	BOSS	Security Monitoring Services	Database Monitoring	X	A		A	X	X	B	B	B	A	
29	BOSS	Security Monitoring Services	Application Monitoring	X	X	X	A	X	X	B	B	B	A	
30	BOSS	Security Monitoring Services	End-Point Monitoring	X	X	X	A	A	A	B	B	B	A	
31	BOSS	Security Monitoring Services	Cloud Monitoring	X	X	X	X	X	X	B	B	B	A	
32	BOSS	Data Governance	Secure Disposal of Data	X	A	A	X	X*	X*	A	A	A	A	A
33	BOSS	Human Resource Security	Employee Termination	X	X	X	X	X	X	B	B	B	A	A
34	BOSS	Human Resource Security	Employment Agreements	X	X	X	X	X	X	B	B	B	A	A
35	BOSS	Human Resource Security	Background Screening	X	X	X	X	X	X	B	B	B	A	A
36	BOSS	Human Resource Security	Job Descriptions	X	X	X	X	X	X	B	B	B	A	A
37	BOSS	Human Resource Security	Roles and Responsibilities	X	X	X	X	X	X	B	B	B	A	A
38	BOSS	Human Resource Security	Employee Code of Conduct	X	X	X	X	X	X	B	B	B	A	A
39	BOSS	Compliance	Information Systems Regulatory Mapping	A	A	A	X	X*	X*	B	B	B	X	A
40	BOSS	Data Governance	Data Ownership - Personnel	X	X	X	A	X*	X*	A	A	A	A	A
41	BOSS	Data Governance	Data Classification	X	X	X	X	X*	X*	A	A	A	A	A
42	BOSS	Security Monitoring Services	Managed (Outsourced) Security Services	X	X	X	A	X	X	B	B	B	A	

(a)

					IaaS				PaaS				SaaS				Carrier	Auditor
					Con	Pro	Brk	U	Con	Pro	Brk	U	Con	Pro	Brk	U	ALL	ALL
118	S & RM	Infrastructure	Network	Deep Packet Inspection (DPI)	X	X	B		A	X	B		A	X	B		X	A
119	S & RM	Infrastructure	Network	Wireless Protection	A	X	B		A	X	B		A	X	B		X	A
120	S & RM	Infrastructure	Network	Link Layer Network security	A	X	B		A	X	B		A	X	B		X	A
121	S & RM	Infrastructure	Application	XML Appliance	X	A	B		X	X	B		A	X	B		A	A
122	S & RM	Infrastructure	Application	Secure Messaging	X	A	B		X	A	B		A	X	B		A	A
123	S & RM	Data Protection	Data Lifecycle	Data De-Identification	X	A	B		X	X	B		X	X	B		A	A
124	S & RM	Data Protection	Data Lifecycle	Data Masking	X	A	B		X	X	B		X	X	B		A	A
125	S & RM	Data Protection	Data Lifecycle	Data Tagging	X	A	B		X	X	B		A	X	B		A	A
126	S & RM	Data Protection	Data Lifecycle	Data Obscuring	X	A	B		X	X*	B		X	X*	B		A	A
127	S & RM	Data Protection	Data Leakage Prevention	Data Discovery	X	A	B		X	X*	B		X	X*	B		A	A
128	S & RM	Data Protection	Data Leakage Prevention	Network (Data in Transit)	X	X	B		X	X	B		A	X	B		A	A
129	S & RM	Data Protection	Data Leakage Prevention	End-Point (data in Use)	X	X	B		X	X*	B		X	X*	B		A	A
130	S & RM	Data Protection	Data Leakage Prevention	Server (data at Rest)	X	X	B		X	X*	B		A	X*	B		A	A
131	S & RM	Cryptographic Services	Key Management	Symmetric Keys	X	X	B		X	X	B		X	X	B		X	A
132	S & RM	Cryptographic Services	Key Management	Asymmetric Keys	X	X	B		X	X	B		X	X	B		X	A
133	S & RM	Cryptographic Services	PKI		X	X	B		X	X	B		X	X	B		X	A
134	S & RM	Cryptographic Services	Data in use (memory)		X	X	B		X	X*	B		A	X*	B		X	A
135	S & RM	Cryptographic Services	Data in Transit Encryption		X	X	B		X	X	B		X	X	B		X	A
136	S & RM	Cryptographic Services	Data as Rest Encryption		X	X	B		X	X	B		X	X	B		A	A
137	S & RM	Infrastructure	Server	Anti-virus	X	X	B		X	X	B		A	X	B		A	
138	S & RM	Infrastructure	Server	HIPS/HIDS (Intrusion Protection	X	X	B		A	X*	B		A	X*	B		A	
139	S & RM	Infrastructure	End-Point	Anti-Virus, Anti-Spam, Anti-	X	A	B		X	A	B		A	X	B		A	
140	S & RM	Infrastructure	End-Point	HIPS/HIDS (Intrusion Protection	X	A	B		X	X*	B		A	X*	B		A	A
141	S & RM	Infrastructure	End-Point	Hardware Based trusted Assets	A	X	B		A	X	B		A	X	B		X	A
142	S & RM	Infrastructure	Network	NIPS/NIDS	X	X	B		A	X	B		A	X	B		X	A
143	S & RM	Data Protection	Data Lifecycle	eSignature	X	A	B		X	X	B		X	X	B		A	A
144	S & RM	Cryptographic Services	Signature Services		X	X	B		X	X	B		X	X	B		X	A

(b)

FIGURE 2. Data aggregation samples for the capability-oriented methodology: (a) actor-centric sample and (b) service-centric sample.

that cloud consumers need to clearly distinguish between the responsibility for identifying and setting security component requirements and the responsibility for implementing them. As the data owner, the cloud consumer must ensure an effective security control environment.

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 (Figure 2a) aggregates the information for the IaaS, PaaS, and SaaS service models pertaining to each actor and each capability. This representation allows for a better understanding of cloud actor roles and responsibilities for implementing the selected functional capabilities and associated security components. It also indicates how these roles and responsibilities shift among cloud actors with changes in the service model. 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 each security component's implementation. It's 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 (Figure 2b) aggregates data for the cloud consumer, provider, and broker pertaining to each service model and each capability. This representation facilitates data validation using criteria described in the document as the "security conservation principle." For each service type, the data collected for each security component and each

Table 1. Security index system (SIS) definitions.

Security index symbol	Security index value	Security index applicability*
SI0	0	None
SI1	1	Limited. The loss of a C/I/A property might cause degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of those functions is noticeably reduced; result in minor damage to organizational, critical infrastructure, or national security assets; result in minor financial loss; or result in minor harm to individuals.
SI2	2	Serious. The loss of a C/I/A property might cause a significant degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of those functions is significantly reduced; result in significant damage to organizational, critical infrastructure, or national security assets; result in significant financial loss; or result in significant harm to individuals exceeding mission expectations.
SI3	3	Severe. The loss of a C/I/A property might cause a severe degradation in or loss of mission capability to an extent and duration that the organization can't perform one or more of its primary functions; result in major damage to organizational, critical infrastructure, or national security assets; result in major financial loss; or result in severe harm to individuals exceeding mission expectations.
SI4	4	Critical. The loss of a C/I/A property might generate vulnerabilities in system architecture/design or sabotage or subvert a system's security functions or critical security components, as defined in NIST SP 800-53[6]; cause a catastrophic loss of mission capability to such an extent and duration that the organization can't recover one or more of its system security functions; result in irrecoverable failure to organizational, critical infrastructure, or jeopardized national security assets; result in total financial loss; or result in catastrophic harm to individuals exceeding mission expectations.

*The security index symbol should be applied to a security component if the loss of a confidentiality, integrity, or availability property associated with the functional capability and its security component is expected to cause what adverse effects on the cloud ecosystem's security posture?

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.

We encourage you to use the data made available in NIST SP 500-299 to more closely examine the actor-centric and service-centric aggregations.

Based on NIST SP 500-292, definitions of the cloud carrier, the data collected for this actor, and its security responsibilities don't 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 don't 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

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 on the adverse effects of the loss of confidentiality, integrity, and availability (C/I/A). The definitions leverage those provided by the Committee on National Security Systems in CNSS Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*.[7] 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 indi-

vidual 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).

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 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.

Using the SRA, a cloud actor, especially a cloud consumer, can more easily make well-informed decisions about its cloud ecosystem architectures. The capability-oriented methodology guides the actor in developing the prioritized set of functional capabilities and drives the actor to consider both that set and the 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*, vol. 2, no. 6, 2015, pp. 51–57.
2. National Institute of Standards and Technology, *NIST Cloud Computing Security Reference Architecture* (draft), NIST Special Publication 500-299, 2013; www.nist.gov/itl/cloud/publications.cfm.
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, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Revision 1, 2010; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.
5. P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, 2011; http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
6. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, 2013; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
7. Committee on National Security Systems (CNSS), *Security Categorization and Control Selection for National Security Systems*, CNSS Instruction 1253, 2014; 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. Scarfone has master's degrees in both computer science and technical writing. Contact her at karen@scarfonecybersecurity.com.*