Managing Risk in a Cloud Ecosystem

DUE TO ECONOMIES OF SCALE, CUTTING-EDGE TECHNOLOGY ADVANCEMENTS, AND HIGHER CONCENTRATION OF EXPERTISE, CLOUD PROVIDERS HAVE THE POTENTIAL TO OFFER STATE-OF-THE-ART CLOUD ECOSYSTEMS THAT ARE RESILIENT, SELF-REGENERATING, AND SECURE—FAR MORE SECURE THAN THE ENVIRONMENTS OF CONSUMERS WHO MANAGE THEIR OWN SYSTEMS. This has the potential to greatly benefit many organizations. The key to successful implementation of a cloud-based information system is a level of transparency into the cloud provider's service. This level of transparency allows businesses to build the necessary trust and to properly weigh the benefits of adopting such solutions. In this assessment process, businesses need to consider the sensitivity of the stored information against the incurred security and privacy risks. For example, the benefits of a cloud-based solution would depend on the cloud model, type of cloud service considered, type of data involved, the system's criticality/impact level, cost savings, service type, and any associated regulatory requirements.

Cloud-based information systems are exposed to threats that can have adverse effects on organizational operations (such as missions, functions, image, or reputation), organizational assets, individuals, and other organizations. Malicious entities can exploit both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems.

Risk management activities can be grouped based upon the level at which they address the risk-related concerns:

- organization level (tier 1);
- mission and business process level (tier 2); and
- information system level (tier 3).

In this article, we focus only on the tier 3 security risks related to the operation and use of cloud-based information systems. To prevent and mitigate any risks, adverse actions, service disruptions, attacks, or compromises, organizations need to quantify their residual risk (that is, the portion of risk remaining after security measures have been applied[1]) below the threshold of the acceptable level of risk.

Security Risk and Cloud

Information systems risk management (tier 3) is guided by the risk decisions at tier 1 and tier 2. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from standardized catalogs of security and controls.[2–4]

Volume 1 of National Institute of Standards and Technology (NIST) Special Publication (SP) 500-293, *US Government Cloud Computing Roadmap*, highlights that boundaries in a cloud ecosystem are more complex and therefore renders traditional risk management mechanisms, such as perimeter-based defense mechanisms, less effective.[5] Moreover, in a cloud ecosystem, the complex relationships among cloud actors,[6]

Michaela Iorga
National Institute of Standards and Technology

Anil Karmel
C2 Labs

2325-6095/15/$31.00 © 2015 IEEE

the actors' individual missions, business processes, and their supporting information systems require an integrated, ecosystem-wide risk management framework (RMF) that addresses all cloud actors' needs. As with any information system, for a cloud-based information system, cloud actors are responsible for evaluating their acceptable risk, which depends on the threshold set by their risk tolerance to the cloud ecosystem-wide residual risk.

In general, organizations have maximum flexibility in how risk assessments are conducted. Because risk assessments facilitate decision making at all three tiers (organization level, mission/business process level, and information system level), they're key processes of effective risk management and in maintaining the residual risk below the threshold, and therefore the methods employed to assess the risks are of crucial importance. We recommend reading NIST SP 800-30, *Guide for Conducting Risk Assessment*, which provides quantitative, qualitative, or semiqualitative methods that use scores or levels, respectively.[7]

To effectively manage information security risk at the ecosystem level, the following high-level elements must be established:

- Assignment of risk management responsibilities to the cloud actors involved in the orchestration of the cloud ecosystem. Internally, cloud actors need to further assign responsibilities to their senior leaders, executives, and representatives.
- Establishment of a cloud ecosystem-wide tolerance for risk and communication of this risk tolerance through service-level agreements (SLA), including information on decision-making activities that impact the risk tolerance.
- Near real-time monitoring, recognition, and understanding, by each cloud actor, of the information security risks arising from the operation and/or use of the information system leveraging the cloud ecosystem.
- Accountability by the cloud actors and near real-time information sharing of the cloud actors' incidents, threats, risk management decisions, and solutions.

Risk is often expressed as a function of the *magnitude of harm* caused by the occurrence of a circumstance or event, multiplied by the *likelihood of its occurrence*. In information security, *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given *threat* is capable of exploiting a given *vulnerability*. Accordingly, security risk assessments focus on identifying where in the cloud ecosystem damaging events could take place.

The risk-based approach to managing information systems is a holistic activity that needs to be fully integrated into every aspect of the organization. An RMF provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. An RMF operates primarily at tier 3 in the risk management hierarchy, but it can also have interactions at tier 1 and tier 2.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, introduces a risk management process mandated for federal agencies but widely vetted by state and local governments and by private sector organizations as a best practice for traditional information systems.[8] As that document states, defining information system requirements is a critical part of any system development process and needs to begin in a system's initiation phase. Since the security requirements are a subset of the overall functional and nonfunctional requirements, security requirements need to be integrated into the system development life cycle (SDLC) simultaneously with the functional and nonfunctional requirements. Treating security as a patch or addition to the system and architecting and implementing solutions independent of the SDLC is a more difficult process that can incur higher costs with a lower potential to effectively mitigate risk.

We encourage you to review NIST SP 800-37, Revision 1, as well, which we use here as a reference framework for the current discussion of applying the RMF in a cloud ecosystem. For the sake of brevity, we won't review in this article the six steps and the tasks described in that document. It's important to note that even though the NIST document addresses complex information systems composed of multiple subsystems operated by different entities, it doesn't address cloud-based information systems, or any other kind of systems that leverage utility-based resources, and hence the need for the current discussion.

When orchestrating a cloud ecosystem for a cloud-based information system, cloud consumers, as owners of the data associated with the system, remain responsible for securing the system and the data commensurate with the data sensitivity. However, cloud consumers' level of control and direct management varies based on the cloud deployment model. NIST defined in SP 800-145, *The NIST Definition of Cloud Computing,* the cloud, cloud deployment models (public, private, hybrid, and community), and cloud service models (infrastructure as a service [IaaS], platform as a service [PaaS], and software as a service [SaaS]).[9] In an IaaS cloud, the cloud consumer manages the top part of the functional stack above the hypervisor, while the consumer-managed functional stack proportionally decreases for a PaaS cloud and is reduced to a minimum in a SaaS cloud ecosystem.

The RMF introduced in NIST SP 800-37, Revision 1 is applicable by a cloud actor to the layers of the functional stack that are under management. In a simplified cloud ecosystem model, which is orchestrated only by the cloud consumer and the cloud provider, the cloud provider applies the RMF to the lower part of the stack, which is built as part of the service offered. Cloud consumers will apply the RMF to the upper functional layers, the ones built and deployed on top of the cloud infrastructure offered as a service.

However, prior to acquiring a cloud service, a cloud consumer needs to analyze the risk associated with adopting a cloud-based solution for a particular information system, and plan for the risk-treatment and risk-control activities associated with the cloud-based operations of this system. To do so, a cloud consumer needs to gain the perspective of the entire cloud ecosystem that will serve the operations of their cloud-based information system. Cloud consumers must also apply the RMF in a customized way that allows them to

- perform a risk assessment,
- identify the best-fitting cloud architecture,
- select the most suitable cloud service,
- gain necessary visibility into the cloud offering, and
- define and negotiate necessary risk treatment and risk control mitigations before finalizing the SLA and proceeding with the security authorization.

Figure 1 depicts this RMF for the cloud ecosystem (RMF4CE) from the cloud consumer's perspective, showing it as a repeatable process that encompasses the entire cloud ecosystem.

In a cloud ecosystem, cloud consumers must establish the clear demarcation of information-system boundaries on all levels in a vendor-neutral manner. Furthermore, the cloud consumer must establish measures to ensure appropriate protection, regardless of vendor, ownership, or service level for the cloud-based information system.

Cloud Provider's Risk Management Process

A cloud provider's selection and implementation of its security and privacy controls consider their effectiveness, efficiency, and constraints based on the applicable laws, directives, policies, standards, or regulations with which the provider must comply. The cloud consumers' specific requirements and mandates are unknown and therefore are projected as a generic core set.

Cloud providers have significant flexibility in determining what constitutes a cloud service and therefore its associated boundary, but at the time the system is architected and implemented, they can only assume the nature of data their cloud consumers will generate. Therefore, the security and privacy controls selected and implemented by a cloud provider are sets that meet the needs of a large number of potential consumers. However, the centralized nature of the offered cloud service enables a cloud provider to engineer highly technical, specialized security solutions that can provide a higher security posture than that in traditional IT systems.

Applying standardized or well-vetted approaches to cloud service risk management is critical to the success of the entire cloud ecosystem and its supported information systems. Since the offered cloud service is directly managed and controlled by the cloud provider, applying the RMF to this system doesn't require additional tasks beyond those of a classical IT system; therefore, a risk management approach like the one discussed previously is a good example of a broadly accepted, well-vetted approach.

It's important to note that a cloud ecosystem's security posture is only as strong as the weakest subsystem or functional layer. Since a cloud provider's reputation and business continuity depend

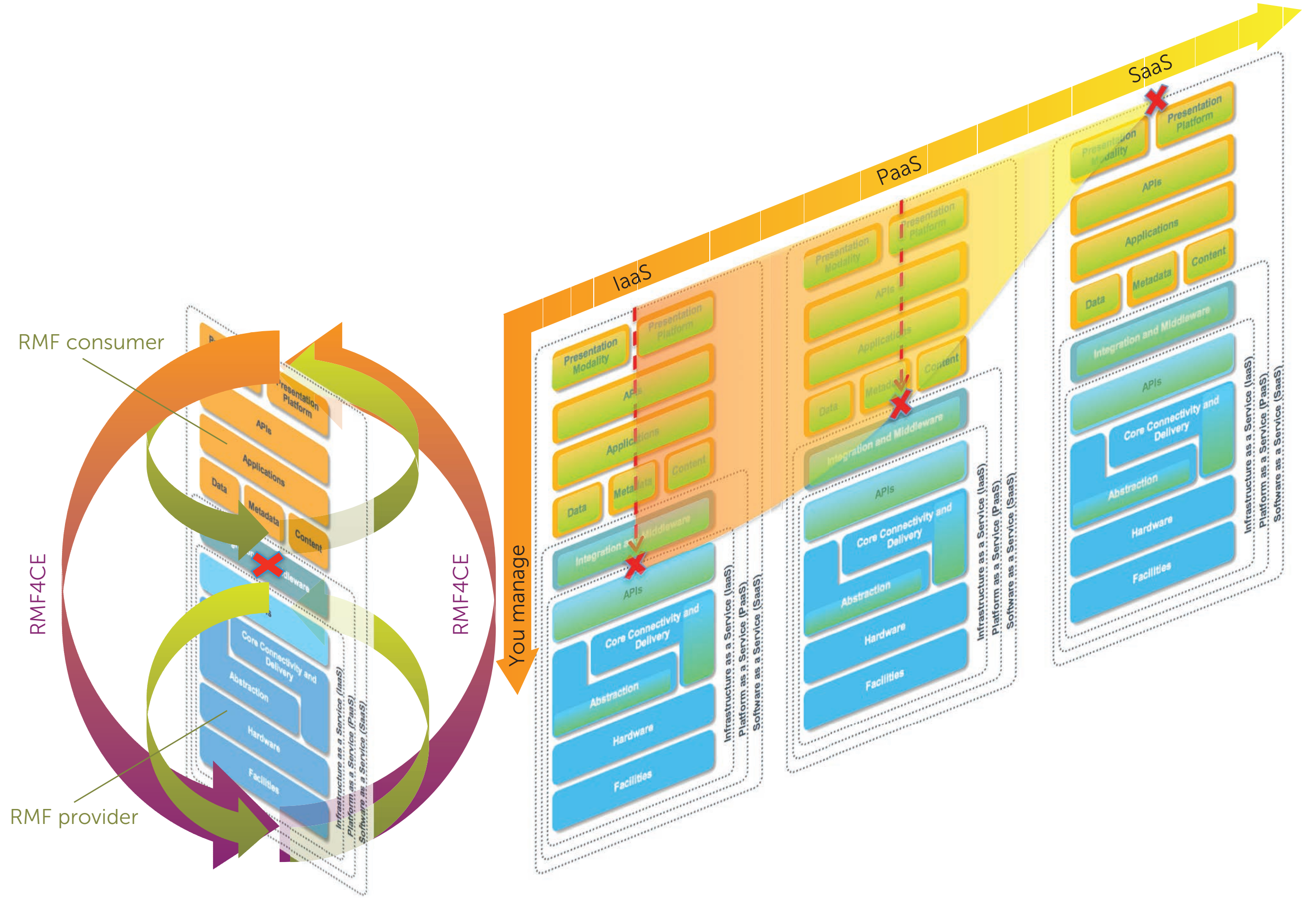

FIGURE 1. Applying a risk management framework (RMF) to a cloud ecosystem (RMF4CE). (Functional stack image courtesy of Cloud Security Alliance, 2009)

on the smooth operation and high performance of their consumers' solutions, when applying the RMF a cloud provider aims to compensate for possible weakness in their cloud consumers' solutions.

Cloud Consumer's Risk Management Process

For successful adoption of a cloud-based information system solution, the cloud consumer must be able to clearly understand the system's cloud-specific characteristics, the architectural components for each service type and deployment model, and the cloud actors' roles in establishing a secure cloud ecosystem. Furthermore, it is essential to cloud consumers' business and mission-critical processes that they have the ability to

- identify all cloud-specific, risk-adjusted security and privacy controls;
- request from the cloud providers and brokers (when applicable and via contractual means) service agreements and SLAs where the cloud providers are responsible for implementing security and privacy controls;
- assess the implementation of said security and privacy controls; and
- continuously monitor all identified security and privacy controls.

Since the cloud consumers directly manage and control the functional capabilities they implement, applying the RMF to these functional layers doesn't require more tasks or operations than necessary in a classical IT system; therefore, the risk management approach discussed earlier is a good example of a broadly accepted, well-vetted approach.

With cloud-based services, some subsystems or subsystem components fall outside the direct control of a cloud consumer's organization. Since a cloud-based solution doesn't inherently provide the same level of security and compliance as the traditional IT model, being able to perform a comprehensive risk assessment is key to building trust in the cloud-based system as the first step in authorizing its operation.

Cloud characteristics often present a cloud consumer with security risks that are different from those in traditional information technology solutions. To preserve the security level of their information system and data in a cloud-based solution, cloud consumers must be able to identify all cloud-specific, risk-adjusted security and privacy controls in advance of cloud service acquisition. They must also request from the cloud providers and brokers, through contractual means and SLAs, that all security and privacy components are identified and that their controls are fully and accurately implemented.

Understanding the relationships and interdependencies between the different cloud computing deployment models and service models is critical to understanding the security risks involved in cloud computing. The differences in methods and responsibilities for securing different combinations of service and deployment models present a significant challenge for cloud consumers. They need to perform a thorough risk assessment to accurately identify the security and privacy controls necessary to preserve their environment's security level as part of the risk treatment process, and to monitor the operations and data after migrating to the cloud in response to their risk control needs.

In general, a cloud consumer adopting a cloud-based solution needs to follow the same RMF steps discussed earlier in addition to the tasks listed in Table 1. The table aligns risk management activities with their corresponding steps from NIST SP 800-37, Revision 1, and provides additional tasks (in italics) that map to Figure 2.

The RMF applied to the cloud ecosystem from the consumer's perspective can be used to address the security risks associated with cloud-based information systems by incorporating the outcome into the terms and conditions of the contracts with external cloud providers and cloud brokers. Performance aspects of these terms and conditions are also incorporated into the SLA, which is an intrinsic part of the security authorization process and of service agreements between the cloud consumer, provider, and broker (when applicable). Contractual terms should include guarantees of the cloud consumer's timely access to or the provider's timely delivery of cloud audit logs, continuous monitoring logs, and any user access logs.

The approach covered by the steps in Table 1 enables organizations to systematically identify their common, hybrid, and system-specific security controls and other security requirements to procurement officials, cloud providers, carriers, and brokers.

BEFORE ADOPTING A CLOUD-BASED SOLUTION FOR AN INFORMATION SYSTEM, CLOUD CONSUMERS MUST DILIGENTLY IDENTIFY THEIR SECURITY REQUIREMENTS. In addition, they must assess each prospective service provider's security and privacy controls, negotiate SLAs and service agreements, and build trust with the cloud provider before authorizing the service. A thorough risk analysis coupled with the secure cloud ecosystem orchestration introduced here, along with adequate guidance on negotiating SLAs, are intended to assist cloud consumers in managing risk and making informed decisions when adopting cloud services.

References

1. *National Information Assurance (IA) Glossary*, Committee on National Security Systems Instruction No. 4009, Apr. 2010; www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf.
2. 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.
3. International Organization for Standardization, *Information Technology—Security Techniques—Information Security Management—Requirements*,

Table 1. Risk management framework (RMF) applied to a cloud ecosystem from a cloud consumer's perspective.

Risk management activities	NIST SP 800-37 RMF steps	Description
Risk assessment (analyze cloud environment to identify potential vulnerabilities and shortcomings)	1. Categorize	Categorize the information system and the information processed, stored, and transmitted by that system based on a system impact analysis. Identify operational, performance, security, and privacy requirements.
	2. Select (includes evaluate-select-negotiate)	*Identify and select functional capabilities for the entire information system.* Identify and select the associated baseline security controls based upon the system's impact level, and the privacy controls. Tailor and supplement the security controls by selecting enhancements and/or additional controls deemed necessary.
		Identify and select best-fitting cloud architecture for this information system.
		Evaluate/review cloud providers that meet consumer's criteria (architecture, functional capabilities, and controls).
		Select cloud provider(s) that best meet(s) the desired architecture and the security requirements (ideally should select the provider that provides as many controls as possible to minimize the number of controls that will have to be tailored). *In the process, identify the controls that will be implemented by the consumer, the controls implemented by the provider as part of the offering, and the controls that need to be tailored (via compensating controls and/or parameter selection).*
		Negotiate SLA, metrics, and sign service agreement as part of the procurement process. *Document all the controls in the security plan. Review and approve the security plan.*
Risk treatment (design mitigation policies and plans)	3. Implement	Implement security and privacy controls for which the cloud consumer is responsible.
	4. Assess	*Assess the cloud provider's implementation of the tailored security and privacy controls.*
		Assess the implementation of the security and privacy controls, and identify any inheritance and dependency relationships between the provider's controls and consumer's controls.
	5. Authorize	Authorize the cloud-based information system to operate.
Risk control (risk monitoring—surveying, reviewing events, identifying policy adjustments)	6. Monitor	Continuous/near real-time monitoring of operations and effectiveness of the security and privacy controls under consumer's management.
		Continuous/near real-time monitoring of cloud provider's operations related to the cloud-based information system and assessment of the systems' security posture.
		Reassess and reauthorize (periodic or ongoing) the cloud provider's service.

ISO/IEC 27001, 2013; www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

4. International Organization for Standardization, *Information Technology—Security Techniques—Code of Practice for Information Security Controls*, ISO/IEC 27002, 2013; www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533.

5. L. Badger et al., *US Government Cloud Computing Technology Roadmap*, NIST Special Publication 500-293, volumes 1 and 2, 2014; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf.

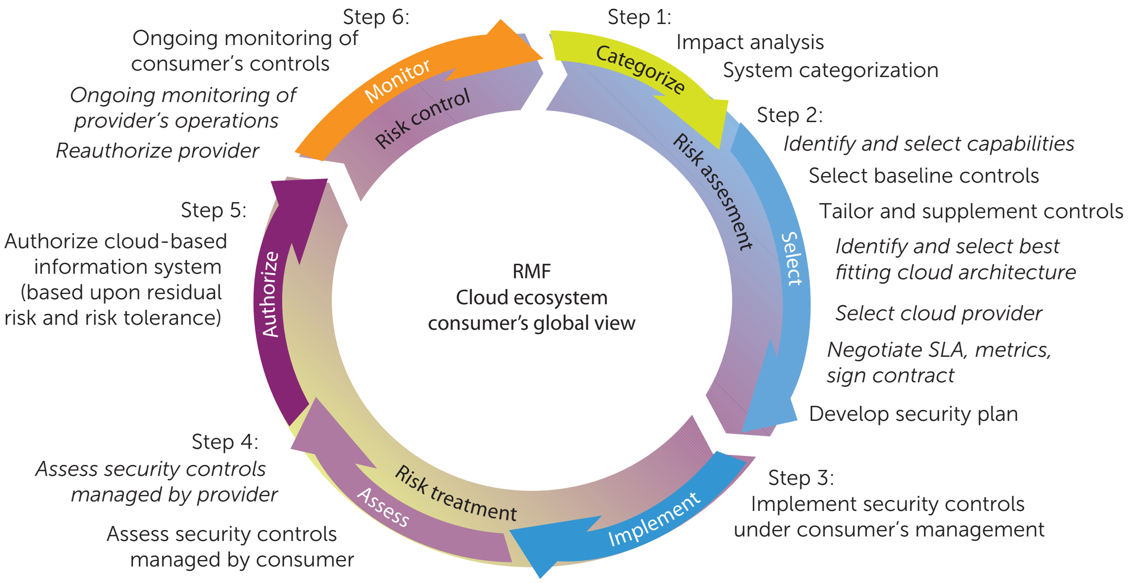
Step 6:
Ongoing monitoring of consumer's controls
Ongoing monitoring of provider's operations
Reauthorize provider
Monitor
Risk control
Step 1:
Impact analysis
System categorization
Categorize
Step 2:
Identify and select capabilities
Select baseline controls
Tailor and supplement controls
Identify and select best fitting cloud architecture
Select cloud provider
Negotiate SLA, metrics, sign contract
Develop security plan
Risk assessment
Select
RMF
Cloud ecosystem
consumer's global view
Step 5:
Authorize cloud-based information system (based upon residual risk and risk tolerance)
Authorize
Step 4:
Assess security controls managed by provider
Assess security controls managed by consumer
Assess
Risk treatment
Implement
Step 3:
Implement security controls under consumer's management

FIGURE 2. Cloud consumers' view of the risk management framework (RMF) applied to a cloud ecosystem.

6. 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.
7. National Institute of Standards and Technology, *Guide for Conducting Risk Assessment*, NIST Special Publication 800-30, Revision 1, 2012; http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
8. 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.
9. 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.

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 the cyberspace. Iorga has a PhD in engineering from Duke University. Contact her at michaela.iorga@nist.gov.*

ANIL KARMEL *is the cofounder and CEO of C2 Labs as well as the cochair of the National Institute of Standards and Technology's Cloud Security Working Group. His research interests include cloud computing security and privacy, secure DevOps, and container and microservices security. Karmel has a bachelor of science degree from the University of Illinois, Urbana/Champaign. Contact him at akarmel@c2labs.com.*