Table of Contents

List of Figures

List of Tables

Chapter 8 Managing Risk in the Cloud

Due to economies of scale, cloud Providers have the potential to offer state-of-the-art cloud Ecosystems that are resilient and secure—far more secure than the environments of Consumers who manage their own systems. This has the potential to greatly benefit many organizations. In Chapter 3, we discussed the need for businesses to gain visibility into a cloud Provider's service, to build the necessary trust and properly weigh the benefits of adopting a cloud-based solution to store a cloud Consumers' data. The sensitivity of the stored information needs to be considered 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, the type of data involved, the system's criticality/impact level, the cost savings, the service type, and any associated regulatory requirements.

Cloud-based information systems are exposed to *threats* that can have adverse effects on organizational operations (i.e., 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.

There are many types of risk that organizations need to address: program management, investment, budget, legal liability, safety, inventory, supply chain, security, and more. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Risk management activities can be grouped into three categories based upon the level at which they address the risk-related concerns:

a) The *organization* level (tier 1);
b) The *mission and business process* level (tier 2); and
c) The *information system* level (tier 3).

Risk management needs to be a cyclically executed process comprised of a set of coordinated activities for overseeing and controlling risks. This process targets the enhancement of strategic and tactical security and includes the execution of a *risk assessment*, the implementation of a *risk mitigation* strategy, and the employment of *risk control* techniques and procedures for the continuous monitoring of the security state of the information system. Cloud-based information systems, as with traditional information systems, require that risks be managed throughout the system development life cycle (SDLC).

In this chapter, we focus only on the tier 3 security risk related to the operation and use of cloud-based *information systems*. To prevent and mitigate any threats, adverse actions, service disruptions, attacks, or compromises, organizations need to quantify their *residual risk* below the *threshold* of the acceptable level of risk.

The information systems risk management (tier 3 risk management) is guided by the risk decisions at tier 1 and tier 2. Risk decisions at tiers 1 and 2 impact the ultimate selection of

the organization's systems based on their data sensitivity, the suitable cloud architecture[1] and of the safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from standardized catalogs of security and controls (i.e., National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, ISO/IEC 27001, ISO/IEC 27002, etc.).

In a cloud Ecosystem, the complex relationships among cloud Actors, the Actors' individual missions, business processes, and their supporting information systems require an integrated, ecosystem-wide risk management framework 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*.

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, each cloud Actor needs to further assign responsibilities to their senior leaders, executives and representatives;

- Establishment of the cloud Ecosystem-wide tolerance for risk and communicate this risk tolerance through their Service-Level Agreements (SLA), including the 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; and

- Accountability by the cloud Actors and near real-time information sharing of the cloud Actors' incidents, threats, risk management decisions, and solutions.

8.1 The Risk Management Framework

Risk is often expressed as a function of the *likelihood* that an adverse outcome occurs, multiplied by the *magnitude* of such an adverse outcome. In information security, *likelihood* is understood as a function of the threats to the system, the vulnerabilities that can be exploited, and the consequences of those vulnerabilities being exploited. Accordingly, security *risk assessments* focus on identifying where in the cloud Ecosystem damaging events could take place.

The risk-based approach of managing information systems is a holistic activity that needs to be fully integrated into every aspect of the organization, from planning to system development life cycle processes, to security controls allocation and continuous

[1] Cloud architecture combines a cloud deployment type (public, private, hybrid, community) and cloud service model (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)).

monitoring. Therefore, a Risk Management Framework (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. Some example interactions include providing the risk executive with feedback from ongoing monitoring and from authorization decisions; disseminating the updated risk information to authorizing officials and to information system owners; etc.

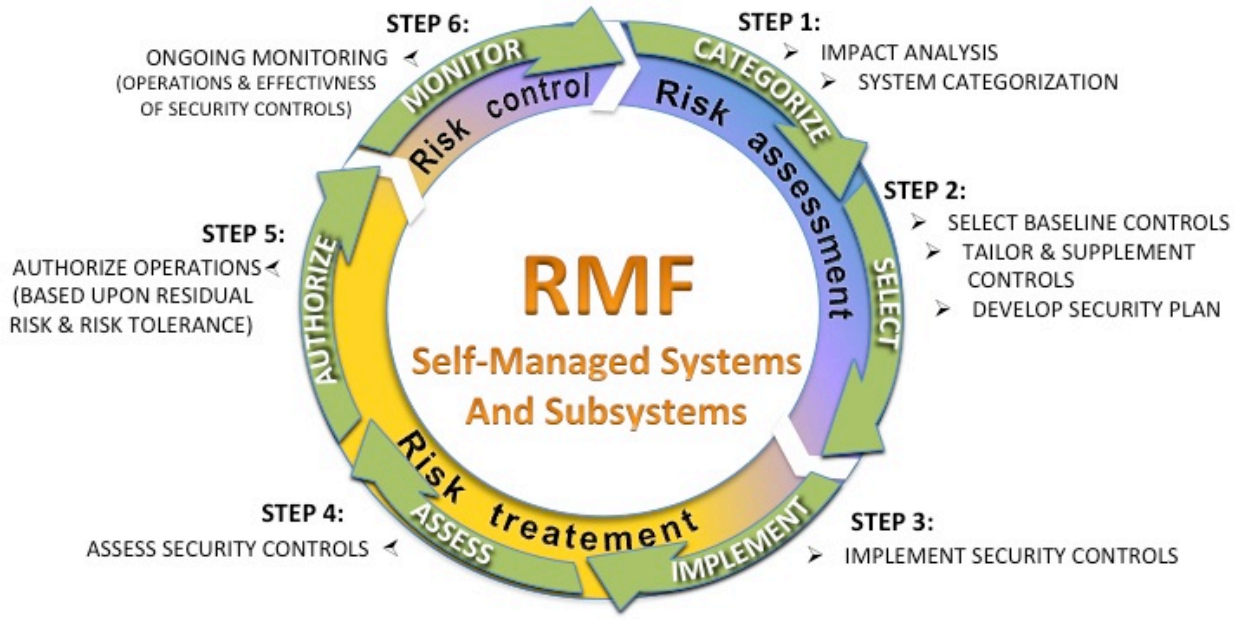

Figure 1: Risk Management Framework (NIST SP 800-37 Rev. 1)

The Risk Management Framework illustrated in Figure 1 reproduces the NIST Special Publication (SP) 800-37 Revision 1 risk management process - a process government agencies and private sector organizations have vetted as a best practice for their traditional information systems. As stated in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, 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 SDLC simultaneously with the functional and nonfunctional requirements. The security requirements need to be defined, and solutions should be researched and engineered from inception of the system's development. 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.

Table 1: Risk management activities and Risk Management Framework steps.

(NIST SP 800-37 Rev1)

Risk assessment (analyze cloud environment to identify potential vulnerabilities and shortcomings)	Step 1: 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.
	Step 2: Select, based on the security categorization, the initial set of security controls for the information system (referred to as baseline security controls). Then, tailor and supplement the baseline security controls set based on the organizational assessment of risk and the conditions of the operational environment. Develop a strategy for the continuous monitoring of security control effectiveness. Document all the controls in the security plan. Review and approve the security plan.
Risk treatment (design mitigation policies and plans)	Step 3: Implement the security controls and describe how the controls are employed within the information system and its environment of operation.
	Step 4: Assess the security controls using appropriate assessment procedures as documented in the assessment plan. The assessment determines if the controls are implemented correctly and if they are effective in producing the desired outcome.
	Step 5: Authorize information system operation based on the determined risk resulting from the operation of the information system and the decision that this risk is acceptable. The assessment is performed considering the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations.
Risk control (risk monitoring-surveying, reviewing events, identifying policy adjustments)	Step 6: Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of these changes, and reporting the security state of the system to designated organizational officials.

The process of applying the RMF's six well-defined, risk-related steps should be executed concurrently by selected individuals or groups in well-defined organizational roles, as part of (or in parallel with) the SDLC process. These steps or tasks are also listed in Table 1**,** in alignment with the risk management actions described earlier in this section.

NIST SP 800-37 Rev. 1 provides detailed information regarding security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The document promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes. The reader is encouraged to review NIST SP 800-37 Rev. 1, which is leveraged here for the current discussion of applying the RMF in a cloud Ecosystem. It is important to note that even though the NIST document addresses complex information systems composed of

multiple subsystems operated by different entities, it does not address cloud-based information systems, or any other kind of systems that leverage utility-based resources.

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, the cloud Consumers' level of control and direct management varies based upon the cloud deployment model.

Figure 2 is building upon the Consumer's level of control discussed in Chapter 3 of this book, and illustrates this aspect in parallel with the RMF applied to different layers of the functional stack, showing that for 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.

As stated above, Figure 2 also shows that the RMF process listed in

Table 1 and in NIST SP 800-37 Rev. 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 RMF as listed in

Table 1**,** is applied by the cloud Provider 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.

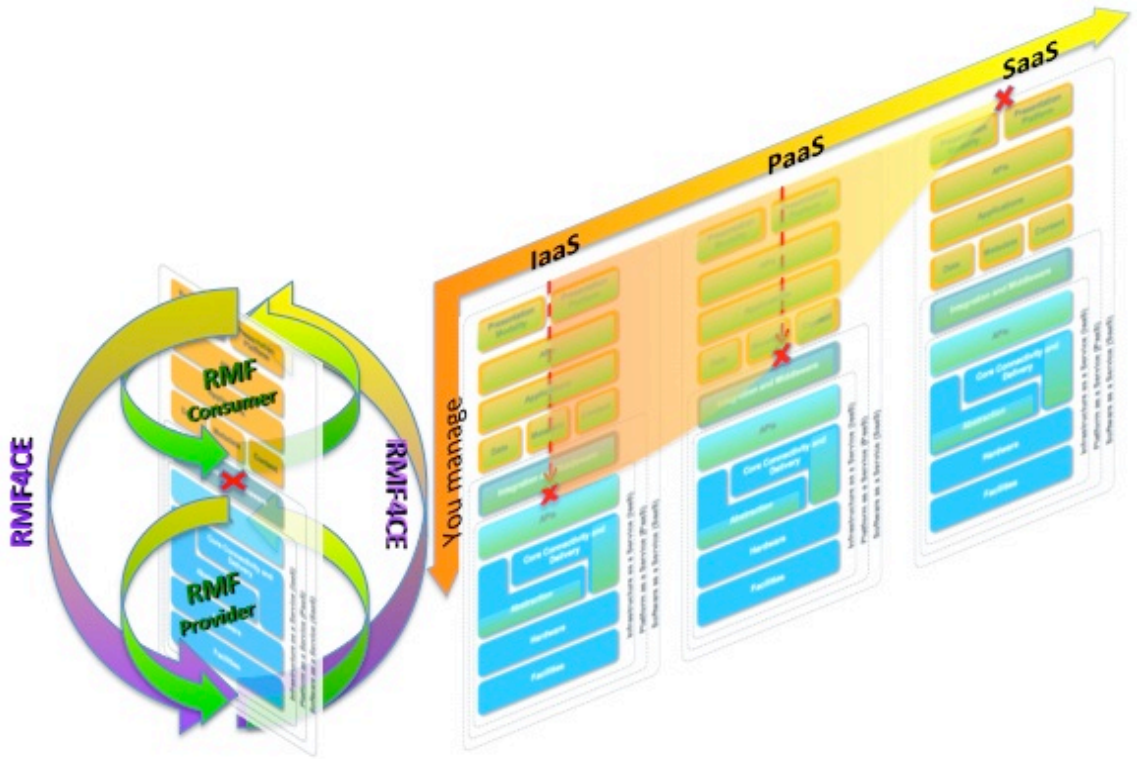

Figure 2: Applying Risk Management Framework to a cloud Ecosystem (RMF4CE).

However, prior to acquiring a cloud service, a cloud Consumer needs to analyze the risk associated with the adoption of 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 2 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. Section 8.3 further discusses this topic, after Section 8.2 provides an overview of the cloud Provider's risk management process.

8.2 Cloud Provider's Risk Management Process

Cloud Providers develop cloud architectures and build cloud services that incorporate core functionality and operational features, including security and privacy controls that meet baseline requirements. Their solutions aim to satisfy the needs of a large pool of cloud Consumers in a way that requires minimum customization. A cloud Provider's selection and implementation of its security and privacy controls considers their effectiveness, efficiency, and constraints based on applicable laws, directives, policies, standards, or regulations with which the cloud Provider must comply. The cloud Consumers' specific requirements and mandates are not known and therefore are projected as a generic core set.

In Chapter 3, Figures 8, 10, and 12 depict the *service boundaries* for IaaS, PaaS, and SaaS respectively, illustrating the set of resources allocated to a cloud service. 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 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 does not require additional tasks beyond those of a classical IT system; therefore, the risk management approach described in **Section 8.1** above is a good example of a broadly accepted, well-vetted approach.

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

8.3 Cloud Consumer's Risk Management Process

Generally speaking, organizations are more comfortable accepting risk when they have greater control over the processes and equipment involved. A high degree of control enables organizations to weigh alternatives, set priorities, and act decisively in their own best interest when faced with an incident. For successful adoption of a cloud-based information system solution, the cloud Consumer must be able to clearly understand the cloud-specific characteristics of the system, 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 a) identify all cloud-specific, risk-adjusted security and privacy controls; b) request from the cloud Providers and Brokers—when applicable and via contractual means—Service Agreements and Service-Level Agreements where the implementation of security and privacy controls is the cloud Providers' responsibility; c) assess the implementation of said security and privacy controls; and d) continuously monitor all identified security and privacy controls.

Since the cloud Consumers are directly managing and controlling the functional capabilities they implement, applying the RMF to these functional layers does not require additional tasks or operations than necessary in a classical IT system; therefore, the risk management approach described in **Section 8.1** above is a good example of a broadly accepted, well-vetted approach.

With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a cloud Consumer's organization. Since the adoption of a cloud-based solution does not inherently provide for the same level of security and compliance with the mandates in 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. Chapter 3 discussed at length the importance of visibility and trust in Section 3.4 and introduced the *trust boundary* in Section 3.5.

Characteristics of a cloud Ecosystem include:

- Broad network access,
- Decreased visibility and control by cloud Consumers,
- Dynamic system boundaries and comingled roles/responsibilities between the cloud Consumer and cloud Provider,
- Multi-tenancy,
- Data residency,
- Measured service, and
- Significant increase in scale (on demand), dynamics (elasticity, cost optimization), and complexity (automation, virtualization).

These 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 need the ability to identify all cloud-specific, risk-adjusted security and privacy controls in advance. 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 the security level of their environment 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.

Cloud Consumers are currently facing several challenges when seeking to determine which cloud service offering most effectively addresses their cloud computing requirement(s) while supporting their business and mission-critical processes and services in the most secure and efficient manner. The objective of this section is to apply, from the cloud Consumer's perspective, the Risk Management Framework described in **Section 8.1** and to demystify for the cloud Consumers the process of describing, identifying, categorizing, analyzing, and selecting cloud-based services.

In general, a cloud Consumer adopting a cloud-based solution needs to follow these steps:

1. Describe the service or application for which a cloud-based solution may be leveraged;
2. Identify all functional capabilities that must be implemented for this service;
3. Identify the security and privacy requirements and the security controls needed to secure the service or application. For adopters of NIST standards and guidelines, cloud Consumers need to determine the security category and associated impact level of information systems in accordance with Federal Information Processing

Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, respectively. The information system's impact level determines the security control baseline that needs to be implemented. Three sets of baseline controls correspond to low-impact, moderate-impact, and high-impact information systems.

4. Analyze and select the most appropriate cloud Ecosystem architecture, by combining a cloud deployment model (public, private, hybrid, community) and cloud service model (IaaS, PaaS, SaaS):
    - Public IaaS, Public PaaS, Public SaaS;
    - Private IaaS, Private PaaS, Private SaaS;
    - Hybrid IaaS, Hybrid PaaS, Hybrid SaaS; and
    - Community IaaS, Community PaaS, and Community SaaS.
5. Identify and select the cloud Actors involved in orchestrating the cloud Ecosystem (e.g., Provider(s) and/or Broker(s));
6. Understand the cloud Provider(s)' and Broker(s)' security posture and inherited security and privacy controls. Tailor the security and privacy controls to fulfill the security and privacy requirements for the particular use case or identify additional compensating security controls, when necessary;
7. Assign specific values to organization-defined security parameters via explicit assignment and selection statements;
8. Supplement baselines with additional security and privacy control enhancements, if needed; and
9. Provide additional specification information for the implementation of security and privacy controls.

Based upon the selected cloud Ecosystem architecture, the organization would retain and take upon itself the implementation of the security controls identified for the cloud Consumer, augmented with the supplemental set of controls specific to the Consumer's use case.

In Figure 3**,** we illustrate the RMF as applied to a cloud Ecosystem from the cloud Consumer's perspective. The additional operations and steps a cloud Consumer needs to perform are highlighted in blue.

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 SA between the cloud Consumer, cloud Provider, and Broker (when applicable). Contractual terms should include guarantees of the cloud Consumer's timely

access to or Provider's timely delivery of cloud audit logs, continuous monitoring logs, and any user access logs.

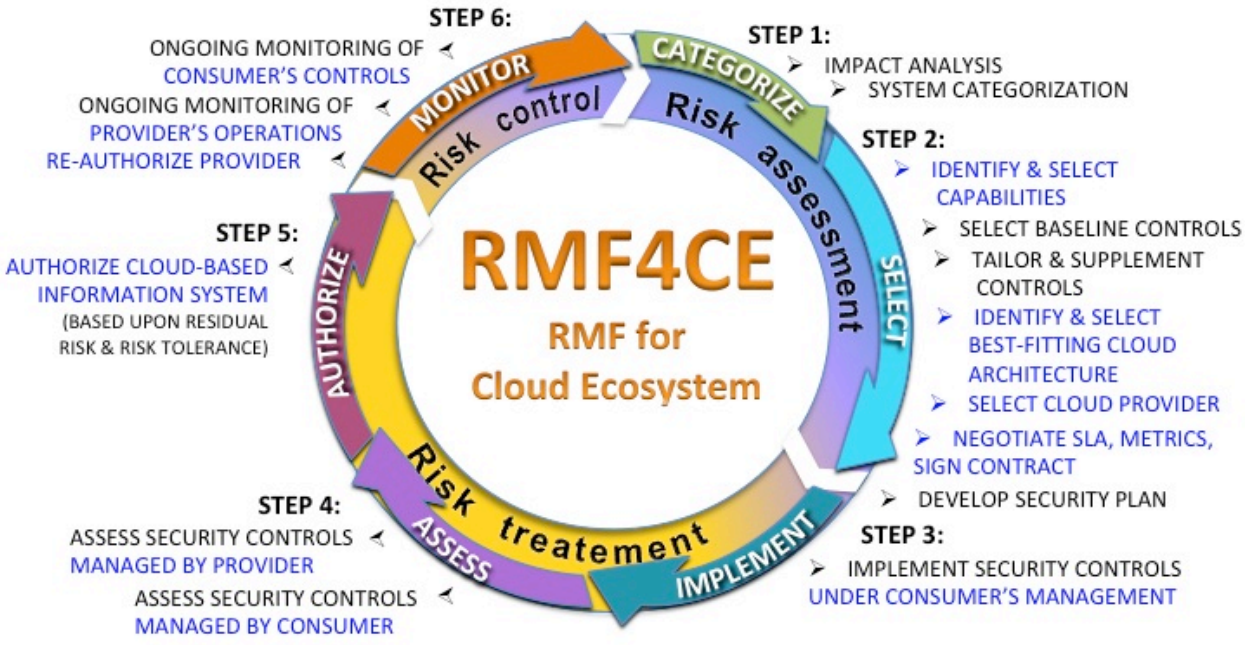

Figure 3: Cloud Consumers' View of the Risk Management Framework Applied to a Cloud Ecosystem

Table 2 aligns risk management activities with their corresponding steps from NIST SP 800-37 Rev. 1, and provides additional details that map to Figure 3 above.

Table 2: Risk Management Framework applied to a cloud Ecosystem - cloud Consumer's perspective.

Risk management activities	NIST SP 800-37 RMF Steps	Risk Management Framework Applied to a Cloud Ecosystem from the Cloud Consumer's Perspective
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, the associated baseline security controls based upon the system's impact level, the privacy controls, and the security control enhancements.
		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 SA 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 assess the systems' security posture.
		Reassess and reauthorize (periodic or ongoing) the cloud Provider's service.

The approach covered by the steps in Table 2 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.

A cloud Consumer remains responsible for performing a risk assessment, identifying all the security requirements for their cloud-based service(s), and selecting the appropriate security and privacy controls before selecting a cloud Provider(s) and/or Broker(s). Providers and Brokers that best meet the cloud Consumer's needs should be selected either directly or from a repository of authorized cloud suppliers. The cloud Consumer needs to perform a thorough assessment, ideally using third-party independent assessors, to assess the risk from using this service. Successful creation of and migration to a robust cloud Ecosystem depend on assessing a cloud Provider's security posture and system performance, identifying remaining security and privacy controls that should be implemented to secure the service or application, and identifying the cloud Actors responsible for implementing those controls. The set of remaining security and privacy controls needs to be addressed in agreements between the cloud Consumer and other relevant cloud Actors.

The SLA is the component of the SA that details the levels and types of services that are to be provided, including but not limited to, the delivery time and performance parameters. Cloud Providers use service-based agreements to describe their offerings and terms of service to potential cloud Consumers. In some cases, a cloud Consumer might be satisfied with the cloud Provider's offer and service terms; however, there are instances when the cloud Consumer is interested in a customer-based agreement and a customized service. The cloud Consumer needs to pay special attention to the SLAs and involve the organizations' procurement, technical, and policy experts to ensure that the terms of the SLA will allow the organization to fulfill its mission and performance requirements.

A challenge in comparing and selecting service offerings is that cloud Providers may offer a default contract written from the Provider's perspective. Such default contracts may not adequately meet the cloud Consumers needs and may constrain the visibility of the cloud Consumer into the delivery mechanisms of the service.

In summary, adopting a cloud-based solution for an information system requires from cloud Consumers to diligently identify their security requirement, assess each prospective service provider's security and privacy controls, negotiate SLA and SA and build trust with the cloud Provider before authorizing the service. A thorough risk analysis coupled with secure cloud Ecosystem orchestration introduced in this book, along with adequate guidance on negotiating SLAs, are intended to assist the cloud Consumer in managing risk and making informed decisions in adopting cloud services.

References

NIST Special Publication 800-37 (Revision 1): *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, February 2010.

NIST Special Publication 800-53 (Revision 4): *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 [updated January 22, 2015].

NIST Special Publication 800-144: *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011.

NIST Special Publication 800-145: *The NIST Definition of Cloud Computing*, September 2011.

NIST Special Publication 800-146: *Cloud Computing Synopsis and Recommendations,* May 2012.