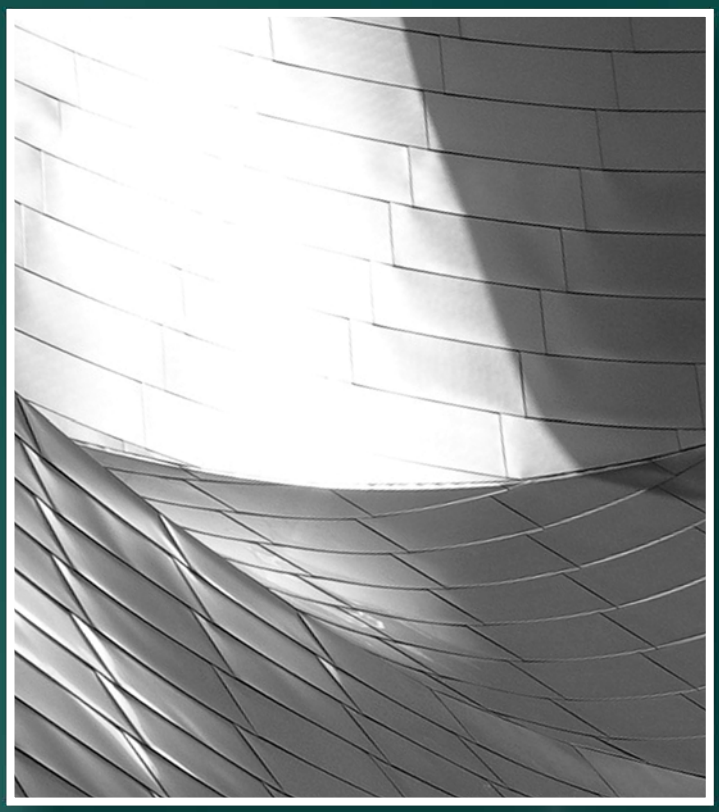

Appendix E

Cloud-Adapted Risk Management Framework

Risk management was introduced in Chapter 6 as a cyclically executed process comprising a set of coordinated activities for overseeing and controlling risks. This set of activities is composed of risk assessment, risk treatment, and risk control tasks that collectively target the enhancement of strategic and tactical security.

How confident cloud consumers feel about whether the amount of risk related to using cloud services is acceptable depends on how much trust they place on those involved in the surrounding cloud ecosystem's orchestration. The risk management process ensures that issues are identified and mitigated early on in the investment cycle and followed by periodic reviews. Since cloud consumers, cloud carriers, and other types of actors (such as cloud brokers), in a cloud ecosystem all have differing degrees of control over cloud-based IT resources, they need to share the responsibility of implementing the security requirements.

The Special Publication (SP) 500-299: NIST Cloud Computing Security Reference Architecture specification discusses several key aspects of managing risks associated with a cloud environment. The document highlights the high-level steps of the Cloud-Adapted Risk Management Framework (CRMF) and stresses the importance of adhering to the security conservation principle.

NOTE

Further details about the NIST Cloud Reference Architecture can be found in the NIST Special Publication 500-292: NIST Cloud Computing Reference Architecture.

Figure E.1 depicts the NIST Cloud Reference Architecture in the background, over which a graphical representation (as presented in NIST SP 500-299) of the secure orchestration of a cloud ecosystem is layered. This illustrates how secure orchestration encompasses all of the cloud actors and depicts their shared responsibilities in orchestrating and operating a cloud ecosystem.

Secure orchestrations typically have two intrinsic considerations. The first is the cloud delivery model (SaaS, PaaS, or IaaS), whose correlation can be depicted by building

blocks. The second is the cloud deployment model (public, private, hybrid, or community) that can most successfully fulfill the cloud consumer's business objectives and security requirements.

For each cloud-based solution, cloud consumers need to identify the threats, perform a risk assessment, and evaluate the security requirements of their individual cloud architectural context. The requirements also need to be mapped to the proper security controls and practices in the technical, operational, and management classes.

The type of cloud delivery model that is chosen for adoption does not impact the security posture of the cloud-based system. The overall security requirements either remain unchanged or at a logical constant, and are, at minimum, equivalent to the security requirements of an on-premise technology architecture or solution. Conversely, the type of deployment model that is selected does have an impact on the distribution of security responsibilities among the cloud actors, which relates to the security conservation principle as discussed in the NIST Special Publication 500-299.

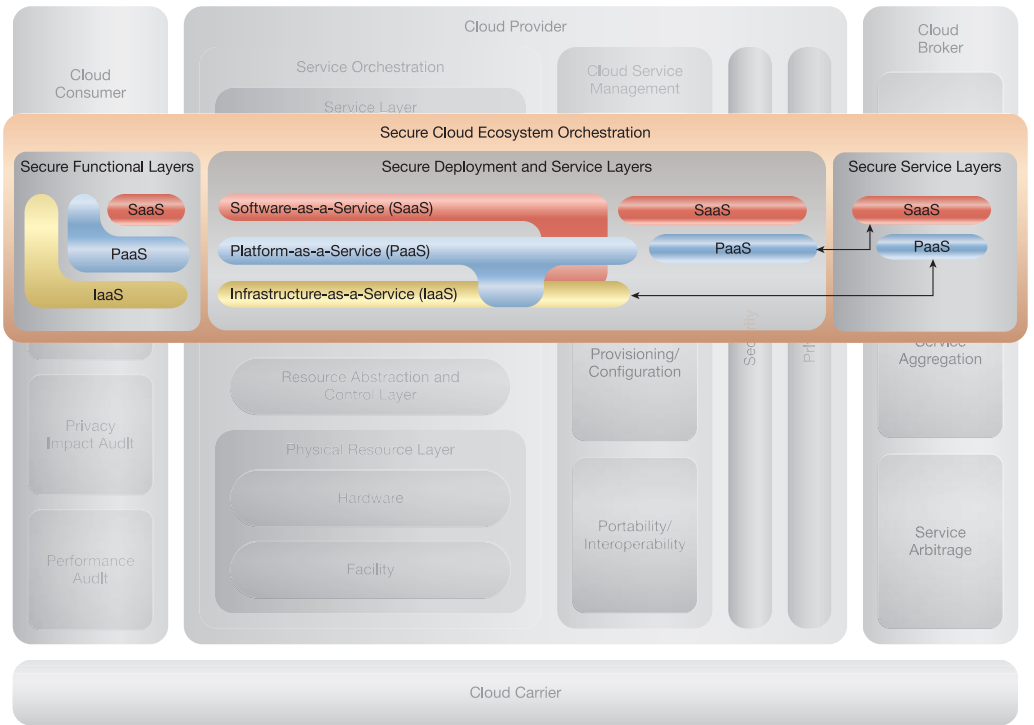

Figure E.1
A visual representation of the NIST Cloud Computing Reference Architecture and ecosystem orchestration.

When adopting cloud-based solutions, cloud consumers need to exercise due diligence in fully grasping the distinct security requirements that can be triggered, such as:

- broad network access
- data residency
- measured usage
- multitenancy
- dynamic system boundaries
- shared roles and responsibilities between the cloud consumer and cloud provider
- decrease in cloud consumer visibility
- decrease in cloud consumer control
- significant increase in scale (on demand)
- significant increase in dynamics (elasticity, cost optimization)
- significant increase in complexity (automation, virtualization)

These issues often present cloud consumers with security risks that are greater than or different from those in traditional on-premise solutions.

The key element to the successful adoption of a cloud-based system solution is the cloud consumer's full understanding of the cloud-specific traits and characteristics, the architectural components for each cloud service type and deployment model, and each cloud actor's role in orchestrating a secure ecosystem.

Furthermore, it is essential for the cloud consumers' business and mission-critical processes that they be able to identify all cloud-specific risk-adjusted security controls. The cloud consumers need to leverage their contractual agreements to hold the cloud providers (and cloud brokers) accountable for the implementation of the security controls. They also need to be able to assess the correct implementation and continuously monitor all identified security controls.

E.1 Security Conservation Principle

The core concept of the security conservation principle is that a cloud service's full set of security controls needs to remain unchanged or, in a logical sense, at a constant. The responsibility of fulfilling security requirements and implementing mitigatory actions

dynamically shifts between cloud actors according to the dynamics that occur within a cloud. Figure E.2 depicts the security conservation principle for the cloud ecosystem:

For simplicity's sake, this diagram identifies only the cloud consumer and cloud provider roles. It highlights the responsibility of implementing security controls being shared between the cloud consumer and cloud provider to different degrees, depending on which deployment model is adopted. The level of responsibility of either cloud actor fundamentally correlates to each cloud actor's level of control over certain "layers" of the cloud.

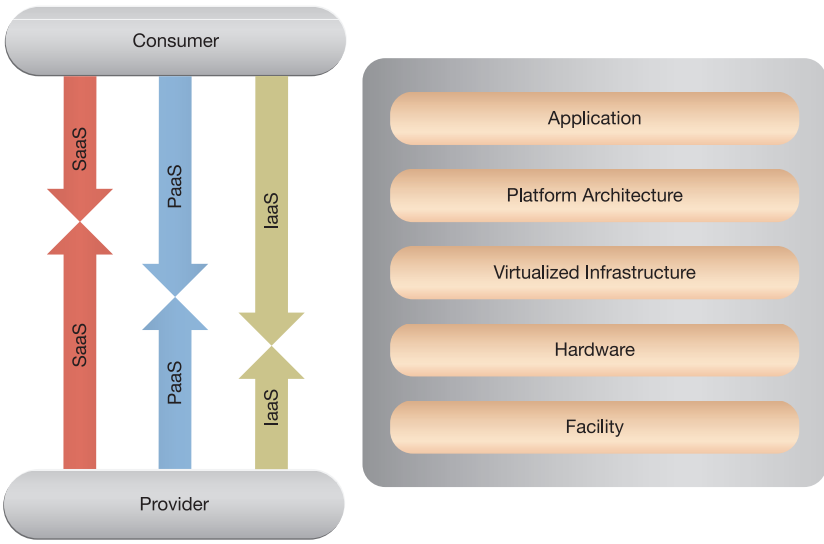

Figure E.2
A visual representation of the security conservation principle (courtesy of NIST, SP 500-299).

In SaaS clouds, the cloud provider assumes most of the responsibility for security controls implementation since the cloud consumer only controls the application layer. Conversely, cloud consumers of IaaS clouds may control everything except the hardware on which the cloud service runs and the facility storing the hardware, meaning they are primarily accountable.

NOTE

See NIST SP 500-299: "NIST Cloud Computing Security Reference Architecture" and NIST 800-144: "Guidelines on Security and Privacy in Public Cloud Computing" for further information.

E.2 The Risk Management Framework

A risk-based approach of managing information systems is a holistic activity that should be fully integrated into every aspect of the organization, from planning and system development lifecycle processes to security controls allocation and continuous monitoring. The selection and specification of security controls support effectiveness, efficiency, and constraints via appropriate laws, directives, policies, standards, and regulations.

The NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems provides a disciplined and structured process that integrates information security and risk management activities into the development lifecycle by identifying the following six steps:

- *Step 1* – Use an impact analysis to categorize the system and the information it processes, stores, and transmits.
- *Step 2* – Select the set of initial or baseline security controls for the system based on the security categorization. Tailor and supplement the set of baseline security controls according to the organizational assessment of the risk and the conditions of the operational environment. Develop a strategy for continuous monitoring to achieve security control effectiveness. Document all the controls in the security plan. Review and approve the security plan.
- *Step 3* – Implement the security controls and describe how the security controls are employed within the system and its environment of operation.
- *Step 4* – Assess the security controls using the appropriate procedures as documented in the assessment plan. This assessment determines whether the security controls have been implemented correctly and will effectively produce the intended outcome.
- *Step 5* – Authorize information system operation if the estimated risk resulting from the operation is acceptable. The assessment considers risk to organizational assets and operations (including mission, functions, image, or reputation), individuals, and other organizations.
- *Step 6* – Monitor the security controls on an ongoing basis. Monitoring includes 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 officials.

While the risk management framework is adaptable to most scenarios, it defaults to the traditional IT environment and requires customization to successfully address the

unique characteristics of cloud-based services and solutions. The CRMF closely follows the original RMF approach. Table E.1 shows the aforementioned six steps listed in the right column, with each step grouped into one of the three main activities in the left column that collectively comprise the risk management process:

CRMF	CRMF Steps
Risk Assessment	*Step 1* – Use an impact analysis to categorize the information system that has been migrated to the cloud, and the information that is processed, stored, and transmitted by that system. (This step is very similar to Step 1 of the traditional RMF.)
	Step 2 – Identify the security requirements of the system by performing a risk assessment (the Confidentiality, Integrity, and Availability (CIA) analysis is recommended). Select the baseline and tailored supplemental security controls.
Risk Treatment	*Step 3* – Select the cloud ecosystem architecture that best suits the assessment results for the system.
	Step 4 – Assess your service provider options. Identify the security controls needed for the system the cloud provider has implemented. Negotiate the implementation of any additional security controls that are identified. Identify any remaining security controls that fall under the cloud consumer's responsibility for their implementation.
Risk Control	*Step 5* – Select and authorize a cloud provider to host the cloud consumer's information system. Draft up a service agreement and SLA that list the negotiated contractual terms and conditions.
	Step 6 – Monitor the cloud provider to ensure that all service agreement and SLA terms are being met. Ensure that the cloud-based system maintains the necessary security posture. Monitor the security controls that fall under the cloud consumer's responsibility.

Table E.1

The six steps are mapped to each of the three activities comprising the CRMF.

Adopting the approach outlined by these steps enables organizations to systematically identify their common, hybrid, and system-specific security controls and other security requirements for procurement officials, cloud providers, cloud carriers and cloud brokers alike.

The CRMF can be used to address the security risks associated with cloud-based systems by incorporating possible outcomes into the cloud provider's contractual terms. Performance aspects of these terms and conditions also need to be represented in the SLA, which is an intrinsic part of the service agreement between the cloud consumer and cloud provider. Contractual terms should, for example, include guarantees concerning the cloud consumer's timely access to cloud audit logs and the details pertaining to the continuous monitoring of the logs.

If permitted by the adopted deployment model, the organization should implement both the cloud consumer's set of identified security controls and the specifically tailored supplemental security controls. Cloud consumers are advised to request that cloud providers (and cloud brokers) provide sufficient evidence to demonstrate that the security controls being used to protect their IT assets have been correctly implemented.