Managing Risk in a Cloud Ecosystem

Authors:
Dr. Michaela Iorga, NIST
Anil Karmel, C2 Labs Inc.

1.1 Overview

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 the level of transparency into the cloud Provider's. 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, 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.

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).

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*[1] below the *threshold* of the acceptable level of risk.

1.2 Security Risk and Cloud

The information systems risk management (tier 3 risk management) is guided by the risk decisions at tier 1 and tier 2. Information security requirements are satisfied by the

[1] Residual risk = Portion of risk remaining after security measures have been applied [CNSSI No. 4009]

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 the SP 500-293: *US Government Cloud Computing Roadmap*, NIST highlights in the vol 1 of the document that boundaries are more complex and therefore perimeter-based defense mechanisms are less effective. The complexity of the boundaries in a cloud ecosystem renders traditional *risk management* mechanisms less effective. Moreover, in a cloud Ecosystem, the complex relationships among cloud Actors[2], 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*.

In general, organizations have maximum flexibility on how *risk assessments* are conducted. Since *risk assessments* facilitate decision-making at all three *tiers* (organization level, mission/business process level, and information system level), they are 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 would like to recommend to our readers the NIST's Special Publication 800-30 Rev 1: "*Guide for Conducting Risk Assessment*" that provides quantitative, qualitative or semi-qualitative methods that use scores or levels, respectively.

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.

Risk is often expressed as a function of the *magnitude of harm* caused by the occurrence of a circumstance or event, multiply by the *likelihood of* its *occurrence*. In information

[2] see NIST Special Publication 500-292: *NIST Cloud Computing Reference Architecture,* September 2011

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 of managing information systems is a holistic activity that needs to be fully integrated into every aspect of the organization. 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.

The NIST Special Publication (SP) 800-37 Rev. 1 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 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 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.

The reader is encouraged to review NIST SP 800-37 Rev. 1, which is used here as reference framework for the current discussion of applying the RMF in a cloud Ecosystem. For the sake of brevity we will not review in this article the six steps and the tasks described in NIST SP 800-37 Rev. 1. 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 and hence the need for 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, the cloud Consumers' level of control and direct management varies based upon the cloud deployment model. NIST defined in the 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). 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 the 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 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.

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 1**,** below**,** 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, it is of critical importance for cloud Consumers to establish the clear demarcation of information-system boundaries on all levels in a vendor-neutral manner. Furthermore, it is incumbent upon the cloud Consumer to establish measures to ensure appropriate protection, regardless of vendor, ownership, or service level for the cloud-based information system.

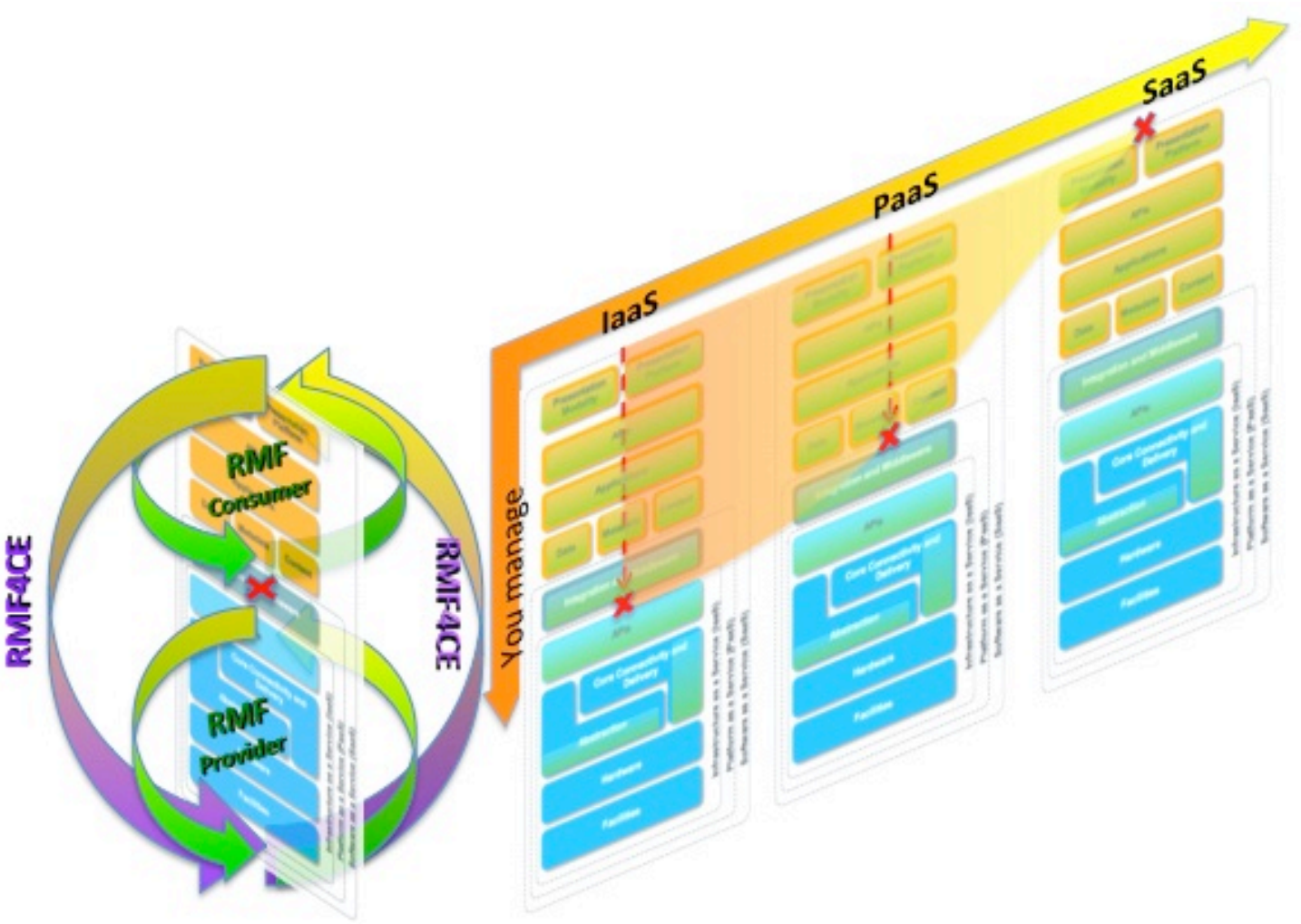

Figure 1: Applying Risk Management Framework to a cloud Ecosystem (RMF4CE).
Functional stack image courtesy of Cloud Security Alliance, 2009

1.3 Cloud Provider's Risk Management Process

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.

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, a risk management approach like the one discussed in Section 1.2 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.

1.4 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 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 discussed in Section 1.2 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.

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 need the ability 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 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.

In general, a cloud Consumer adopting a cloud-based solution needs to follow the same RMF steps discussed in Section 1.2 with additional tasks as listed in Table 1 and graphically depicted in Figure 2. in which, the additional tasks a cloud Consumer needs to perform are highlighted in blue.

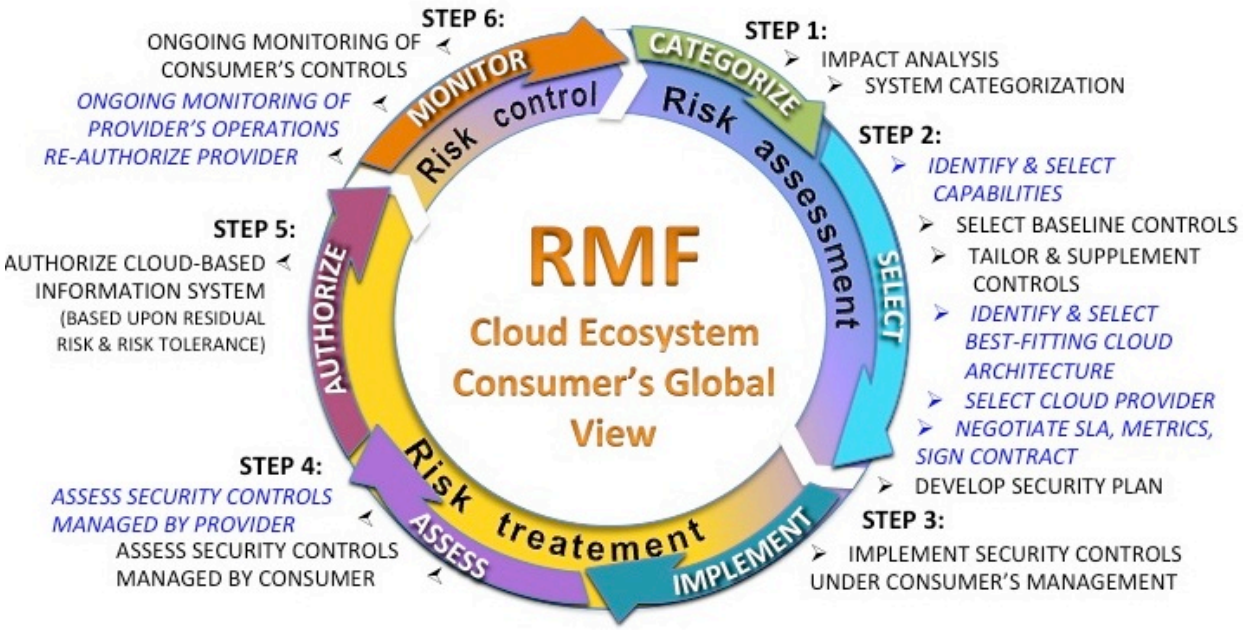

Figure 2: Cloud Consumers' View of the Risk Management Framework Applied to a Cloud Ecosystem

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

Table 1: 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,* Identify and select the associated baseline security controls based upon the system's impact level, 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 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 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.

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.

1.5 Conclusion

In summary, adopting a cloud-based solution for an information system requires 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 article, 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. (http://csrc.nist.gov/publications/PubsSPs.html)

NIST Special Publication 800-30 (Revision 1): *Guide for Conducting Risk Assessment*, Sept 2012. (http://csrc.nist.gov/publications/PubsSPs.html)

NIST Special Publication 800-53 (Revision 4): *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 [updated January 22, 2015]. (http://csrc.nist.gov/publications/PubsSPs.html)

NIST Special Publication 800-144: *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011. (http://csrc.nist.gov/publications/PubsSPs.html)

NIST Special Publication 800-145: *The NIST Definition of Cloud Computing*, September 2011. (http://csrc.nist.gov/publications/PubsSPs.html)

NIST Special Publication 800-146: *Cloud Computing Synopsis and Recommendations,* May 2012. (http://csrc.nist.gov/publications/PubsSPs.html).

NIST Special Publication 500-292: *NIST Cloud Computing Reference Architecture,* September 2011 (http://www.nist.gov/itl/cloud/publications.cfm).

NIST Special Publication 500-293, Vol 1 and 2: US Government Cloud Computing Technology Roadmap, October 2014 (http://www.nist.gov/itl/cloud/publications.cfm).

NIST Special Publication 500-299: NIST Cloud Security Reference Architecture (draft) (http://www.nist.gov/itl/cloud/publications.cfm).

ISO/IEC 27001:2013: Information technology – Security techniques – Information security management – Requirements, 2013.
(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534).

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls, 2013.
(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533)