Information Security Continuous Monitoring (ISCM) Requirements and the Public Cloud

Key Ideas:

- Public cloud IaaS offerings provide tremendous opportunities for cost savings coupled with increased availability and scalability to optimize performance.
- ISCM (as introduced within NIST SP 800-137) requires on-going monitoring of information systems.
- Users share responsibility with cloud providers for ISCM on the infrastructure layer. Users are responsible to track and monitor utilization and usage of compute, storage, memory, and other associated resources.
- Public cloud architecture is fundamentally different than that of a data center and, consequently, the old data center tools fail to provide adequate functionality.
- Automated tools offer particular value given the dynamic nature of the public cloud.

IaaS – The Public Cloud

Public cloud IaaS offerings are increasingly popular alternative to the traditional data center. This popularity stems from a number of areas with availability, scalability, and cost representing the most common.

When considering availability and scalability, IaaS removes the need to pinpoint capacity prior to deployment. Instead of the traditional provisioning model – and the weeks or months that the traditional model requires to add resources – IaaS users are able to rapidly provision resources both up and down to meet capacity demands. The standardized nature and architecture of resources within the IaaS environment insures that demand spikes and lulls are easily accommodated. These features combine to improve overall performance.

When considering cost, cloud IaaS provides users the opportunity to replace up-front capital infrastructure expenses with metered variable costs. IaaS users "rent" necessary resources. Users do not need to build their own datacenter or purchase their own resources. They can entirely avoid CapEx expense. Further, users purchase only the amount required "in the moment". This flexibility enables users to reduce operating costs and purchase resources according real time needs, rather than for maximum peak capacity. Finally, the IaaS provider maintains the infrastructure. This provides a reduction of necessary in-house IT staffing and removes the costs associated with datacenter operation and maintenance.

Information Security Continuous Monitoring

The organization should collect and analyze available data about the state of the system regularly… The goal is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and to respond by accepting, avoiding, or mitigating risk as situations change.[1]

Information Security Continuous Monitoring (ISCM) is defined with NIST SP 800-137 as: "*maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."* [2] Thus, rather than viewing security as a static "point in time", ISCM acknowledges that true information security requires on-going operations.

ISCM resides within Risk Management Framework (RMF) Step 6 which demands an "*ongoing assessment of security control effectiveness supports a system's security authorization over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes."*[3] Fulfillment of this Step is critical to maintaining acceptable compliance.

---

[1] NIST Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, p. 9; http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.
[2] NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, p. 6; http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.
[3] Id. at 17.

The underlying goal of ISCM is to provide *"organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions."*[4] Effective ISCM delivers responsible parties a continuous stream of snapshots of the state of risk to their security, data, and resources. The real-time monitoring of implemented technical controls provides a dynamic view of the effectiveness of those controls. This, in turn, enables decision makers to efficiently improve the organization's security posture.[5]

Further embodied within the value proposition of ISCM is the premise that enterprise architecture, availability, and configurations, are fundamental to ongoing management of information security-related risks.[6] Specifically, assuring performance on the application level is insufficient. Information security-related risks also arise from the loss of confidentiality, *"integrity, or availability of information or information systems."*[7] Note the inclusion of "information systems". The meaning is unmistakable: the security and monitoring of cloud layer infrastructure is critical. Most importantly, failure to track and monitor resources violates NIST compliance standards and leaves users vulnerable to security events.

Users and Providers Share Responsibility for ISCM

"Accountability for security and privacy in public cloud deployments cannot be delegated to a cloud provider and remains an obligation for the organization to fulfill. Federal agencies must ensure that any selected public cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization".[8]

---

[4] NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, p. 16; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[5] NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, p. 7; http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.
[6] Id. at 24; "Risk tolerance, enterprise architecture, security architecture, security configurations, plans for changes to the enterprise architecture, and available threat information provide data that is fundamental to the execution of these steps and to ongoing management of information security-related risks."
[7] NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, p. 19; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[8] NIST Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, p. 62; http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

FISMA controls, as outlined with NIST SP 800-53 (Revision 4), contain a large array of controls that apply to information systems. These range from awareness and training to configuration management to physical environment protection.[9] Importantly, when using the public cloud, users must recognize that fulfilling these controls is a shared responsibility. As explained in NIST SP 800-144, users retain ultimate accountability and should similarly take action to insure that information security is adequately managed.

NIST SP 800-125 further clarifies the need for vigilance throughout the computational stack: "*Virtualization provides simulation of hardware such as storage and network interfaces. This infrastructure is as important to the security of a virtualized guest OS as real hardware infrastructure is to an operating system running on a physical computer.*" [10]

Most importantly, information security cannot simply be outsourced to the cloud provider. Users remain responsible for issues ranging from resource configuration to storage security to availability and cost concerns. ISCM dictates that these issues need to be continuously reviewed. Audit and compliance requirements dictate that changes and tracking be available.

The Public Cloud is Fundamentally Different

"A public cloud computing environment is extremely complex compared with that of a traditional data center." [11]

Users are often quite familiar with the demands and challenges encountered when providing ISCM for a datacenter. The cloud, however, possesses fundamentally different architecture and its operation have a fundamentally different dynamic.

---

[9] NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[10] NIST Special Publication 800-125, *Guide to Security for Full Virtualization Technologies*, p.25; http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf.
[11] NIST Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, p. 20; http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

Resources do not reside within the same traditional firewalls. This structural alteration has significant implications for both computing and data resources. For example, storage buckets need to be properly permissioned and accessible IP addresses of computational resources need to be carefully set and monitored. Whereas a data center firewall allowed centralized control of security, the decentralized cloud structure places greater burdens upon IT operations. Specifically, IT operations retain the responsibility for maintaining security, but IT operations loses the ability to control traffic flow in and out of the deployment.

The distributed nature of the cloud also places fresh challenges from the perspective of resource control. Unlike the data center, cloud resource control is not centralized within IT operations. Within the cloud, resource control is diffused among users. Individual users do not need to notify or requisition additional IT resources. Instead, these same users can quickly create and terminate resources without ever notifying the central IT department. This places unique monitoring, tracking, and security burdens upon IT operations. Whereas centralized control insures a record of transactions, this model challenges everything from the ability to accurately inventory resources to the ability to insure that proper security protocols are being followed on individual computational and storage resources.

Further complicating ISCM in the cloud is the lack of cloud resource persistence. Computational, memory, and storage resources do not necessarily persist within the cloud. Resources are provisioned and terminated by users as needs arise. Similarly, assigned IP addresses do not persist within the cloud environment. Consequently, key traditional data center security tool methodology fails within the cloud environment. Agents, IP scans, and port scans all fail to effectively operate because of the dynamic and variable resource usage.

Finally, without ownership and stringent control of core infrastructure and computational resources, all of these issues are magnified. Unlike the traditional data center model, there are limitations of access. Cloud users are forced to rely upon assurances from cloud provider concerning portions of physical and logical security. Also, depending upon chosen provider, the responsibility boundaries in both of these areas vary.

Automated Tools

Regulatory compliance requirements … may call for specific levels and granularities of audit logging, generation of alerts, activity reporting, and data retention. Traditional forms of direct assessment may not be feasible… [12]

Effective ISCM for cloud operation can be particularly labor intensive and budget debilitating. The reasoning is obvious: cloud operations are dynamic. Consequently, there are far more areas to be monitored and those areas require more frequent monitoring. NIST SP 800-137 is referencing the embedded difficulties within its observations that, *"Real-time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the effectiveness of those controls and the security posture of the organization."* [13] The publication continues with the recommendation that *"organizations can make more effective use of their security budgets by implementing technologies to automate many of the ISCM activities in support of organizational risk management policy and strategy, operational security, internal and external compliance, reporting, and documentation needs.*[14]

When selecting automated tools, users should seek cloud-native solutions. Given the complexity of cloud architecture, this category of solutions is particularly useful when considering automation.[15] Cloud native solutions are specially tailored to function within the dynamic cloud environment. They do not rely upon static scans or deposited agents. Rather, the best automated tools operate fully within the cloud environment and are capable of monitoring and reporting upon its dynamic nature.

Plainly, the increased need for monitoring and reporting combined with the newfound complexity of cloud operations makes effective ISCM even more difficult. Automation augments the security processes by reducing time spent redundant tasks. This, in turn,

---

[12] NIST Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, p. 66; http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.
[13] NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, p. 7; http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.
[14] NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, p. 63; http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.
[15] As discussed earlier, cloud architecture differs from that of the traditional data center. Just as one would not attempt to assess an electric engine with traditional internal combustion tools, one should not attempt to assess a cloud environment with traditional data center tools.

increases the amount of time trained professionals may spend on tasks requiring human cognition.[16] Thus, automated solutions lower costs, enhance efficiency, and improve the reliability of monitoring security-related information.[17]

About CloudCheckr:
CloudCheckr is a software development company based in Rochester, NY. It has developed the leading ISCM solution for AWS and public cloud users. To learn more about ISCM, CloudCheckr and its best-in-class solutions, please visit www.cloudcheckr.com.

About the author:
Aaron Klein is a Founder and COO of CloudCheckr. Aaron has written numerous articles and white papers on AWS, public cloud monitoring, and security from government and enterprise perspectives. To read more about Aaron's background, please visit his bio at: http://cloudcheckr.com/our-company/leadership-team/

[16] NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, p. 19; http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.
[17] Id.