Rethinking Common Controls for Cloud-Based Federal Information Systems

- Published on July 1, 2019
- **Edit article**
- **View stats**

Sarbari Gupta

Founder and CEO, Electrosoft
5 articles

Common controls serve a very important purpose within the realm of information security compliance and operations. However, with the rapid proliferation of cloud-based information systems, there needs to be further clarity in the nomenclature as well as improved guidance regarding inheritance of common controls implemented within an organization versus controls implemented by an external entity such as a cloud service provider (CSP).

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 4 defines common control as "a security control that is inheritable by one or more organizational information systems" and the revised Office of Management and Budget (OMB) Circular A-130 defines common control as a "security or privacy control that is inherited by multiple information systems or programs."

In a traditional IT environment, common controls were considered to be security controls that could be implemented centrally within an organization to support the security requirements for one or more organizational information systems. For example, consider a federal agency that implements 20 distinct information systems (general support systems and major applications). The physical security controls required by NIST SP 800-53 can be implemented centrally within the agency and support the security authorization of most or all of that agency's information systems. Similarly, security controls related to security policies and procedures, security training and acquisition could be implemented very effectively as common controls within the agency. Implemented properly, common controls reduce the burden on individual system owners within an organization and enable implementation of the controls in a standardized, consistent and cost-effective manner.

However, modern day information systems are much more complex. Many agencies are rapidly transitioning their existing information systems to leverage cloud services in the form of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Services (SaaS). These cloud services are provisioned by CSPs external to the agency. Controls that are typically good candidates for allocation as common controls within an organization are often poor candidates for allocation as common controls when implemented by an external entity such as a CSP. Consider controls that implement security policies and procedures, physical security controls and training. When these controls are implemented by a CSP, it may not be appropriate to consider these controls as *common controls* that can be inherited by the agency information system using the cloud service.

While the above logic may appear obvious to security experts, we need to remember that for a typical federal information system categorized at the MODERATE impact level (per Federal Information Processing Standard 199), over 250 controls and control enhancements need to be selected and specified in accordance with NIST SP 800-53. While this is a daunting exercise for system owners in general, it can be made easier when an agency has identified and authorized common controls that can be inherited by other information systems within that agency.

When an agency information system leverages an IaaS/PaaS/SaaS cloud offering, things get more complicated. If the CSP is FedRAMP-authorized, it is very tempting for the system owner to assume that most, if not all, of the security controls implemented by the CSP can be inherited by the agency information system. As described above, though, this may lead to the inappropriate allocation of some controls as common controls that may put the agency information system at significant risk. A well-informed and security-savvy system owner may decide to evaluate each of the security controls implemented by the CSP to determine whether it can be inherited by the agency information system. However, this is a non-trivial exercise.

The FedRAMP body of guidance and templates seek to facilitate the authorization of CSPs to promote agency use of secure cloud services. There is little guidance for system owners that are trying to determine which controls implemented within the authorization boundary for the CSP can be inherited by the agency information system that is leveraging that CSP.

NIST SP 800-53, Rev 4 provides the three baselines for security controls based on the impact level (HIGH, MODERATE or LOW) of the information system. A significant assumption made in NIST SP 800-53, Rev 4 in developing these baselines is that "information systems are located in physical facilities." In other words, if you are implementing an information system that is leveraging cloud services, you are somewhat on your own with respect to the selection and allocation of security controls in your baseline. After the system owner selects the appropriate baseline, what follows is the difficult task of tailoring the baseline security controls to align the controls with the specific conditions within the organization and the information system. The first step of tailoring is identifying and designating common controls. As pointed out above, this is a non-trivial exercise for system owners in general and is even more challenging for agency information systems that are utilizing cloud services.

I believe that overloading the term ***common controls*** to include controls implemented by external entities (such as a CSP) adds more confusion than clarity. It makes it more difficult for system owners to differentiate between common controls implemented by providers within the agency from similar controls implemented by a CSP (and possibly not good candidates for inheritance). It may be better to call such controls ***external controls*** while acknowledging that certain external controls may be inherited by an agency information system. Adding a distinct term for externally-implemented security controls and developing additional *guidance on the potential inheritability of external controls* would be tremendously helpful to system owners as they manage the risk of implementing modern, cloud-based information systems.

- Sarbari Gupta, Information Security Evangelist