WHITE PAPER

Reducing Security and Compliance Risk

Summary of Roundtable, hosted by ATARC on December 1, 2021

During a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC), experts from various Federal agencies shared principles and practices needed to reduce IT security and compliance risk. Participants also discussed the impact a recent Executive Order on Improving the Nation's Cybersecurity may have on compliance and risk management decisions.

Security and Compliance Risk

Roundtable participants agree that allocating time for compliance while simultaneously mitigating security risks and providing high customer value is a challenging balance to achieve. Agencies shared that while compliance is important, reducing security risk often takes priority. Equally important is ensuring taxpayer dollars are used wisely as agencies decide how to allocate resources between security and compliance.

IT professionals understand that there are different levels of risk within an agency and between systems. Disparate systems and processes usually do not contain the same level of risk at a given time and should not be addressed the same. Panelists shared that agencies need to identify and codify these disparate systems in order to identify priorities and to responsibly allocate resources.

Compliance is an important aspect of Federal agency operations, but at its essence, compliance is monitoring and reporting on known risk that agencies should already be mitigating. Roundtable participants shared that the focus and resources of agencies should be put towards locating unknown security risks, rather than spending time reporting on compliance measures that can likely be automated. In this sense, time spent on compliance can be seen as a risk as resources are diverted from identifying unknown security risks.

Adding complexity to compliance is the recent Executive Order on Improving the Nation's Cybersecurity issued by President Biden in May 2021. All roundtable participants agree that the intentions of the Executive Order to standardize and bolster cybersecurity protocols across all Federal agencies is well intentioned; however, the Order raises questions about the operational realities of achieving full compliance, and whether additional resources will be made available for agencies to meet the ambitious security and compliance targets set by the Order.

Agencies represented on the panel shared that many of the Zero-trust cybersecurity protocols and mandates called for in the Executive Order are already in place or scheduled for implementation. Zero-trust protocols like multi-factor authentication, role-based access, and encryption are security practices agencies currently utilize and should be standard best practice across the Federal government. What the Executive Order has done is set the same risk priorities for all Federal agencies. While there are many similarities between agencies, no two agencies experience the same risk or the same level of risk.

The Challenge of Balance

> The May 2021 Executive Order on Improving the Nation's Cybersecurity set the same risk priorities for all Federal agencies. While there are many similarities between agencies, no two agencies experience the same risk or the same level of risk.

Agency leaders aim to provide a reasonable level of security for their agency while meeting the intent of the Executive Order, but they are cautious to ensure taxpayer dollars are not being spent on protocols or programs that are not aligned with the agency's mission. Roundtable participants shared concern of the possibility that the mandates in the Executive Order could lead to over-security in certain instances for the sake of compliance.

When going through the compliance process, agencies are often challenged by the Inspector General (IG) when compliance is not completely met and the nuances surrounding decisions are not clearly understood. Because security risk is unique to each agency and system, agencies must make judgement calls based on individualized risk levels. While technically non-compliant, agencies bolster these decisions with data and analysis to educate the IG on the bigger picture.

Agencies and executives know that achieving compliance with the Executive Order is a multi-year effort. Roundtable participants believe that the Executive Order is intended to push the Federal government towards real change. Agencies will continue to have conversations with auditors and educate them on the nuances of security risk in the hopes that the IG advocates for additional resources to help with compliance.

Automating Security and Compliance

Having quick access to and obtaining information on security risk and compliance documentation are what drives risk management decisions. Locating and anticipating security risk dictate how resources are allocated. As technology advances, security risks inherently increase as do compliance requirements. Not only that, but the needs of the customer become more frequent and urgent as more features and options become available with technology.

Federal agencies must be able to make risk decisions and operate at the same speed as commercial entities. As such, risk management frameworks are evolving from three-year cycles to continuous ones, which help to identify security issues as they emerge. Roundtable participants believe agencies should be placing more focus on risk management rather than compliance management due to the constantly changing environment, but they cannot do so by looking at paper documents alone. Agencies need real-time data and automated processes in order to clearly see security risks and trends and quickly respond to them.

As more teams implement Agile and DevOps frameworks, incorporating security into all team layers from the onset is becoming a standard practice. Security is frequently automated through initial programming or artificial intelligence (AI) integrations. This is especially true when operating in the cloud and functions can be made public instantaneously compared with the production timelines of legacy systems. Agencies have learned from experience that instead of waiting for problems to appear on compliance reports or other manual processes, they can now be identified and fixed much more quickly through automation.

From an operational standpoint, agencies know much more quickly where risks are located and therefore how to allocate resources. What is perhaps more important is monitoring security automations so they do not themselves become security risks. Automating awareness prevents agencies from missing any security risks within processes that have been automated. A human element will always be required despite building feedback loops into automation programs.

Automating Compliance

Automating security features is critically important to successful operations, but so is automating compliance. By nature, compliance documentation is not proactive and does nothing to help identify unknown risks. With continuous monitoring, agencies are aware of other risk factors than the ones already known. By automating compliance, resources become available to focus on security and to address risk that if left unchecked could infiltrate entire organizations.

The ability to access and share data on-demand yields real-time decisions and fast change authorizations, thereby reducing security risk. Roundtable participants believe that the fastest path to providing value in not only security but also customer delivery, is implementing AI technology to pull data from different systems into a single dashboard, creating a clear picture of anything agencies need to monitor. It is usually not practical or financially feasible for the government to completely replace legacy systems with new technology, which is why layering AI technology into existing systems to bridge information is critical to automating security and compliance processes quickly.

Roundtable participants agree that having good situational awareness of where risks are located is how good risk management decisions are made. Automating both security and compliance is the only way to ensure decision-making keeps pace with advancements in technology. As Federal agencies continue working towards compliance of the Executive Order, participants advocate for building stronger partnerships with the IG in order to reframe the use of compliance in improving security. Changing the definition of a successful audit could also help drive quality and value throughout all Federal agencies by focusing on how compliance can improve security instead of maintaining compliance for compliance's sake.

Contact ATARC today to learn more about our Roundtables!