FEDInsider

4 Ways Agencies Can Align Identities & Ensure Successful Audits

Federal agencies are charged with collecting and protecting a variety of important and sensitive information. This can range from the personal information about citizens they serve to military secrets, and everything in between. Much of that information is protected not just by technology, but by laws and regulations about how it can be accessed and ultimately used. So it's no surprise that there is a very detailed and ongoing auditing process by which the government ensures the integrity of its data and protections.

Federal audits address regulatory compliance and evaluate each agency's aptitude in protecting the integrity of their IT systems. Agencies are constantly assessed on their identity management policies, and their ability to prevent and detect inappropriate access by employees, contractors, bad actors or unauthorized users.

The auditing process in government is complex and multifaceted, but ultimately is designed to help improve agencies' operations. Four experts working at all stages of the federal government's auditing process recently joined a FedInsider virtual panel to talk about ways that agencies could use audits to drive success and improve operations. The following are some of their key thoughts about how to ensure a successful federal audit.

Study & Understand the NIST Frameworks, Especially SP 800-63-3

Because many federal audits look at the integrity of data held by agencies, having good identity management is a key factor in keeping it safe. Agencies need to tightly control who has access to what data, and they must constantly monitor for any deviations to those rules. One of the most important frameworks to use when evaluating an identity management program is the NIST Special Publication 800-63-3, the Digital Identity Guidelines. Considered the gold standard in this area, it sits at the core of many government audits.

"The standard itself is extensive and is published in four volumes that address the complete scope of identity management processes," said David Temoshok, the Senior Advisor for Applied Cybersecurity with the NIST Information Technology Laboratory. "It includes identity proofing and enrollment, digital authentication processes and controls, identity federation and the application of risk management principles to identity management in order to both implement FISMA and to meet the risk management frameworks that NIST has published."

Temoshok said that the standard was created to be flexible, with low, medium and high assurance levels. That way, agencies can apply the correct level of security to the various types of data that they protect.

Featuring:

- **Nick Marinos**
  Director, I.T. & Cybersecurity Team, GAO

- **David Temoshok**
  Senior Advisor, Applied Cybersecurity, NIST I.T. Laboratory

- **Alvin "Tony" Plater**
  Acting CIO, Department of the Navy Laboratory

- **Brian Cooke**
  Sr. Security Manager, Accenture Federal Services, Homeland Security Account

Audit Preparation Is a Key to Ultimate Success

Because of the importance of the auditing process, it can sometimes seem extremely grueling to agencies that are undergoing it. But Alvin "Tony" Plater, the Acting Chief Information Security Officer for the Department of the Navy, has gone through many audits without any major problems. He says the key to his success is working with a good team, bringing in the right experts and undergoing a lot of intense preparation prior to the start of the audit.

"So preparation for me typically involves a formal kickoff where

we ensure senior leadership is involved," Plater said. "And then looking at the scope of the audit when it's announced, making sure it's a chief innovation officer or whether it's a chief technical officer who needs to be involved. And then from a cybersecurity perspective, I don't hesitate to bring in the deputy systems administrators as well as the authorization officials or the program officers."

Plater says that managing expectations for a pending audit is critical to its success. Agencies need to fully understand the scope of the audit, make sure the right people are in place, and be ready to assist the auditors with whatever they need to collect the right information.

Find Both Short & Long Term Solutions for Legacy Systems

One of the biggest challenges that many agencies face when trying to pass an audit is how to apply good identity management practices to legacy systems that were never designed to support the higher level of interactivity and controls that the regulations require. "The challenge is to have some sort of an approach that is universal for all of these different legacy systems out there that all have very different technologies," said Senior Security Manager with Accenture Federal Services on the Homeland Security Account Brian Cook. "So in my experience, that has been the biggest challenge, trying to come up with a way to respond to the audit, to answer the questions, when dealing with legacy systems."

Despite the troubles with legacy hardware, Cook says agencies facing an audit should resist the urge to immediately implement modernization or replacement programs that might take years to complete. Instead, focus on ways to centralize and manage data coming from legacy systems which can be used to pass the audit. Then use that work as a foundation to streamline the modernization project in the future.

Remember That Government Auditors Are Ultimately on Your Side

While the audit process can sometimes seem like an adversarial one, it's important to remember that the ultimate goal of an audit is to improve security, identity management and data handling within government. The auditors are working towards the same goals as your agency, and are helping to improve the way that government conducts business.

"On behalf of the audit community, I assure you we are here to help," says Nick Marinos, an auditor by trade who serves as the Director of the Information Technology and Cybersecurity Team at the U.S. Government Accountability Office. "I think that the best audit experiences I have had on the other side of the table end up being when folks are transparent, open, honest, pushback on us in a healthy way, and ask the questions right at the start when we have our entrance meetings to lay out the plans."

The SailPoint Identity Platform allows agencies to Visualize, Control, and stay Compliant through the implementation of Identity Governance controls. When agencies have implemented lifecycle automation with the SailPoint platform they gain a complete picture of when users and accounts are created, when attributes about an identity change, and the access they have – whether on premise, SaaS or cloud infrastructure. Access is granted and provisioned only when a serious of approvals have been made and policies have been evaluated. Access Certifications/ Attestations are a natural part of the SailPoint process that allows agencies to perform scheduled or adhoc reviews of access in business-friendly interface. Policies and Certification/ Attestation ensure that access is only assigned to those that have a current need and are suitable for the access. Analytics and Reports are available to document and provided proof to administrators and auditors."

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft

Carahsoft
1493 Sunset Hills Road
Reston, VA 20190

Contact: Maggie Manfredi

(703) 230-7488
Maggie.Manfredi@Carahsoft.com
Carahsoft.com/vendors/SailPoint
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

SailPoint

SailPoint
11120 Four Points Drive
Austin, TX 78726

Contact: Cathy Cromley

(703) 517-4419
Cathy.Cromley@SailPoint.com
Sailpoint.com/identity-for/government
Facebook.com/SailPoint
Linkedin.com/company/SailPoint-Technologies
@SailPoint