splunk>

TECH BRIEF

MANAGING COMPLIANCE IN FEDERAL AGENCIES

For federal government agencies, complying with industry mandates and policies, regulations and governing law is essential to their ability to operate and meet mission objectives. But evolving standards, audit requirements, data collection challenges and mission priorities make it challenging to meet these mandates.

Challenges in Meeting Compliance Mandates

The primary challenge for public sector organizations to meet compliance mandates has been an inability to identify and collect data from across their organization. The challenge is amplified given disparate and heterogeneous technologies strewn across the agencies, a lack of real-time monitoring across systems and the inability to customize and scale to organizational needs. To effectively demonstrate compliance, information sharing and collaboration are critical for organizations to create end-to-end views, so leadership can observe what is happening across the systems, determine any deviations or non-compliance and take necessary action quickly.

The public sector's focus to address an increasingly adversarial threat landscape has also diverted attention away from a true risk management approach that compliance requirements encourage to ensure cyber hygiene. The issue is exacerbated by the lack of a solution that could help organizations meet these broad compliance requirements painlessly and enhance security posture.

Solution Requirements

The most effective way to implement compliance guidance is to deploy a solution that can meet real-time data collection, monitoring and reporting requirements across the infrastructure and organizational processes. At its core this solution should be:

Flexible: The solution must offer a framework that includes all the organization's business process entities and be able to adapt to changes

Scalable: Must account for growth, including the ability to quickly incorporate new activities, users and processes

Central Management and Federated Access: Must provide centralized management through a single interface to ensure consistent, easy management and self-reporting and organization-wide access to stakeholders through role-based access control

Data Source Agnostic: Must quickly interface with any and all data sources required to monitor, assess and meet compliance requirements

Extensible: Must go beyond compliance and seamlessly enable proactive security measures to enhance information protection against any threats—internal and external. Data collected once should be usable across the organization, beyond security and IT, extending return on investment (ROI).

Real-Time Architecture: Must aggregate log data and other relevant information from across the organization in real time to achieve accurate situational awareness and alert on deviations from desired outcomes

Customization: Must be able to query and build inquisition mechanisms and visualizations reflecting stakeholders' needs and a changing environment to effect quick decisions.

Splunk for Compliance Management

Splunk offers a proven, flexible and extensible monitoring and analytics platform to automate any compliance initiative. It removes the tedium of manual and ad-hoc data collection processes, liberating staff from these time-consuming and error-plagued ventures by cutting across silos of operations and automating the data collection, aggregation and correlation. Splunk overcomes the traditional challenges of ingesting and normalizing data by eliminating the need to fit incoming data into predefined schemas. And once data is collected, it can be used across multiple compliance mandates and to solve other IT and security challenges as well – extending your ROI much farther.

The Splunk platform enables agencies with the following capabilities:

- Collect and aggregate data to develop an asset inventory and track usage
- Role-based dashboards and visualizations to communicate risk posture and activity status across organizational levels
- User behaviors and access control monitoring to detect abnormal or unauthorized activities
- Network and data flows monitoring and security investigations support
- Continuously monitor security controls and assess their effectiveness
- Self-reporting and audit capabilities

Government Compliance

Government agencies use Splunk to monitor common compliance requirements that can be uncommonly difficult without the benefit of automated tools.

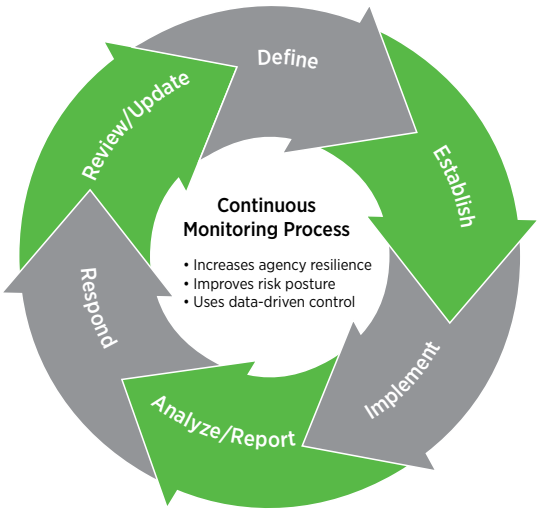
FISMA

The Federal Information Security Modernization Act (FISMA), previously called the Federal Information Security Management Act has evolved significantly since its 2002 inception. FISMA mandates most federal government executive agencies provide information security for the data and systems they and their industry partners manage.

Splunk software can help agencies comply with FISMA, by aligning with security controls as articulated in NIST Special Publication 800-53. It continuously monitors adherence to the various controls put in place by the agencies and provides self-reporting capabilities easing audit burdens. For each supported control, the Splunk platform can provide a detailed view with interactive charts and tables that enable managers to immediately drill down into any event data to further understand causes of deviations.

Risk Management Framework (RMF)

In 2014, NIST issued a revision to its Special Publication 800-37 (Rev 1) to help agencies meet FISMA requirements using a risk-based approach to selecting and implementing security controls most



suitable to the data, networks and information systems they manage. The approach consists of six distinct steps each with a set of security and risk management activities – Categorize, Select, Implement, Assess, Authorize and Monitor.

The Splunk platform can help establish an effective **risk management framework** (RMF) since it requires collecting and correlating data from multiple sources in various formats to Assess (Step 4) and Monitor (Step 6) the effectiveness of an agency's security controls and risk posture.

Many Department of Defense (DoD) organizations are transitioning from the DoD Information Assurance Certification and Accreditation Process (DIACAP) to the Risk Management Framework. Splunk's powerful technology can help these agencies overcome common obstacles and align with **NIST sp800-137** by providing a means to monitor and assess compliance as they make the transition.

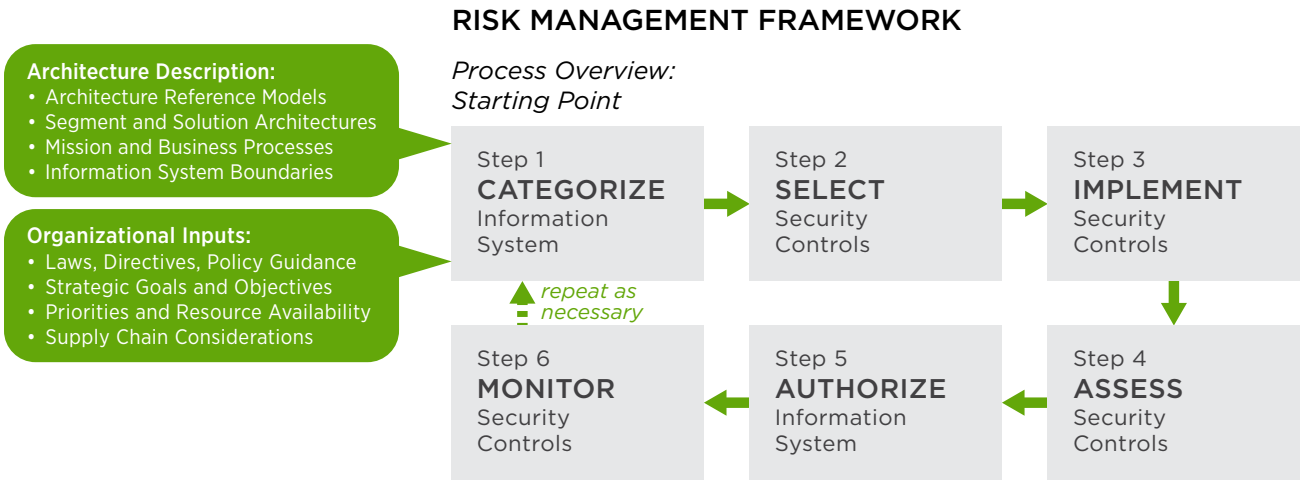
Cybersecurity Framework (CSF)

In response to Presidential Executive Order 13636 from 2013, NIST worked with the private sector to develop the **Framework for Improving Critical Infrastructure Cybersecurity**. Presidential Security Order from May 2017 has also mandated agencies measure themselves against this framework. The goal of the framework is to help an organization reduce risk through a set of activities with desired outcomes in mind. It encourages the organization to first understand its current state and progress towards a target profile defined as part of the maturity framework.

Splunk can help agencies monitor activities and deliver powerful insights to the degree of adherence to profiles and progress towards target profiles.

Beyond NIST Based Compliance Efforts

The same methods and logic can be applied to ensure compliance with additional mandates, including HIPAA (The Health Insurance Portability and Accountability Act), PCI (Payment Card Industry), CJIS (Criminal Justice Information Services) and many others.



Thousands of public and private sector enterprises rely on Splunk products to improve security, increase efficiencies, make data-driven decisions and gain tactical and strategic advantages. **Learn more**.

splunk>

Learn more: **www.splunk.com/asksales**

www.splunk.com