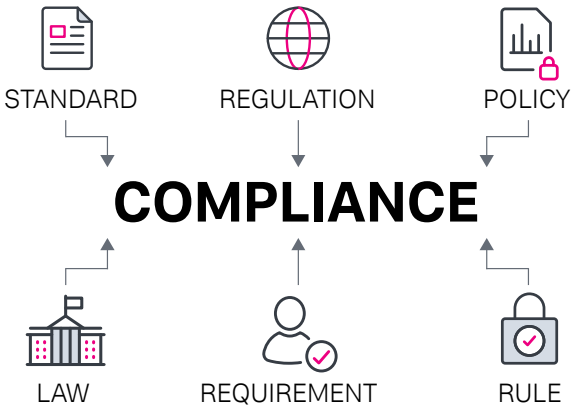
# Compliance Essentials for Splunk (CES)

## Executive Summary

Compliance is a universal problem that affects not only federal agencies, but private sector companies as well. Compliance touches every industry and has become vital to operations in all organizations.
No matter the size of your company or industry, there are cybersecurity laws and regulations that must be followed. These can be mandated at the local, state, federal and international levels. There are a multitude of cybersecurity regulations, including Sarbanes Oxley, Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Cyber Security Maturity Model Certification (CMMC), Risk Management Framework (RMF) and Global Data Protection Act (GDPR), to name a few. Compliance is no longer for just financial services or healthcare, and it's a constantly changing and evolving field.
And these regulations exist for a reason: to protect your business, employees and customers.
Compliance, just like security, is not meant to make business more difficult, but to make it safer — by incorporating security controls into everything, everywhere. We need compliance standards because historically organizations didn't take cybersecurity seriously or meet minimum standards for cyber hygiene. But compliance alone does not create a successful security program.

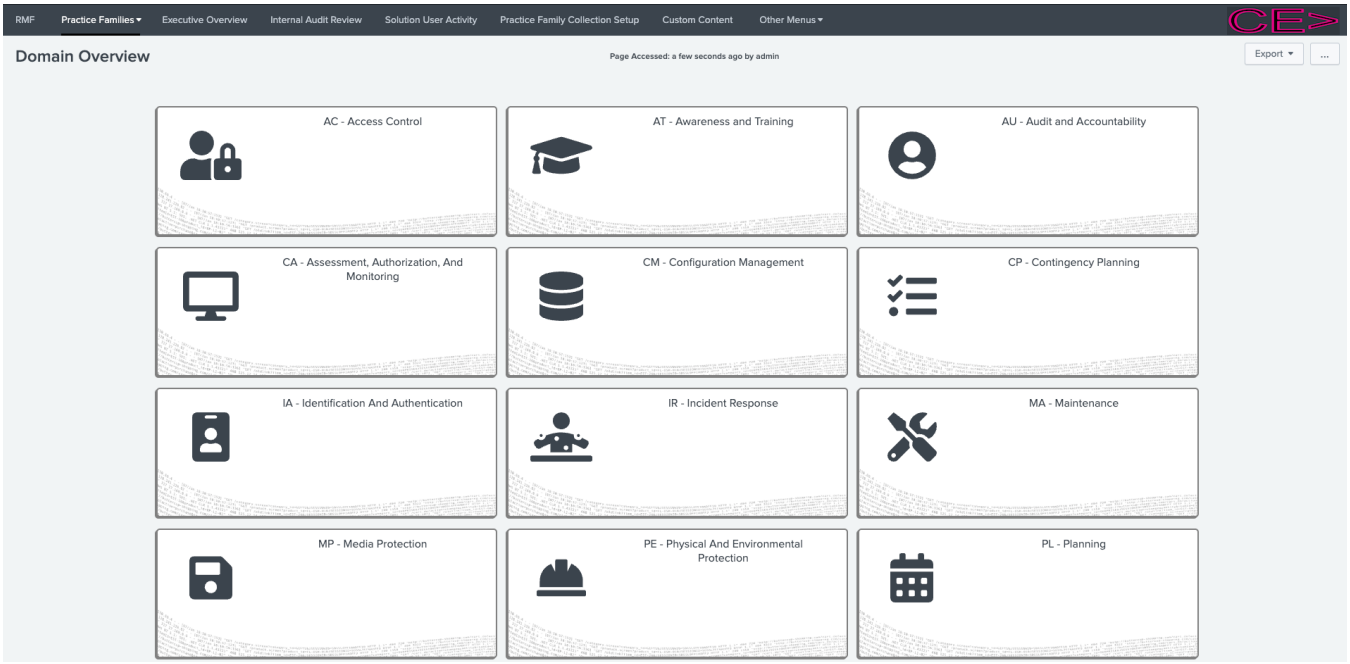



## Customer Perspective

Compliance targets are constantly shifting and organizations operate in silos which can cause critical security events to be missed, while creating gaps in tooling and process breakdown. The organization must be agile in order to respond to threats quickly, so continuous monitoring and compliance have become critical to the success of the business. Organizations must be able to quickly adapt, or they risk introducing additional business risk. Failure to comply with the applicable requirements in a timely manner can also have financial consequences in the form of penalties, lost revenue or lost contracts. Organizations have to take compliance seriously and create comprehensive programs to manage their compliance posture.
Given the volume and scale of data present in modern businesses, a manual spreadsheet with hundreds or thousands of controls that takes weeks or months to complete is no longer sufficient.

## Compliance Essentials for Splunk App

The Compliance Essentials for Splunk (CES) app can assist your organization by continually monitoring your compliance posture across various control frameworks like CMMC, FISMA, RMF, DFARS and even OMB M-21-31. The Splunk CES app gives you a way to quickly and easily visualize your compliance posture in a collection of easy to read dashboards, with searches running in near real time to ensure your organization conforms with the selected control family. This allows you to create repeatable processes that streamline the monitoring of these controls and can provide an auditor with the necessary artifacts to verify the conformance to the many controls. This benefits both the organization in monitoring your compliance status and makes the auditor's job easier.




To do this, the app maps the various control families back to NIST SP 800-53, which has become globally adopted by many organizations and the basis for multiple international standards as well. While this is not a governance risk and compliance (GRC) tool, the app provides a robust set of best practices built on Splunk, the industry's leading log aggregation and correlation platform for security and has the relevant content to scale and meet the demands of the business.

Splunk offers customers a single pane of glass from which the entire enterprise can have visibility across various sensors, geographies, clouds or hosting providers. By using our schema, along with our common information model (CIM) as the backbone for information visualization and data visibility, we can break down these silos and get access to insights from the data in a way that wasn't possible when the activities were performed manually, or even in a semi-automatic fashion using GRC tools.

## Scalable

The CES app is available as a free download from the Splunk App marketplace or Splunkbase and is designed to run in the Splunk Cloud or in a customer premise environment. CES is built on Splunk Enterprise and is complementary to Splunk Enterprise Security (ES), our market-leading security information and event management (SIEM) platform. This provides nearly unlimited scale and the ability to process terabytes and even petabytes of data a day, in near real time, while surfacing tens of thousands of events per second. These capabilities, coupled with assurances like built-in high availability and disaster recovery, mean that Splunk is well-positioned to meet your current and future data needs. CES is meant to provide a fully customizable and tailored approach to meet the needs of any mission in any environment, while allowing the organization to mature and adopt enhanced capabilities as their missions require. This solution is meant to address a multitude of practices across various control families, all from one central location, to lessen the burden of compliance on your organization. By utilizing Splunk's rich security ecosystem with Splunk ES, Splunk SOAR (for security orchestration, automation and response), Business Analytics (BA), and Splunk Intelligence Management, your organization can unlock even more insights.

## Key Benefits

Cybersecurity is critical to both a strong national defense strategy and the intellectual property of your organization. Let's start taking the necessary steps towards a more successful compliance program that is fully integrated into security operations with the Splunk security analytics platform. With Splunk, you can:

- Continuously monitor your environment to achieve and maintain compliance requirements against multiple control families.
- Maintain a single source of truth for compliance needs against the provided control families.
- Accelerate the adoption and achievement of applicable practices.
- Capture operational efficiencies by applying a consistent enterprise data environment.
- Provide the audit team with artifacts in a centralized, easily accessible location.
- Reduce the complexity of audit data by providing traceability and repeatable processes.
- Reduce overall effort with automated data collection.
- Unlock a pathway for more advanced levels of security maturity by integrating security operations and compliance with the Splunk security analytics platform.

Splunk is here to help you meet your organization's compliance needs.Whether you've been using Splunk for years, or you're evaluating Splunk for the first time, you can start turning your data into doing by downloading the CES app today.

Contact us to learn more about how this solution can help your organization be more successful with Splunk.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com



223-89900-PBST Compliance Essentials-DS-SS-104