Data Sheet

Consolidated Compliance Framework

LogRhythm
The Security Intelligence Company

LogRhythm's Consolidated Compliance Framework Benefits

- Greater efficiency in meeting compliance requirements
- Streamlines compliance process by centralizing controls into a single module
- Reduces management overhead and analyst effort by eliminating the need to maintain duplicate content
- Easily accommodates future compliance modules, while retaining proper data segregation

Implementing an effective cybersecurity program is a considerable challenge for organizations. This challenge is made greater by the growing number of compliance standards (e.g., GDPR), that are mandatory for many businesses, depending on geography or industry.

Most compliance frameworks share a common foundation of cybersecurity controls, including privileged access management, monitoring of specific data, and incident response practices. While it is good to see compliance regulations finally catching up to technology and increasingly focusing on cybersecurity, the fact that they share so many foundational controls can cause headaches for those organizations that must adhere to multiple compliance regulations.

If your organization complies with two or more frameworks, you likely find compliance is too time-consuming and too complex as you deal with issues like:

- Encountering duplicate alarms
- Spending time tuning duplicate rule and generating duplicate reports
- Being at the mercy of vendors for release timing on updates

You could, for example, have two rules looking for the exact same scenario as required by different compliance controls, both firing duplicate alarms. Additionally, each rule requires separate administration, separate tuning, and may be on separate update schedules. This all amounts to reduced analyst efficiency.

The Consolidated Compliance Framework

LogRhythm's Consolidated Compliance Framework (CCF) is an integrated component of the LogRhythm NextGen SIEM Platform and aims to reduce the time and resources you spend satisfying compliance regulations. This core compliance module is mapped to dozens of regulations and encompasses the majority of common cybersecurity controls.

This module is built on the "grandfather" frameworks upon which most regulations are based:

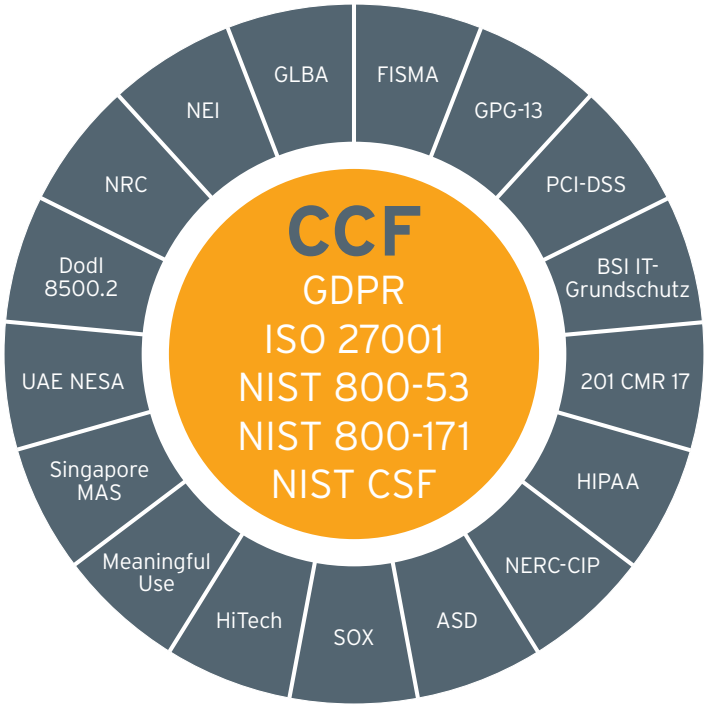
- CIS Critical Security Controls (CSC)
- NIST Cybersecurity Framework, 800-53 and 800-171
- ISO 27001

These seemingly separate frameworks address nearly all current regulations regardless of industry or sector.

The CCF maps standard rules, investigations and reports to common control needs. These controls map well across most compliance frameworks and can thus be shared. This reduces the effort spent on setup and correlating multiple, identical alarms across frameworks.

The CCF module provides segmentation based on what matters – the data. For example, your HIPAA compliance team will only see alarms on their "in scope" data, even if the rule is shared with your PCI compliance team.

For compliance mandates that have specific requirements not covered in the CCF, we provide supplemental, add-on compliance modules designed to meet those specific regulations.



The LogRhythm Consolidated Compliance Framework