Security is paramount for every organization. But it can be challenging to ensure your organization is efficiently and effectively keeping cyber criminals at bay. Use of a security framework, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), is one way to ensure you’re following industry best practices for securing your critical infrastructure and data.

According to Gartner, 30 percent of U.S. organizations are currently using NIST CSF, and the percentage will rise to 50 percent by 2020. Dimensional Research found that 70 percent of organizations use NIST CSF because it aligns with cyber security best practices; 29 percent because it complies with a business partner’s requirements; and 28 percent because complies with a federal contract’s requirements.¹

Many organizations rely on Symantec Control Compliance Suite for NIST CSF risk-prioritized security and compliance as well as continuous assessments and a unified view of their security controls and vulnerabilities. Control Compliance Suite helps you understand exactly where your organization does (and doesn’t) comply with NIST CSF’s requirements—enabling you to minimize security risks and quickly create reports that detail NIST CSF compliance, thus assuring executive management.

Why it’s tough to get a complete picture of your compliance

To demonstrate your organization is in compliance with NIST CSF guidelines, it’s critical that you address these common challenges:

**Challenge #1: Assessing and continuously monitoring NIST CSF security status**

One of the greatest challenges in becoming NIST CSF compliant is demonstrating ongoing compliance—using data to prove that your organization is actually satisfying NIST CSF’s many requirements. You need to collect this type of information for both types of NIST CSF controls: technical and procedural. Many compliance solutions address only one type of control, not both. This limitation creates more manual work because you’ll need to gather the missing data, and it makes it much harder to understand if there are gaps in your security and compliance status.

**Challenge #2: Reconciling multiple mandates or standards**

Many organizations want to develop a security program based on multiple security frameworks, including NIST CSF, NIST 800-53 rev. 4, ISO/IEC 27002, SANS Top 20, and others. But it’s very difficult to reconcile multiple mandates or standards due to the enormous amount of data gathering and reporting that’s involved. Since many of these mandates and standards use the same controls for demonstrating compliance, it’s better to use a compliance solution that maps common controls to any reporting framework without requiring duplicate work.

How Control Compliance Suite helps you attain NIST CSF compliance

A software solution alone can’t make your organization NIST CSF compliant; your processes and properly secured assets ensure compliance. But using a solution such as Symantec Control Compliance Suite to assess security and compliance can make attaining and maintaining compliance much easier and faster.

Control Compliance Suite combines both procedural and technical controls information to help demonstrate NIST CSF security and compliance. These include:

- Aligning with the five key areas of the NIST CSF framework: identify, protect, detect, respond, and recover
- Supporting end-to-end automation of internal and external assessments of procedural, technical, and third-party controls
- Utilizing a common controls framework to map to multiple regulations and standards
- Calculating and aggregating risk scores according to your organization’s unique thresholds
Support the key areas of NIST CSF: Identify, protect, detect, respond, and recover

The ‘core’ of NIST CSF includes five functions that reflect the full lifecycle of a cyber security risk management program: Identify, protect, detect, respond, and recover. NIST CSF breaks these functions down into categories and subcategories that are mapped to various references such as Critical Security Controls, ISO 27001, and NIST SP 800-53.

NIST CSF aligns cyber security activities with business requirements, risk tolerances, and resources. Control Compliance Suite satisfies cyber security objectives using similar alignments that support continuous risk monitoring and reduction. These include:

- **Identify**—NIST CSF encourages organizations to develop an understanding of how to manage cyber security risks. Control Compliance Suite has planning tools, such as Policy Manager and Risk Manager, that aid customers in establishing high-level enterprisewide security objectives, business goals, policies, and programs. Control Compliance Suite specifically enables asset discovery, management, and classification as well as controls-based risk assessment, action planning, and monitoring.

- **Protect**—NIST CSF calls for customers to develop and implement safeguards that limit or contain the impacts of potential cyber security events. Control Compliance Suite can ensure your configuration settings and protection tools are implemented effectively. If events are triggered, Control Compliance Suite can consolidate them and facilitate a review and action planning to address failed checks on a risk-ranked and controls basis.

- **Detect**—NIST CSF recommends customers develop and implement continuous activity monitoring to identify when cyber security events occur. You can better detect risks before they are exploited when you assess security on an automated and scheduled, as well as ad-hoc, basis. Control Compliance Suite tools, such as Standards Manager, Assessment Manager, Risk Manager, and Vulnerability Manager can assess security for technical controls on physical and virtual IT assets, as well as for users through security questionnaires, vendor surveys, and other procedural assessments.

- **Respond**—NIST CSF recommends customers develop and implement appropriate responses when a cyber security event is detected; these include incident response planning, communications, and mitigation. Control Compliance Suite can assess your ability to respond by measuring the readiness of your Incident Response programs and tools. Additionally, Control Compliance Suite has tools—such as Assessment Manager, Policy Manager, and Standards Manager—that enable you to track evidence during incident response efforts. All information collected or imported into Control Compliance Suite can be mapped to the common controls framework, which allows for expedited compliance reporting as well as risk management. The Standards Manager can also carry out scripted technical checks, which facilitate agile IT methods. The ability to directly integrate with third-party ticketing systems enables agile remediation and closes the loop on response capability.

- **Recover**—NIST CSF encourages organizations to develop and implement activities and plans for resilience and restoring capabilities/services, including recovery planning, communications, and improvement. Your ability to quickly recover functionality after cyber security incidents is often dependent on the successful implementation of recovery plans and procedures. Control Compliance Suite can evaluate the readiness of these plans and procedures, and test them via user questionnaires and simulations. The Assessment Manager can carry out these assessments, and report on success, to support continuous improvements. The Risk Manager can monitor these trends and enable action planning to reduce risks associated with recovery efforts.

Realize end-to-end automation for technical and procedural controls

To verify NIST CSF compliance, you will have to collect and maintain an enormous amount of data about the controls in your environment. Control Compliance Suite automates
the assessment of technical controls that require secure configuration settings by using network and asset discovery including third-party systems.

By automating IT infrastructure assessments, you can quickly identify misconfigured assets and prioritize issues for remediation. If a technical asset requires attention that affects your compliance status, such as a laptop requiring a configuration setting change or security update, Control Compliance Suite will list the prioritized issue in a remediation report that you can use to take appropriate action. It even integrates with Symantec ServiceDesk and third-party service desk tools, ensuring your help desk can be automatically notified when an issue requires attention.

**Out-of-the-box support for NIST CSF and 100+ compliance mandates**

Control Compliance Suite helps you pinpoint gaps in your procedural controls with out-of-the-box support for NIST CSF regulations and standards, which it translates into policies and questionnaires. You can use these questionnaires to assess the effectiveness of your procedural security controls, evaluate overall employee security awareness, and support security awareness training.

Control Compliance Suite also offer out-of-the-box support for over 100 mandates and frameworks, including PCI DSS, ISO, HIPAA, and highly referenceable ones such as NIST 800-53 rev.4 and NIST 800-171. The advantage is, if a framework you’re using is modified by the government (or another regulatory organization) and it references a framework that’s already supported by Control Compliance Suite (such as NIST 800-53 rev. 4), you don’t have to start from scratch. Instead, you can use NIST 800-53 rev. 4 as a starting point to create the new framework and modify it as needed.

**Centrally collect and manage evidence with a Common Controls Framework**

Control Compliance Suite can combine evidence from multiple sources—including other solutions such as Symantec Data Loss Prevention or your vulnerability scanning solution—so you gain a complete view of your compliance posture. Evidence collected by Control Compliance Suite is formatted appropriately and mapped to controls that are linked to NIST policies and regulations.

Many organizations must satisfy multiple mandates, such as ISO/IEC 27002 or SANS Top 20, in addition to choosing to comply with NIST CSF. Control Compliance Suite supports a Common Controls Framework for over 100 regulations and frameworks, so you can assess your technical and procedural control status once and utilize that information to report on multiple mandates. No need to repeat work.

**Understand your risk posture with reports and dashboards**

Now you can create reports at a moment’s notice—no more digging through data or massaging it into the appropriate format so executives can easily digest it. Control Compliance Suite gives you a holistic view with customizable, multilevel reports for NIST CSF-based reporting that combine both Control Compliance Suite and third-party data.

Dynamic dashboards show your overall NIST CSF compliance status so you can focus on your most important priorities. If you need a prioritized response plan, use the Control Compliance Suite risk-ranked results to help determine which risks pose the biggest threats and, thus, should be included in your plan. You can also set up roles-based viewing for reports and dashboards, ensuring users view only the information that’s appropriate for them.
Figure 1: All controls are configurable in Control Compliance Suite and each control statement can be mapped to the appropriate NIST CSF mandate.
Figure 2: Procedural assessment questions are mapped to controls in Control Compliance Suite.
Figure 3: Reports and dashboards help you quickly assess your overall compliance.
Next Steps

Take the next step in learning how Control Compliance Suite can support your NIST Cybersecurity Framework compliance program—and give you a unified view of your security controls and vulnerabilities. Learn more.


About Symantec

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.