SOLUTION BRIEF

Achieve NIST Cybersecurity Framework Compliance with Symantec Control Compliance Suite

Symantec™

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

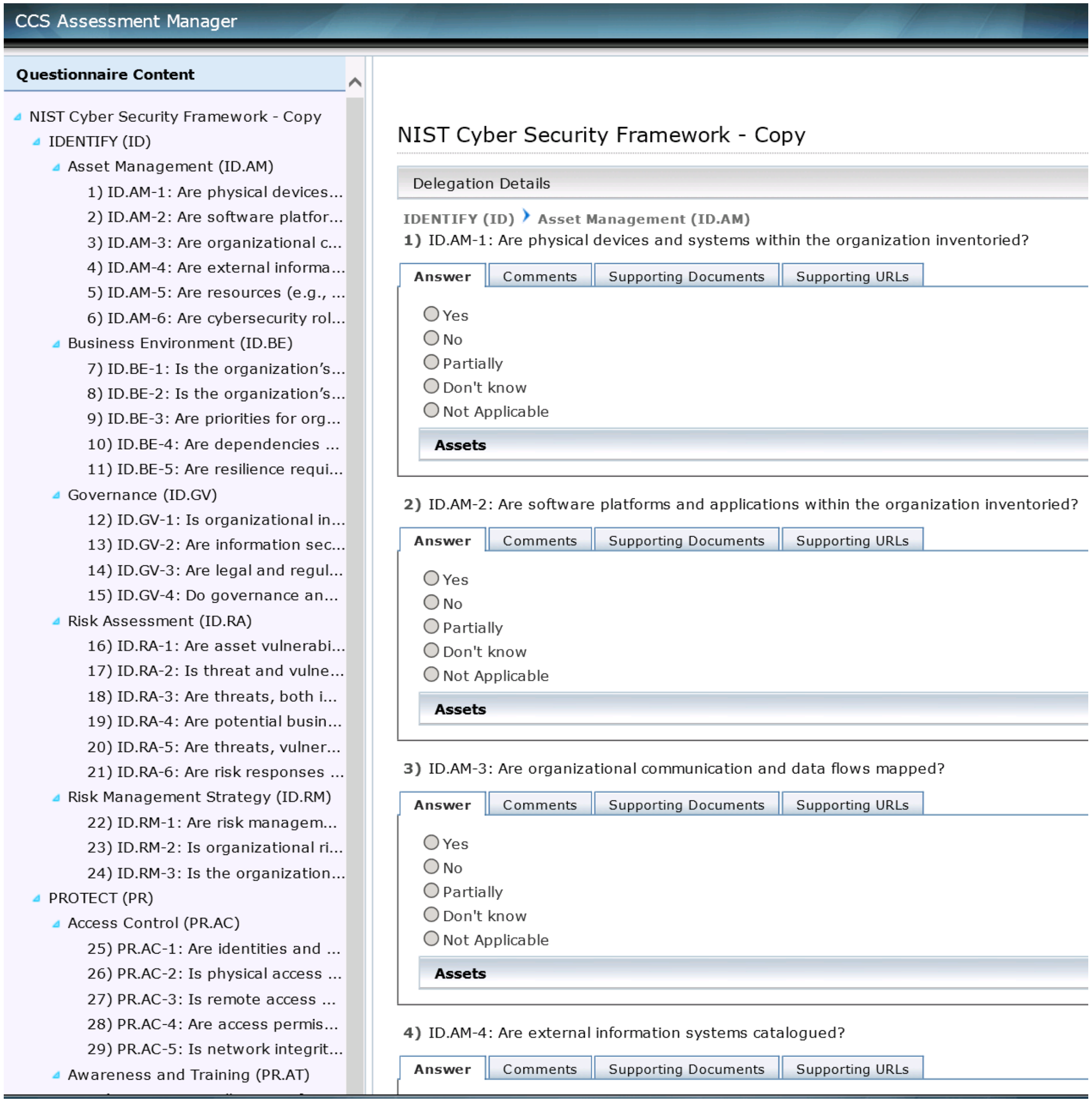
Control Compliance Suite can combine evidence from multiple sources—including other solutions such as Symantec Data Loss Prevention or your vulnerability scanning solution—so you gain a complete view of your compliance posture. Evidence collected by Control Compliance Suite is formatted appropriately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



Questionnaire Content

- NIST Cyber Security Framework - Copy
  - IDENTIFY (ID)
    - Asset Management (ID.AM)
      - 1) ID.AM-1: Are physical devices...
      - 2) ID.AM-2: Are software platfor...
      - 3) ID.AM-3: Are organizational c...
      - 4) ID.AM-4: Are external informa...
      - 5) ID.AM-5: Are resources (e.g., ...
      - 6) ID.AM-6: Are cybersecurity rol...
    - Business Environment (ID.BE)
      - 7) ID.BE-1: Is the organization's...
      - 8) ID.BE-2: Is the organization's...
      - 9) ID.BE-3: Are priorities for org...
      - 10) ID.BE-4: Are dependencies ...
      - 11) ID.BE-5: Are resilience requi...
    - Governance (ID.GV)
      - 12) ID.GV-1: Is organizational in...
      - 13) ID.GV-2: Are information sec...
      - 14) ID.GV-3: Are legal and regul...
      - 15) ID.GV-4: Do governance an...
    - Risk Assessment (ID.RA)
      - 16) ID.RA-1: Are asset vulnerabi...
      - 17) ID.RA-2: Is threat and vulne...
      - 18) ID.RA-3: Are threats, both i...
      - 19) ID.RA-4: Are potential busin...
      - 20) ID.RA-5: Are threats, vulner...
      - 21) ID.RA-6: Are risk responses ...
    - Risk Management Strategy (ID.RM)
      - 22) ID.RM-1: Are risk managem...
      - 23) ID.RM-2: Is organizational ri...
      - 24) ID.RM-3: Is the organization...
  - PROTECT (PR)
    - Access Control (PR.AC)
      - 25) PR.AC-1: Are identities and ...
      - 26) PR.AC-2: Is physical access ...
      - 27) PR.AC-3: Is remote access ...
      - 28) PR.AC-4: Are access permis...
      - 29) PR.AC-5: Is network integrit...
    - Awareness and Training (PR.AT)

NIST Cyber Security Framework - Copy

Delegation Details

IDENTIFY (ID) › **Asset Management (ID.AM)**

1) ID.AM-1: Are physical devices and systems within the organization inventoried?

○ Yes
○ No
○ Partially
○ Don't know
○ Not Applicable

Assets

2) ID.AM-2: Are software platforms and applications within the organization inventoried?

○ Yes
○ No
○ Partially
○ Don't know
○ Not Applicable

Assets

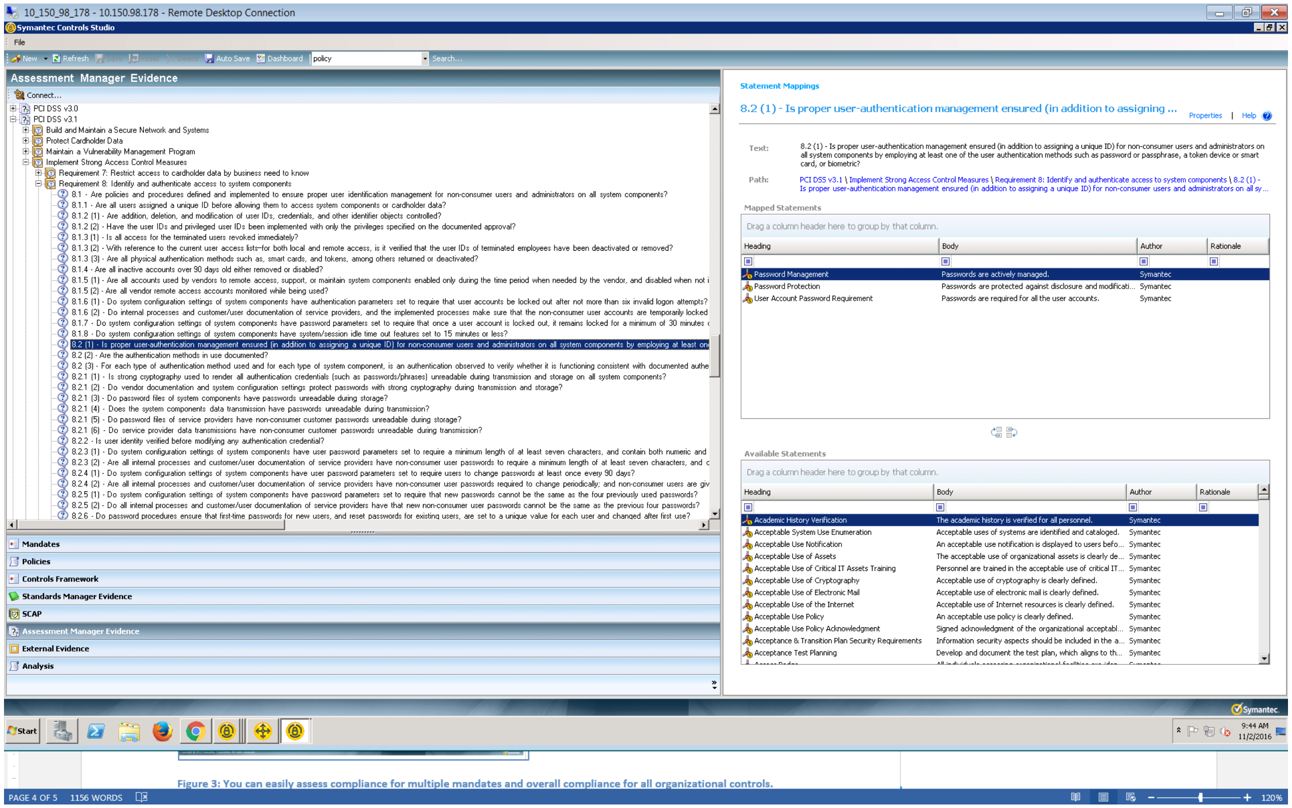
3) ID.AM-3: Are organizational communication and data flows mapped?

○ Yes
○ No
○ Partially
○ Don't know
○ Not Applicable

Assets

4) ID.AM-4: Are external information systems catalogued?

Figure 1: All controls are configurable in Control Compliance Suite and each control statement can be mapped to the appropriate NIST CSF mandate.



- PCI DSS v3.0
- PCI DSS v3.1
  - Build and Maintain a Secure Network and Systems
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
    - Requirement 7: Restrict access to cardholder data by business need to know
    - Requirement 8: Identify and authenticate access to system components
      - 8.1 - Are policies and procedures defined and implemented to ensure proper user identification management for non-consumer users and administrators on all system components?
      - 8.1.1 - Are all users assigned a unique ID before allowing them to access system components or cardholder data?
      - 8.1.2 (1) - Are addition, deletion, and modification of user IDs, credentials, and other identifier objects controlled?
      - 8.1.2 (2) - Have the user IDs and privileged user IDs been implemented with only the privileges specified on the documented approval?
      - 8.1.3 (1) - Is all access for the terminated users revoked immediately?
      - 8.1.3 (2) - With reference to the current user access lists–for both local and remote access, is it verified that the user IDs of terminated employees have been deactivated or removed?
      - 8.1.3 (3) - Are all physical authentication methods such as, smart cards, and tokens, among others returned or deactivated?
      - 8.1.4 - Are all inactive accounts over 90 days old either removed or disabled?
      - 8.1.5 (1) - Are all accounts used by vendors to remote access, support, or maintain system components enabled only during the time period when needed by the vendor, and disabled when not i
      - 8.1.5 (2) - Are all vendor remote access accounts monitored while being used?
      - 8.1.6 (1) - Do system configuration settings of system components have authentication parameters set to require that user accounts be locked out after not more than six invalid logon attempts?
      - 8.1.6 (2) - Do internal processes and customer/user documentation of service providers, and the implemented processes make sure that the non-consumer user accounts are temporarily locked
      - 8.1.7 - Do system configuration settings of system components have password parameters set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes
      - 8.1.8 - Do system configuration settings of system components have system/session idle time out features set to 15 minutes or less?
      - 8.2 (1) - Is proper user-authentication management ensured (in addition to assigning a unique ID) for non-consumer users and administrators on all system components by employing at least one
      - 8.2 (2) - Are the authentication methods in use documented?
      - 8.2 (3) - For each type of authentication method used and for each type of system component, is an authentication observed to verify whether it is functioning consistent with documented authe
      - 8.2.1 (1) - Is strong cryptography used to render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components?
      - 8.2.1 (2) - Do vendor documentation and system configuration settings protect passwords with strong cryptography during transmission and storage?
      - 8.2.1 (3) - Do password files of system components have passwords unreadable during storage?
      - 8.2.1 (4) - Does the system components data transmission have passwords unreadable during transmission?
      - 8.2.1 (5) - Do password files of service providers have non-consumer customer passwords unreadable during storage?
      - 8.2.1 (6) - Do service provider data transmissions have non-consumer customer passwords unreadable during transmission?
      - 8.2.2 - Is user identity verified before modifying any authentication credential?
      - 8.2.3 (1) - Do system configuration settings of system components have user password parameters set to require a minimum length of at least seven characters, and contain both numeric and
      - 8.2.3 (2) - Are all internal processes and customer/user documentation of service providers have non-consumer user passwords to require a minimum length of at least seven characters, and c
      - 8.2.4 (1) - Do system configuration settings of system components have user password parameters set to require users to change passwords at least once every 90 days?
      - 8.2.4 (2) - Are all internal processes and customer/user documentation of service providers have non-consumer user passwords required to change periodically; and non-consumer users are giv
      - 8.2.5 (1) - Do system configuration settings of system components have password parameters set to require that new passwords cannot be the same as the four previously used passwords?
      - 8.2.5 (2) - Do all internal processes and customer/user documentation of service providers have that new non-consumer user passwords cannot be the same as the previous four passwords?
      - 8.2.6 - Do password procedures ensure that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use?

8.2 (1) - Is proper user-authentication management ensured (in addition to assigning ...

Text: 8.2 (1) - Is proper user-authentication management ensured (in addition to assigning a unique ID) for non-consumer users and administrators on all system components by employing at least one of the user authentication methods such as password or passphrase, a token device or smart card, or biometric?

Path: PCI DSS v3.1 \ Implement Strong Access Control Measures \ Requirement 8: Identify and authenticate access to system components \ 8.2 (1) - Is proper user-authentication management ensured (in addition to assigning a unique ID) for non-consumer users and administrators on all sy...

Mapped Statements

Drag a column header here to group by that column.

Heading	Body	Author	Rationale
Password Management	Passwords are actively managed.	Symantec	
Password Protection	Passwords are protected against disclosure and modificati...	Symantec	
User Account Password Requirement	Passwords are required for all the user accounts.	Symantec	

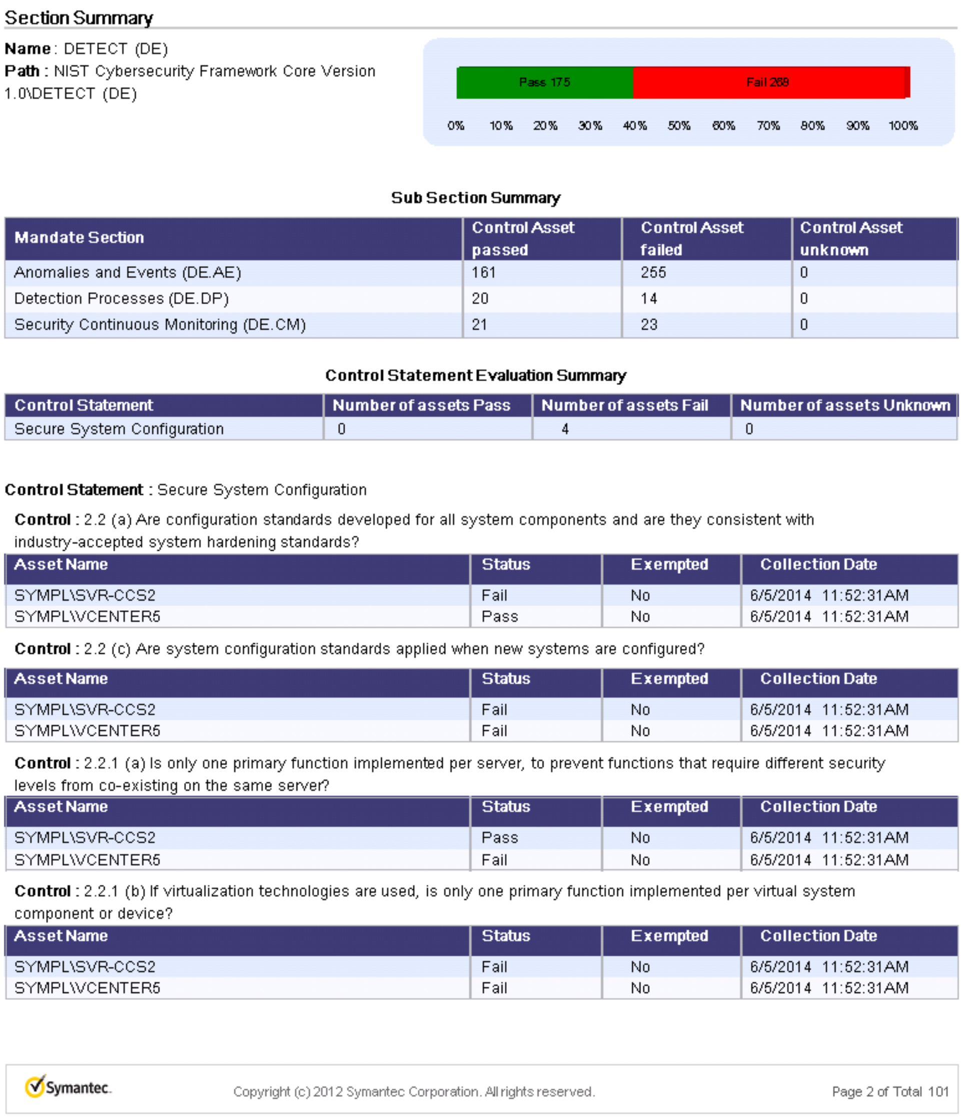
Available Statements

Drag a column header here to group by that column.

Heading	Body	Author	Rationale
Academic History Verification	The academic history is verified for all personnel.	Symantec	
Acceptable System Use Enumeration	Acceptable uses of systems are identified and cataloged.	Symantec	
Acceptable Use Notification	An acceptable use notification is displayed to users befo...	Symantec	
Acceptable Use of Assets	The acceptable use of organizational assets is clearly de...	Symantec	
Acceptable Use of Critical IT Assets Training	Personnel are trained in the acceptable use of critical IT...	Symantec	
Acceptable Use of Cryptography	Acceptable use of cryptography is clearly defined.	Symantec	
Acceptable Use of Electronic Mail	Acceptable use of electronic mail is clearly defined.	Symantec	
Acceptable Use of the Internet	Acceptable use of Internet resources is clearly defined.	Symantec	
Acceptable Use Policy	An acceptable use policy is clearly defined.	Symantec	
Acceptable Use Policy Acknowledgment	Signed acknowledgment of the organizational acceptabl...	Symantec	
Acceptance & Transition Plan Security Requirements	Information security aspects should be included in the a...	Symantec	
Acceptance Test Planning	Develop and document the test plan, which aligns to th...	Symantec	

Figure 3: You can easily assess compliance for multiple mandates and overall compliance for all organizational controls.

Figure 2: Procedural assessment questions are mapped to controls in Control Compliance Suite.



Section Summary

Name : DETECT (DE)
Path : NIST Cybersecurity Framework Core Version 1.0\DETECT (DE)

Sub Section Summary

Mandate Section	Control Asset passed	Control Asset failed	Control Asset unknown
Anomalies and Events (DE.AE)	161	255	0
Detection Processes (DE.DP)	20	14	0
Security Continuous Monitoring (DE.CM)	21	23	0

Control Statement Evaluation Summary

Control Statement	Number of assets Pass	Number of assets Fail	Number of assets Unknown
Secure System Configuration	0	4	0

Control Statement : Secure System Configuration

Control : 2.2 (a) Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards?

Asset Name	Status	Exempted	Collection Date
SYMPL\SVR-CCS2	Fail	No	6/5/2014 11:52:31AM
SYMPL\VCENTER5	Pass	No	6/5/2014 11:52:31AM

Control : 2.2 (c) Are system configuration standards applied when new systems are configured?

Asset Name	Status	Exempted	Collection Date
SYMPL\SVR-CCS2	Fail	No	6/5/2014 11:52:31AM
SYMPL\VCENTER5	Fail	No	6/5/2014 11:52:31AM

Control : 2.2.1 (a) Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server?

Asset Name	Status	Exempted	Collection Date
SYMPL\SVR-CCS2	Pass	No	6/5/2014 11:52:31AM
SYMPL\VCENTER5	Fail	No	6/5/2014 11:52:31AM

Control : 2.2.1 (b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?

Asset Name	Status	Exempted	Collection Date
SYMPL\SVR-CCS2	Fail	No	6/5/2014 11:52:31AM
SYMPL\VCENTER5	Fail	No	6/5/2014 11:52:31AM

Copyright (c) 2012 Symantec Corporation. All rights reserved.

Page 2 of Total 101

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.

[1] *"The Future of the NIST Cybersecurity Framework," April 25, 2016.*

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.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com