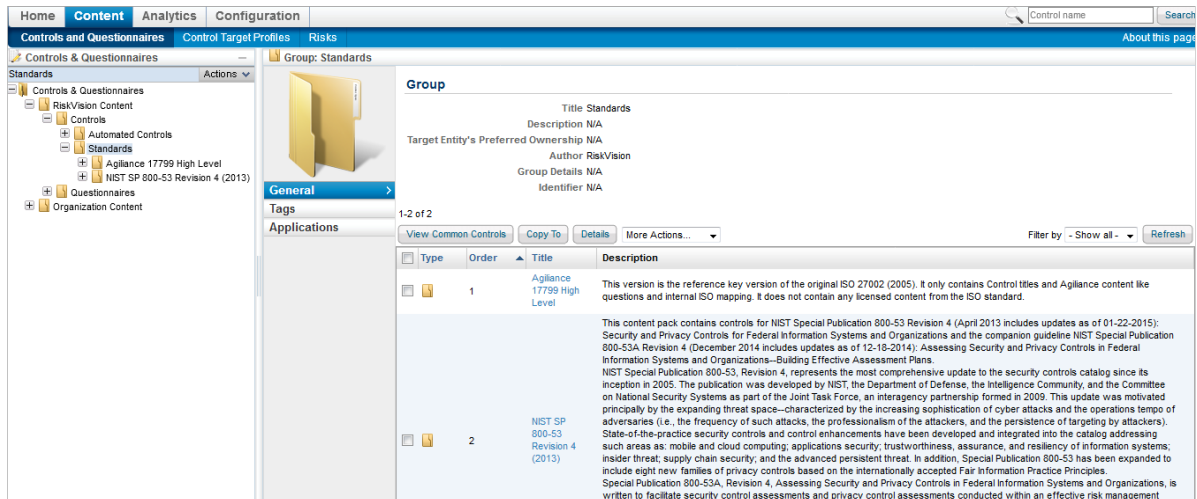


Common Control Framework

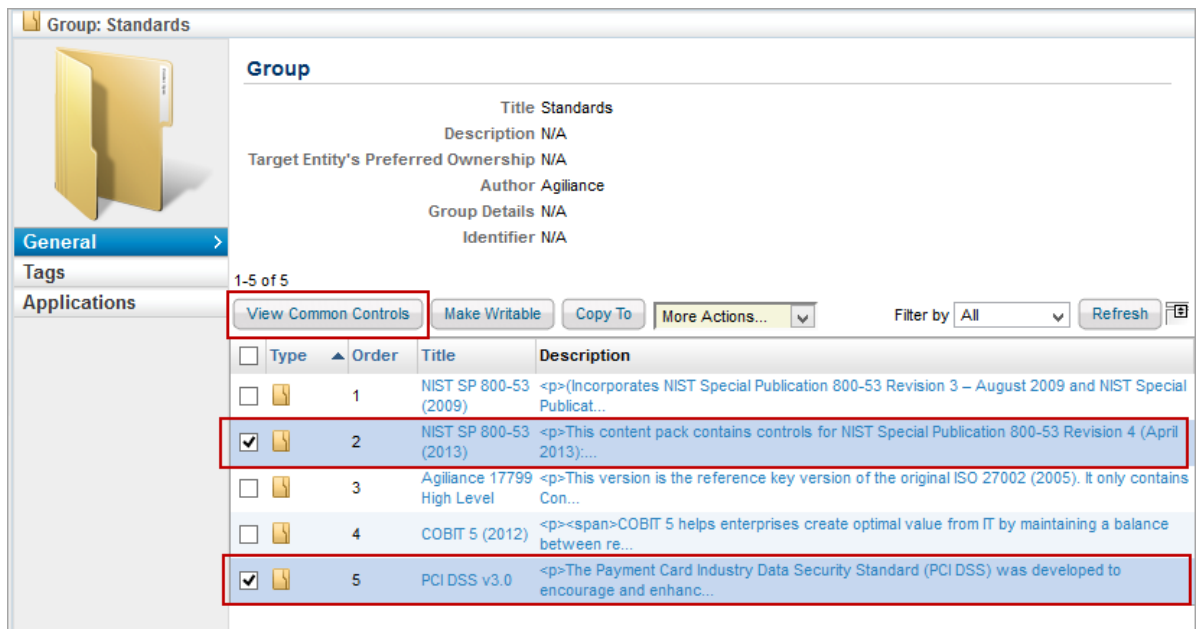
To compare controls from two or more standards:

1. Go to **Content > Controls and Questionnaires**.
2. Expand the **Controls and Questionnaires** tree and go to **Controls and Questionnaires > Content > Controls > Standards**. A grid view of the available standards appears in the right pane.



A grid view of the available standards.

3. Select two standards, then click **View Common Controls** to open the **Common Control Report**.



Agilience Common Control Report

https://10.100.1.51/spc/policy/AgilCommonControlReport.jsp?policysetId=HB0eHzUwNURdDTovxTuXm9aPfw5MleRiLZ25X12345ejKatHuZsqm-123457XQ&comp:

Common Controls Report

Printable Version Export to Excel overlap 49%

1-50 of 1422 Show 50 rows Page 1 2 3 13 ... 29 Go to 1 Go Filter by - Show all - Refresh

| Control | Sub Control | NIST SP 800-53 (2013) | PCI DSS v3.0 |
|--|-------------|-----------------------|--------------|
| 1 NIST SP 800-53 (2013)/AC - Access Control/AC-1 ACCESS CONTROL POLICY AND PROCEDURES | AC-1.1 | ✓ | ✓ |
| 2 NIST SP 800-53 (2013)/AC - Access Control/AC-1 ACCESS CONTROL POLICY AND PROCEDURES | AC-1.2 | ✓ | ✓ |
| 3 NIST SP 800-53 (2013)/AC - Access Control/AC-10 CONCURRENT SESSION CONTROL | AC-10.1 | ✓ | |
| 4 NIST SP 800-53 (2013)/AC - Access Control/AC-11 SESSION LOCK | AC-11.1 | ✓ | ✓ |
| 5 NIST SP 800-53 (2013)/AC - Access Control/AC-11 SESSION LOCK | AC-11.E1 | ✓ | ✓ |
| 6 NIST SP 800-53 (2013)/AC - Access Control/AC-12 SESSION TERMINATION | AC-12.1 | ✓ | ✓ |
| 7 NIST SP 800-53 (2013)/AC - Access Control/AC-12 SESSION TERMINATION | AC-12.E1 | ✓ | ✓ |
| 8 NIST SP 800-53 (2013)/AC - Access Control/AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | AC-14.1 | ✓ | |
| 9 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.1 | ✓ | ✓ |
| 10 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E1 | ✓ | ✓ |
| 11 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E10 | ✓ | ✓ |
| 12 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E2 | ✓ | ✓ |
| 13 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E3 | ✓ | ✓ |
| 14 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E4 | ✓ | ✓ |
| 15 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E5 | ✓ | ✓ |
| 16 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E6 | ✓ | ✓ |
| 17 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E7 | ✓ | ✓ |
| 18 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E8 | ✓ | ✓ |
| 19 NIST SP 800-53 (2013)/AC - Access Control/AC-16 SECURITY ATTRIBUTES | AC-16.E9 | ✓ | ✓ |

The Common Control Report.


The Common Control Report shows a visual comparison of the sub-controls common to the selected standards. For example, "CSC-5.1 Automated tools to continuously monitor" has sub-controls in common with both NIST SP 800-53 (2013) and SANS 20 Critical Security Controls V5.0.

4. **Optional:** Click on a check mark in the standard column to see details of the common sub-controls.
5. **Optional:** Click on a sub-control to display a pop-up with information related to the sub-control.

Agilience RiskVision

https://10.100.1.51/spc/detail.jsp?id=HB0eHzE5QjnFbX77XUIW4eCwEQj6WlhZfciZ-BLd8w0ZvbyOUC123453g

Subcontrol: CSC-2.3 Scanning for unauthorized software



Title CSC-2.3 Scanning for unauthorized software

Description Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components).

Parent CSC-2 Inventory of Authorized and Unauthorized Software

Control

Identifier SANS-20-CSC-5.0-2.3

Attributes

| | | |
|--------------------------|--|---|
| Reference Numbers | NIST-800-53-13-CM-1.1,NIST-800-53-13-CM-2.1,NIST-800-53-13-CM-2.E2,NIST-800-53-13-CM-3.1,NIST-800-53-13-CM-5.1,NIST-800-53-13-CM-5.E2,NIST-800-53-13-CM-7.1,NIST-800-53-13-CM-7.E1,NIST-800-53-13-CM-7.E2,NIST-800-53-13-CM-8.1,NIST-800-53-13-CM-8.E1,NIST-800-53-13-CM-8.E2,NIST-800-53-13-CM-8.E3,NIST-800-53-13-CM-8.E4,NIST-800-53-13-CM-8.E6,NIST-800-53-13-CM-9.1,NIST-800-53-13-PM-6.1,NIST-800-53-13-SA-6.1,NIST-800-53-13-SA-7.1,SANS-20-CSC-4.1-2.3,SANS-20-CSC-5.0-2.3 | Weight 1.0 |
| Key No | | Version 1.0 |
| Control | | Author Agilience |
| Status Final | | Created 2014-08-27 10:31:28 |
| | | Last updated 2015-05-26 15:59:52 |

General >

Question

Dependency

Classification

Remediation

References

Tags

Documents

Risks

Target Profiles


Assignment

If the sub-control identifier of the first sub-control is used as a reference number in the second sub-control or vice versa, then those two sub-controls are common controls.

Agilience RiskVision

https://10.100.1.51/spc/detail.jsp?id=HB0eHzE5QjkZH112345R0zMa3KoAMHr6Gz4qNRLGqZrC0XWsmk64INjsBg

Subcontrol: CM-8.1



General >

- Question
- Dependency
- Classification
- Remediation
- References
- Tags
- Documents
- Risks
- Target Profiles
- Assignment

Title CM-8.1

Description Control: The organization:

- Develops and documents an inventory of information system components that:
 - Accurately reflects the current information system;
 - Includes all components within the authorization boundary of the information system;
 - Is at the level of granularity deemed necessary for tracking and reporting; and
 - Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
- Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

Related controls: CM-2, CM-6, PM-5.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation: P1: LOW CM-8; MOD CM-8 (1) (3) (5); HIGH CM-8 (1) (2) (3) (4) (5)

Parent Control CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Identifier [NIST-800-53-13-CM-8.1](#)


Attributes

| | | | |
|-------------------|---|--------------|---------------------|
| Reference Numbers | ISO-7.1.1,ISO-7.1.2,NIST-800-53-13-CM-8.1 | Weight | 1.0 |
| Key Control No | | Version | 1.0 |
| Status | Final | Author | Agilience |
| | | Created | 2013-05-13 10:49:15 |
| | | Last updated | 2015-04-20 15:11:49 |

Agilience RiskVision

https://10.100.1.51/spc/detail.jsp?id=HB0eHzE5QjnFlX77XUIW4eCwEQi6WihZfCIZ-BLd8w0ZvbyOUC123453g

Subcontrol: CSC-2.3 Scanning for unauthorized software



General >

- Question
- Dependency
- Classification
- Remediation
- References
- Tags
- Documents
- Risks
- Target Profiles
- Assignment

Title CSC-2.3 Scanning for unauthorized software

Description Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLL's and other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components).

Parent Control CSC-2 Inventory of Authorized and Unauthorized Software

Identifier SANS-20-CSC-5.0-2.3

Attributes

| | | | |
|-------------------|--|--------------|---------------------|
| Reference Numbers | NIST-800-53-13-CM-1.1,NIST-800-53-13-CM-2.1,NIST-800-53-13-CM-2.E2,NIST-800-53-13-CM-3.1,NIST-800-53-13-CM-5.1,NIST-800-53-13-CM-5.E2,NIST-800-53-13-CM-7.1,NIST-800-53-13-CM-7.E1,NIST-800-53-13-CM-7.E2, NIST-800-53-13-CM-8.1 ,NIST-800-53-13-CM-8.E1,NIST-800-53-13-CM-8.E2,NIST-800-53-13-CM-8.E3,NIST-800-53-13-CM-8.E4,NIST-800-53-13-CM-8.E6,NIST-800-53-13-CM-9.1,NIST-800-53-13-PM-6.1,NIST-800-53-13-SA-6.1,NIST-800-53-13-SA-7.1,SANS-20-CSC-4.1-2.3,SANS-20-CSC-5.0-2.3 | Weight | 1.0 |
| Key No | | Version | 1.0 |
| Control | | Author | Agilience |
| Status | Final | Created | 2014-08-27 10:31:28 |
| | | Last updated | 2015-05-26 15:59:52 |

You can now compare the degree of overlap between the controls and sub-controls of the various frameworks and regulations that you need to comply with. You can also see the controls and sub-controls

from which answers can be copied.

Example 1

EXAMPLE

Organization ABC is completing the following assessment:

| | |
|-----------------|---|
| Program Name | Compliance with Access Control |
| Entity | ABC Office |
| Security Owner | John J |
| Controls in use | <p>NIST SP 800-53 (2013)</p> <ul style="list-style-type: none">• AC-1 ACCESS CONTROL POLICY AND PROCEDURES• AC-11 SESSION LOCK• AC-12 SESSION TERMINATION |

Mike, the entity owner, answers the questions from the above control. John, the security owner, approves the responses and signs off on the assessment. The compliance scores are calculated and the risk is determined.

Home Entities **Assessments** Content Analytics Configuration

Assessments Programs Notifications and Alerts Data Feeds About this page

Programs > Program: Compliance with Access Control Back

Program: Compliance with Access Control Edit

Assessments Summary Changes Documents Comments Findings Charts Applications

Assessments

1-1 of 1

New Entity Assessment New Entity Collection Assessment Remove More Actions...

Hide Non Applicable Assessment Filter by - Show all - Refresh

| <input type="checkbox"/> | Name | Type | Status | Owner | Compliance | Risk | Progress |
|--------------------------|------------|----------|--------|--------|--|--|---|
| <input type="checkbox"/> | ABC Office | Location | Closed | Mike L | <div style="width: 47%;"><div style="width: 47%;"></div></div> 47% | <div style="width: 100%;"><div style="width: 100%;"></div></div> Low | <div style="width: 100%;"><div style="width: 100%;"></div></div> 100% |

The completed assessment.

Example 2

EXAMPLE

You want to create a new program with the following details:

| | |
|----------------|--------------------------|
| Program Name | Access Control practices |
| Entity | ABC Office |
| Entity Owner | Mike L |
| Security Owner | John J |

When creating the program, click **New Program** wizard > **Options** tab. Click **Automatically answer unanswered controls using results from related controls.**

New Program [Close]

1. Basic Details

2. Content

3. Workflow

4. Recurrence

5. Options

6. Review

Step 5: Additional program Options * = required

Configure the program options

Controls

Automatically Answer Controls

- Automatically answer unanswered controls using results from related controls.
 - Apply compliance score from the related controls
 - Apply answers from the related controls when controls have exactly the same set of choices
- Automatically fail controls when vulnerabilities, mapped to the controls, are reported in the entity.
- Automatically pass controls when vulnerabilities, mapped to the controls, are not present or closed in the entity.
- Automatically update controls when data feeds, mapped to the controls, are reported in the entity.

Key Controls

- Key Controls Only

Controls with Preferred Ownerships

- Do not assess controls with preferred ownership configured when the entities being assessed have no owners that correspond to the preferred owners associated with the control.

Control pass threshold

N/A ▾

Entities

Max Entities

Cancel < Back Next >

This will ensure that if the questionnaire in the current program is not answered, the unanswered controls will use results from related controls that were answered in a different assessment. This is where the Common Controls Framework comes into use. If the controls overlap, then the responses used to answer controls in one assessment will be automatically re-used to answer controls in a different assessment.

- **Apply compliance score from the related controls:** Responses from a related control will be used to calculate the compliance scores.
- **Apply answers from the related controls when controls have exactly the same set of choices** The framework will first validate if the same set of answer choices are used in the related controls. If they are, then they will be used as responses to the questionnaire.

Now, when an assessment using the control "Access Control practices" moves through the workflow, if it does not have responses to all the controls, responses from "Compliance with Access Control program will be used (since the controls are common and overlapping), to populate the compliance scores.

Home Entities **Assessments** Content Analytics Configuration

Assessments Programs Notifications and Alerts Data Feeds About this page

Programs > Program: Access Control practices Back

Program: Access Control practices Edit

Assessments Summary Changes Documents Comments Findings Charts Applications

Assessments

1-1 of 1

New Entity Assessment New Entity Collection Assessment Remove More Actions...

Hide Non Applicable Assessment Filter by - Show all - Refresh

| <input type="checkbox"/> | Name | Type | Status | Owner | Compliance | Risk | Progress |
|--------------------------|------------|----------|--------|--------|--|---|--|
| <input type="checkbox"/> | ABC Office | Location | Closed | Mike L | <div style="width: 27%; background-color: red;"></div> 27% | <div style="width: 100%; background-color: green;"></div> Low | <div style="width: 100%; background-color: green;"></div> 100% |

Apply answers from the related controls when controls work only when the controls have the same question text and the same set of choices. Common Control Framework works only with the combination of same question text and the same set of choices.