

Common Control Framework

The RiskVision solution provides a common control framework out of the box, allowing you to test once and comply with many different standards. Using the Common Control Framework, one assessment rather than many will suffice to certify against any number of regulations. The Common Control Framework supports:

- Mapping of controls from 17799/27001, CoBIT, CoSo, NIST, FFIEC, and GAISP, among others, as well as custom-built controls to one common set of controls based on the ISO standard.
- Utilizing the relationship between the common controls based on the ISO standard and the corresponding regulation-specific controls to share control results for mapped controls, reducing the resources required to comply with, and track compliance with multiple regulations.

The Common Control Framework simplifies the process because controls only need to be tested once, and not once for each framework. This will increase operational efficiency and reduce expenses.

The Common Controls report lets you see a visual comparison of the controls employed in two or more standards.

To compare controls from two or more standards:

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

The screenshot shows the RiskVision interface with the 'Standards' section selected. The left pane shows a tree view with 'Standards' expanded under 'Controls and Questionnaires'. The right pane shows a grid view of standards with columns for Type, Order, Title, and Description. Two standards are visible: 'Agilience 17799 High Level' and 'NIST SP 800-53 Revision 4 (2013)'. The 'View Common Controls' button is highlighted.

Type	Order	Title	Description
Agilience	1	17799 High Level	This version is the reference key version of the original ISO 27002 (2005). It only contains Control titles and Agilience content like questions and internal ISO mapping. It does not contain any licensed content from the ISO standard.
NIST SP 800-53	2	Revision 4 (2013)	This content pack contains controls for NIST Special Publication 800-53 Revision 4 (April 2013 includes updates as of 01-22-2015); Security and Privacy Controls for Federal Information Systems and Organizations and the companion guideline NIST Special Publication 800-53A Revision 4 (December 2014 includes updates as of 12-18-2014); Assessing Security and Privacy Controls in Federal Information Systems and Organizations—Building Effective Assessment Plans. NIST Special Publication 800-53, Revision 4, represents the most comprehensive update to the security controls catalog since its inception in 2005. The publication was developed by NIST, the Department of Defense, the Intelligence Community, and the Committee on National Security Systems as part of the Joint Task Force, an interagency partnership formed in 2009. This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat. In addition, Special Publication 800-53 has been expanded to include eight new families of privacy controls based on the internationally accepted Fair Information Practice Principles. Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, is written to facilitate security control assessments and privacy control assessments conducted within an effective risk management

3. Select two standards, and click on **View Common Controls**.

Group: Standards

Group

Title Standards
 Description N/A
 Target Entity's Preferred Ownership N/A
 Author Agilience
 Group Details N/A
 Identifier N/A

1-5 of 5

View Common Controls Filter by

<input type="checkbox"/>	Type	Order	Title	Description
<input type="checkbox"/>		1	NIST SP 800-53 (2009)	<p>(Incorporates NIST Special Publication 800-53 Revision 3 – August 2009 and NIST Special Publicat...
<input checked="" type="checkbox"/>		2	NIST SP 800-53 (2013)	<p>This content pack contains controls for NIST Special Publication 800-53 Revision 4 (April 2013):...
<input type="checkbox"/>		3	Agilience 17799 High Level	<p>This version is the reference key version of the original ISO 27002 (2005). It only contains Con...
<input type="checkbox"/>		4	COBIT 5 (2012)	<p>COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between re...
<input checked="" type="checkbox"/>		5	PCI DSS v3.0	<p>The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhanc...

4. A Common Control Report appears in a pop-up window.

Agilience Common Control Report

https://10.100.1.51/spc/policy/AgICommonControlReport.jsp?policysetId=HB0eHzUwNURDDTovxTuXm9aPfw5MieRiLZ25X12345ejKatHuZsqm-123457XQ&comp...

Common Controls Report overlap 49%

1-50 of 1422 Show rows Page 1 2 3 13 ... 29 Go to

Filter by

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	✓	✓

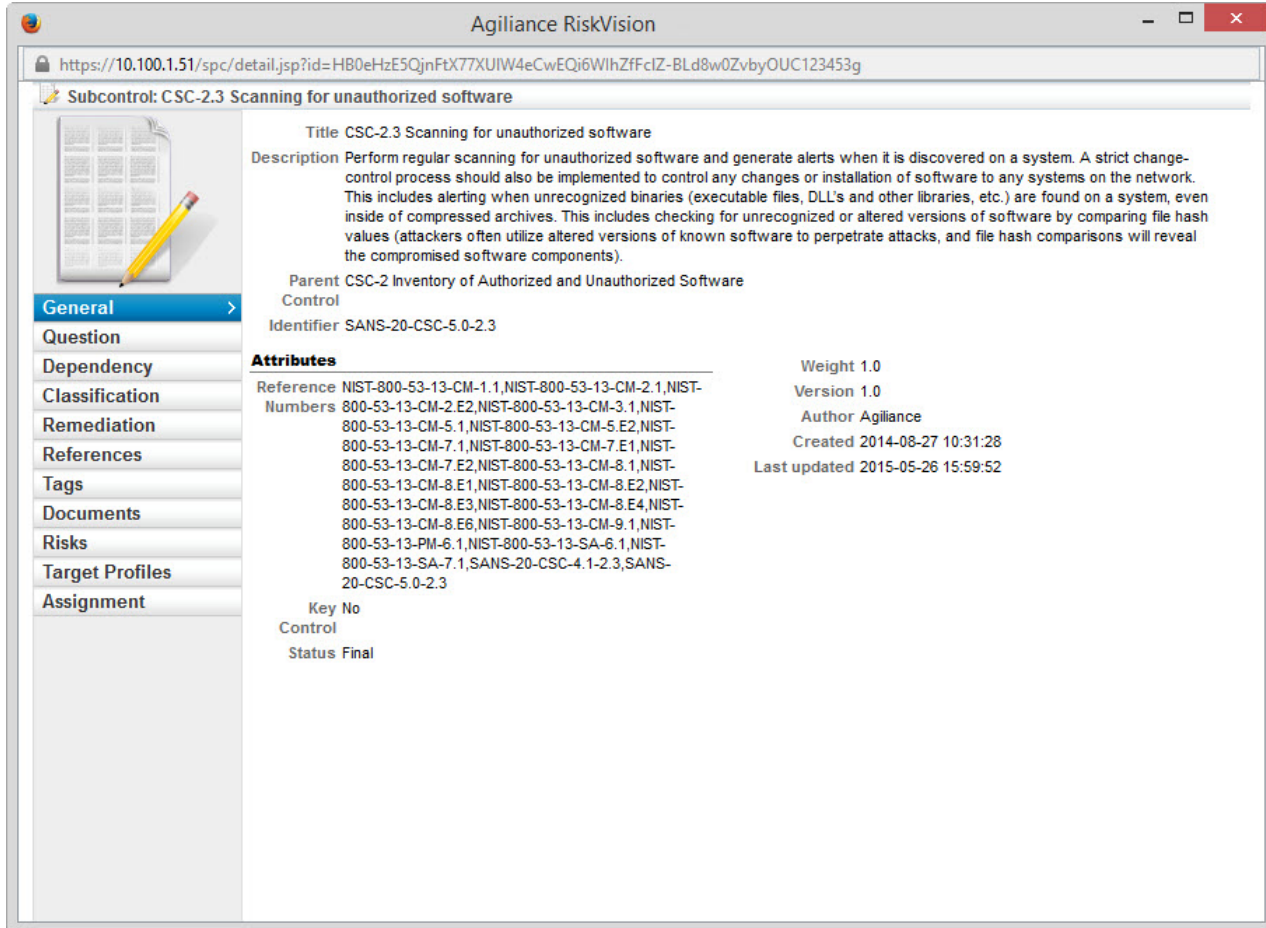
This Common Control Report shows a visual comparison of the sub-controls common to the selected standards.

For example: 'CSC-5.1 Automated tools to continuously monitor' has sub-controls common in both NIST SP 800-53

(2013) and SANS 20 Critical Security Controls V5.0.

Click on tick mark in the standard column to see details of the common sub-controls.

Clicking on the sub-control displays a pop-up with information related to the sub-control.




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:

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

The screenshot shows a web browser window with the URL `https://10.100.1.51/spc/detail.jsp?id=HB0eHzE5QjnFtX77XUIW4eCwEQi6WIhZfclZ-BLd8w0ZvbyOUC123453g`. The page title is "Subcontrol: CSC-2.3 Scanning for unauthorized software".

General (selected in the left sidebar):

- 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
- Weight:** 1.0
- Version:** 1.0
- Author:** Agilience
- Created:** 2014-08-27 10:31:28
- Last updated:** 2015-05-26 15:59:52

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
- Key No Control:**
- Status:** Final

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

To demonstrate the use of the Common Control framework, we will consider an assessment with the following details:

Program Name	Compliance with Access Control
Entity	ABC Office
Entity Owner	Mike L
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

As an entity owner, Mike answers the questions from the above control. As the Security Owner, John approves the responses and sign's off the assessment. As a result, the compliance scores are calculated and the risk is determined.

The screenshot shows a navigation menu with 'Assessments' selected. Below the menu, there are tabs for 'Assessments', 'Summary', 'Changes', 'Documents', 'Comments', 'Findings', 'Charts', and 'Applications'. The 'Assessments' tab is active, displaying a table with one assessment entry:

Name	Type	Status	Owner	Compliance	Risk	Progress
ABC Office	Location	Closed	Mike L	47%	Low	100%

Now we will create a new program with the following details:

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

While creating the program, in the Option's tab of the **New Program** wizard, we will select **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

Next Entity

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.

- Selecting **Apply compliance score from the related controls** will make sure that responses from a related control are used to calculate the compliance scores.
- Selecting **Apply answers from the related controls when controls have exactly the same set of choices** will first validate if the same set of answer choices are used in the related controls and if yes, then they will be used as responses to the questionnaire.

Now, when the assessment using the control 'Access Control practices', moves through the workflow, and 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

Hide Non Applicable Assessment
 Filter by - Show all -

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

The option 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.