Define Control Frameworks

Introduction

The Define Control Frameworks page allows you to create and manage both frameworks and controls. If you are looking for some help getting started we offer several methods to obtain frameworks and controls with minimal effort. One way would be to use the Compliance Forge SCF Extra, this extra is offered free of charge to all SimpleRisk Instances that are registered. Once an instance is registered (Configure → Register & Upgrade) you will then be able to activate and use the Compliance Forge SCF which is a common controls framework containing 875 controls mapped to 148 frameworks. While the exact wording may vary from control to control the overall expectation set should provide you with a great start to getting a handle on governance in your organization. The other main method we offer is through the use of the paid extra Import/Export. Using this you have the ability to not only import frameworks and controls you may already have defined in a CSV format you can also make use of our one-click installs which includes a host of frameworks and controls to work with. Frameworks available for one-click install include:

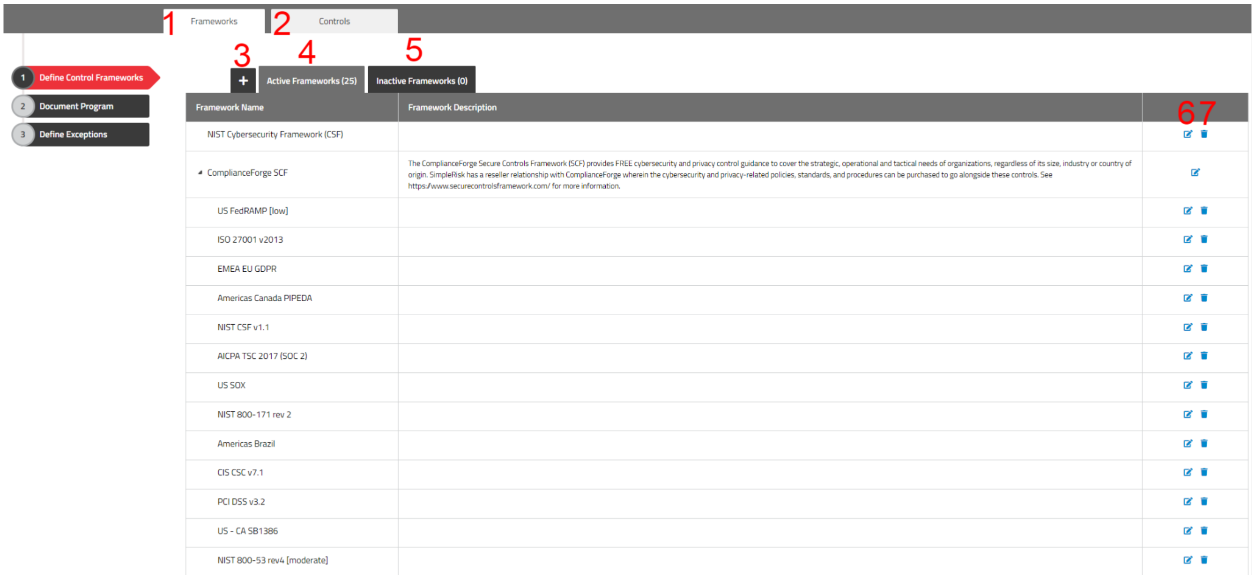
- AICPA 2017 SOC2 Trust Services Criteria (TSC)
- CIS Critical Security Controls v7
- CMMC v1.02 Maturity Level 1
- CMMC v1.02 Maturity Level 2
- CMMC v1.02 Maturity Level 3
- CMMC v1.02 Maturity Level 4
- CMMC v1.02 Maturity Level 5
- FedRAMP Low Baseline Controls
- FedRAMP Moderate Baseline Controls
- FedRAMP High Baseline Controls
- Information Security Regulation Version 2.0
- NIST 800-53
- NIST 800-171
- NIST Cybersecurity Framework (CSF)
- PCI Data Security Standard v3.2.1

With the basic usage of this page covered and ways to populate it now we will dive into the various features and capabilities of this page below.

Page Breakdown

This breakdown is divided into two sections Frameworks and Controls. Frameworks governs the status, usage, and descriptions of frameworks while the controls side

Frameworks



Framework Name	Framework Description	
NIST Cybersecurity Framework (CSF)		✎ 🗑
▴ ComplianceForge SCF	The ComplianceForge Secure Controls Framework (SCF) provides FREE cybersecurity and privacy control guidance to cover the strategic, operational and tactical needs of organizations, regardless of its size, industry or country of origin. SimpleRisk has a reseller relationship with ComplianceForge wherein the cybersecurity and privacy-related policies, standards, and procedures can be purchased to go alongside these controls. See https://www.securecontrolsframework.com/ for more information.	✎
US FedRAMP [low]		✎ 🗑
ISO 27001 v2013		✎ 🗑
EMEA EU GDPR		✎ 🗑
Americas Canada PIPEDA		✎ 🗑
NIST CSF v1.1		✎ 🗑
AICPA TSC 2017 (SOC 2)		✎ 🗑
US SOX		✎ 🗑
NIST 800-171 rev 2		✎ 🗑
Americas Brazil		✎ 🗑
CIS CSC v7.1		✎ 🗑
PCI DSS v3.2		✎ 🗑
US - CA SB1386		✎ 🗑
NIST 800-53 rev4 [moderate]		✎ 🗑

1. Frameworks - This tab allows you to see the Frameworks defined in the system. At this point it will do nothing as we are already looking at the Frameworks section of the Define Frameworks page.
2. Controls - This tab will take us to the controls section where we can define, manage, and delete controls. This section will be covered later in this document.

3. Add (“+”) - This button allows the user to create a new framework. You will be given the opportunity to assign a Name, A description, and any parent association it may have relating to another framework already defined in the system.

4. Active Frameworks - In this tab we display the currently active frameworks. These frameworks will be available for use in the Compliance section and any notifications based on testing that may be currently active will be sent as long as the framework remains active. You may click and drag frameworks from active to inactive or vice versa.

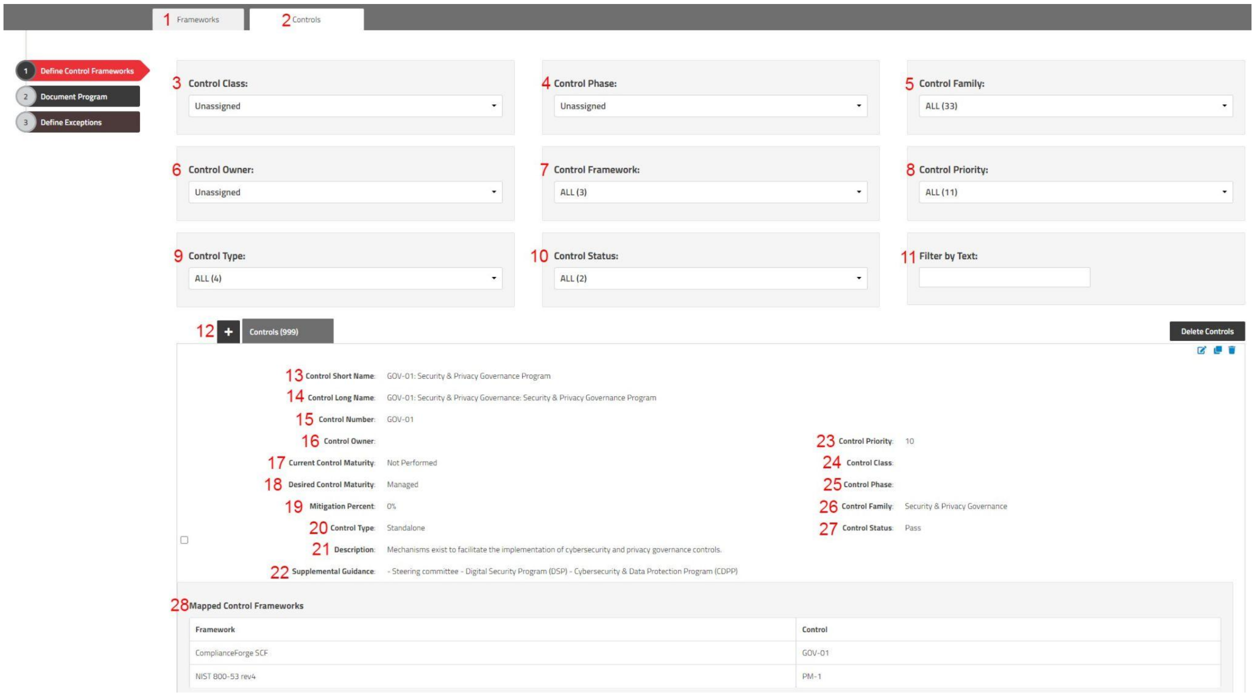
5. Inactive Frameworks - In this tab we display the inactive frameworks. These frameworks and their controls will not show up in any other section of SimpleRisk as long as they remain active. No notifications will be sent on their behalf for any tests they may have already had defined prior to deactivation. Frameworks can be clicked and dragged to the active tab from here.

6. Edit Framework - This button allows you to edit the details of an already defined framework. The controls associated with this framework are not displayed or configurable here that will be

in the Controls tab and will be covered later in this document.

7. Delete Framework - This button allows the user to delete a framework. Deleting a framework does not inherently delete its controls. The mapping for that framework will simply be removed from the control.

Controls



Control Class: Unassigned

Control Phase: Unassigned

Control Family: ALL (33)

Control Owner: Unassigned

Control Framework: ALL (3)

Control Priority: ALL (11)

Control Type: ALL (4)

Control Status: ALL (2)

Filter by Text:

□

Control Short Name: GOV-01: Security & Privacy Governance Program

Control Long Name: GOV-01: Security & Privacy Governance: Security & Privacy Governance Program

Control Number: GOV-01

Control Owner:

Current Control Maturity: Not Performed

Desired Control Maturity: Managed

Mitigation Percent: 0%

Control Type: Standalone

Description: Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.

Supplemental Guidance: - Steering committee - Digital Security Program (DSP) - Cybersecurity & Data Protection Program (CDPP)

Control Priority: 10

Control Class:

Control Phase:

Control Family: Security & Privacy Governance

Control Status: Pass

Mapped Control Frameworks

Framework	Control
ComplianceForge SCF	GOV-01
NIST 800-53 rev4	PM-1

1. Frameworks Tab - This tab will take you back to the frameworks tab allowing you create and manage frameworks.
2. Controls Tab - This tab would take you to the Controls tab allowing you to create and manage controls.
3. Control Class Filter - This filter allows you to make a selection of one or more control classes you would like to view. Once a selection is made only those control classes will be displayed.
4. Control Phase Filter - This filter allows you to make a selection of one or more control phases you would like to view. Once a selection is made only those control phases will be displayed.
5. Control Family Filter - This filter allows you to make a selection of one or more control families you would like to view. Once a selection is made only those control families will be displayed.
6. Control Owner Filter - This filter allows you to make a selection of one or more control owners you would like to view. Once a selection is made only those control owners will be displayed.
7. Control Framework Filter - This filter allows you to make a selection of one or more control frameworks you would like to view. Once a selection is made only those control frameworks will be displayed. Please note that only active frameworks will be displayed.

8. Control Priority Filter - This filter allows you to make a selection of one or more control priority levels you would like to view. Once a selection is made only those control priority levels will be displayed.
9. Control Type Filter - This dropdown allows you to select and filter down the controls displayed by the type. By default options are Standalone, Project, and Enterprise.
10. Control Status Filter - This filter allows you to narrow down results by the current pass/fail status of a given control.
11. Filter By Text - This allows you to search all fields associated with any control.
12. Add Control (“+”) - This will open the menu that allows you to enter the details of a new control. Any information entered is not saved until the save button is clicked.
13. Control Short Name - This field is a place to store the short form name of a control. This will be the name you will see the most often when referencing controls.
14. Control Long Name - This field can store a full length name and is less often display when referencing throughout SimpleRisk.
15. Control Number - Generally a section ID or identifier to determine the location of in depth information for a given control.
16. Control Owner - This field depicts the responsible party for knowledge and execution of a given control.
17. Current Control Maturity - This field allows the organization to save their current control maturity as expressed by the following options for levels of maturity: Not Performed, Performed, Documented, Managed, Reviewed, or Optimizing.
18. Desired Control Maturity - This field allows the organization to save their desired control maturity as expressed by the following options for levels of maturity: Not Performed, Performed, Documented, Managed, Reviewed, or Optimizing.
19. Mitigation Percent - This field allows you to store a percentage that when this control is applied to a mitigation for a risk this percentage will be applied to the inherent risk to get the residual risk score. If this value is not the highest mitigation percentage on a mitigation it will not be used. Only the single highest mitigation percentage is calculated into the residual risk score.
20. Control Type - You have three different types of control in SimpleRisk. Standalone, which have no further strings attached to their use. Project, which are controls used to keep projects on track and within budget. Enterprise, which has the ability to combine information gathered across multiple processes. With Enterprise selected the control is then tracked when an audit test or compliance assessment is failed this state is displayed on any mitigation this control is being used for and the mitigation percent provided by this control will be dropped to 0. if a question is performing a compliance assessment and passes the assessment, and the mapped control has both the “Project” and “Enterprise” control types selected for it, then the Control Validation Mitigation Percent in the Mitigation will be set to half of the Mitigation Percent value for that given control.
21. Description - This field is for the description of the control and its requirements.
22. Supplemental Guidance - This allows users to upload any supporting information related to the control. The file formats supported are dictated by the extensions and file types set in Configure → Settings → File Upload tab.

23. Control Priority - This field allows you to associate a level priority with for a control.
24. Control Class - This field offers the ability to further define and categorize your controls by class. The available values can be updated via the Add & Remove Values page in the Configure menu at the top.
25. Control Phase - This field allows you to store a control phase. The default selections are Physical, Procedural, Technical, Legal & Regulatory. New options can be added via the Add & Remove page found in the Configure menu at the top.
26. Control Family - This field allows you to categorize a control based on family.
27. Control Status - This field is for recording the current pass/fail status of a control. This is the value you will see updated when the Control Type is Enterprise when an assessment compliance test is failed or passed.
28. Mapped Frameworks - This section allows you to click the add "+" button to map the control to an already existing framework. The system allows for users to select multiple frameworks for a single control to map to and lets you label them with a control number to make cataloging controls spanning multiple frameworks much easier.

Summary

The Governance Define Frameworks page allows you to add and manage your Control Frameworks in SimpleRisk. This page should have served to answer all questions related to the Define Frameworks page but if you feel anything has been missed or just seek further clarification please reach out to us at support@simplerisk.com.