



Security Dashboard - Action Plan Recommendation

- [Introduction](#)
- [How does it work?](#)
- [Accessing the Action Plan Recommendation](#)
- [Action Plan Recommendation interface](#)



 **Summary:** This page provides information about the **Action Plan Recommendation** feature.

 This feature is currently in BETA.

Introduction

The **Action Plan Recommendation** is a feature designed to help you automatically build an **Action Plan** to **improve the score of a chosen Health Factor** (Business Criteria). In short, for a given Health Factor, you can configure one of the "remediation targets" listed below and the Action Plan Recommendation will automatically suggest a list of violations to be added to the **Action Plan** for future correction. The correction of the suggested violations will match the desired remediation target when a new snapshot is generated and therefore improve the grade of the chosen Health Factor. Available remediation targets:

- The number of violations you want to fix, OR
- The amount of effort in man/days you would like to "spend" on fixing the violations

- 
- The feature requires a login with the **QUALITY_MANAGER** role.
 - This feature supports Health Factors introduced by the following industry standard extensions:
 - **CISQ**
 - **MIPS Reduction**
 - **OMG-ASCQM**
 - **OWASP**
 - This feature is supported only in AIP versions 8.3.29
 - This feature does not work for old snapshots (the "APR" and "download data as excel file" icons  are disabled)

How does it work?

The Action Plan Recommendation uses an **optimization algorithm** to build an **Action Plan** according to the target you want to achieve. This algorithm functions as follows for each of the available remediation targets:

- You select a **specific number of violations to fix**: the system will search for an Action Plan (i.e. a list of violations) that matches (where possible) the selected number of violations and that maximizes the grade/score of the chosen Health Factor.
- You select a **specific effort**: the system will search for an Action Plan (i.e. a list of violations) that matches with the selected total effort and that maximizes the grade/score of the chosen Health Factor.

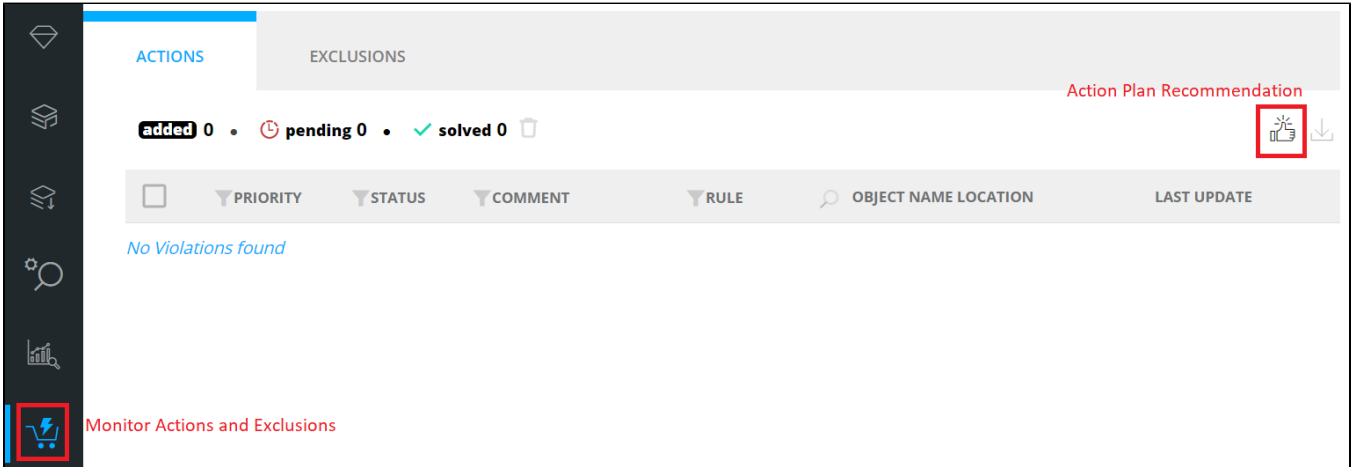
This algorithm attempts to solve a "combinatorial optimization problem". This means that the perfect solution (i.e. Action Plan or list of violations) is unknown, and the algorithm will try to find the very best solution it can by selecting the best result using the three heuristics (grade/score, number of violations and effort). As a result, the algorithm may find a solution (i.e. Action Plan or list of violations) which may differ slightly from your requested remediation target.

Notes:

- As soon you **re-select** or **deselect** a rule in the interface the algorithm will re-compute the action plan recommendation. Depending on the rules you have already excluded, some rules may be added/removed by the algorithm compared to a previous recommendation.
- The effort is calculated for a number of objects and does not depend on the number of objects to fix (especially for cost complexity).
- An effort "unit" is set by a hard coded rule. The value of the effort unit depends on the parent Technical Criterion of the rule.
- By default, all rules that belong to the same Technical Criterion are set with the same effort unit.
- By default, an **initial remediation target** is set when the interface is first opened - this is to **correct one violation** - if you already have violations added to Action Plan, this initial remediation target will be set to **correct one additional violation**.

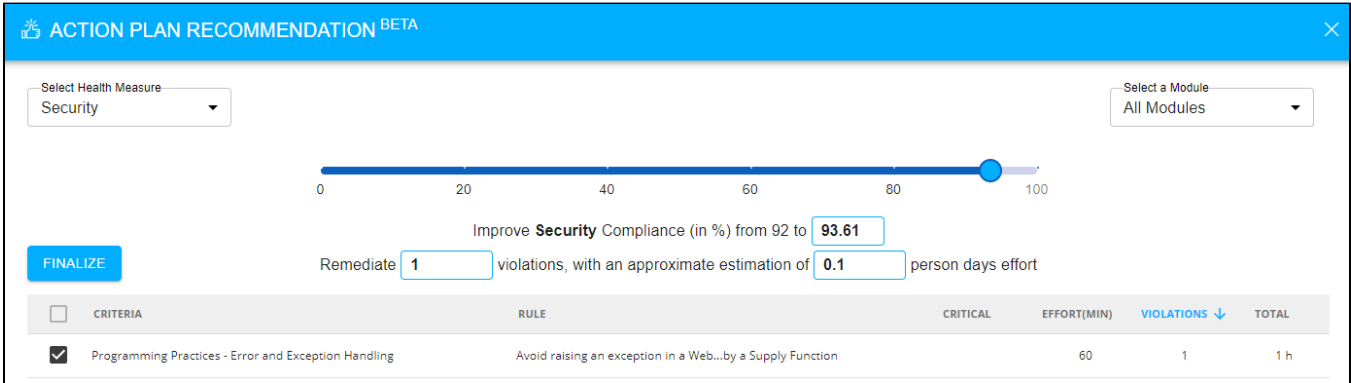
Accessing the Action Plan Recommendation

The Action Plan Recommendation feature can be accessed from the [Action Plan](#) using the icon in the top right corner:



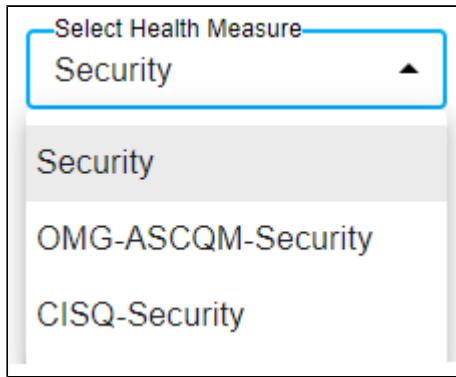
Action Plan Recommendation interface

Click to enlarge



Select Health Measure

This option provides a drop down list of the available Health Factors to target for grade improvement. By default the **Total Quality**



Select Health Measure
Security

Security

OMG-ASCQM-Security

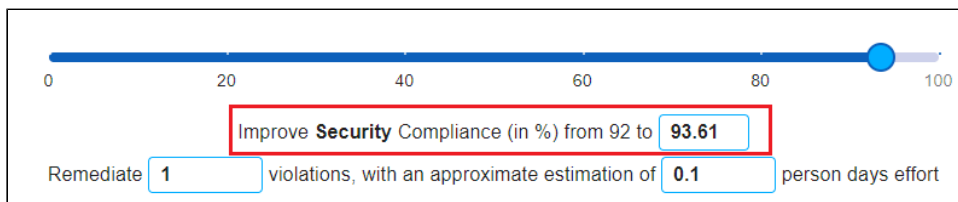
CISQ-Security



- If you have **filterHealthFactor** set to **false**, additional Health Factors will be displayed.
- This feature supports Health Factors introduced by the following industry standard extensions:
 - **CISQ**
 - **MIPS Reduction**
 - **OMG-ASCQM**
 - **OWASP**

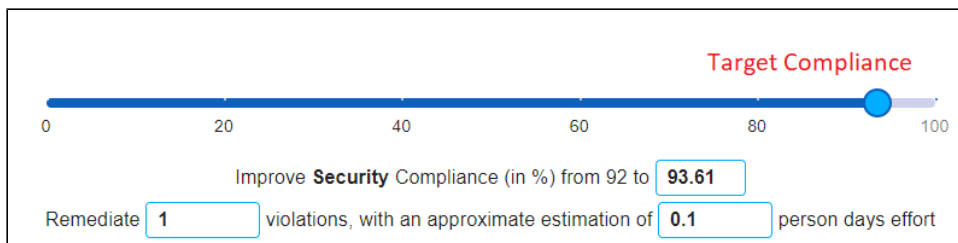
Improve Security Compliance (in %)

This option allows you to Improve **Total Security Compliance (in%)**.



Compliance (in %) slider

The Compliance slider indicates the target Compliance (in %) you would like to achieve for the chosen Health Factor (Compliance

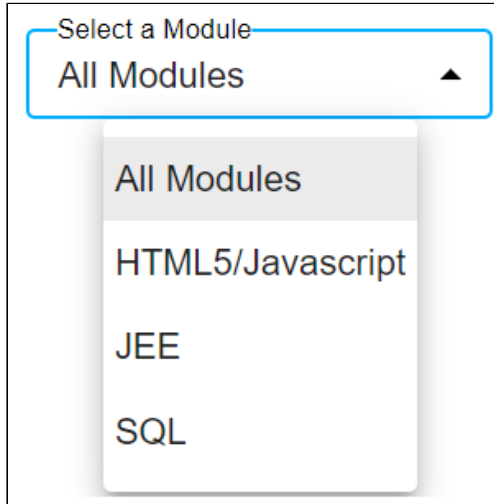


When you select **Compliance (in %)** from the Improve **Total Quality Index** drop-down, **Minimize** (Violations and Effort) o

- You can manually move the slider by clicking the circle and dragging it to a new position - this is a quick method to build an ac
- The Action Plan Recommendation will recalculate the suggested Action Plan each time you move the slider.
- The Compliance (in %) shown in the slider will match the Target Compliance shown in the Compliance manual entry box (see

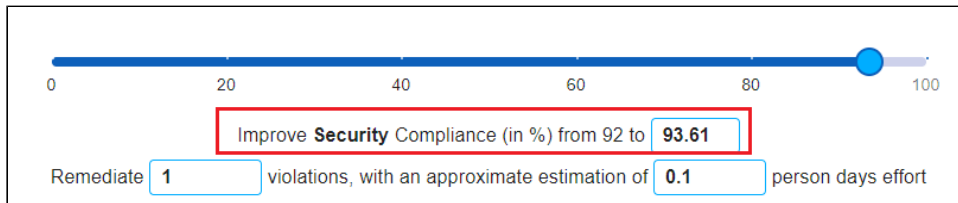
Select a Module

This option provides the drop down list of the available Modules, by default "All Modules" is selected. Users can specify the improv can be selected from the module dropdown.



Compliance manual entry

This option indicates the target Compliance you would like to achieve for the chosen Health Factor (Compliance percentage go fro



- When the Compliance is selected the first time, the box will indicate a target Compliance based on the default initial remediation this initial remediation target will be set to **correct one additional violation**.
- You can manually change the Compliance percentage in the box using the up/down buttons or by manually entering the grad



- The Action Plan Recommendation will recalculate the suggested Action Plan each time you change the value in the box.
- The target Compliance shown in the box will match the target Compliance shown on the **Compliance slider** (see above).

Violation manual entry

This option indicates the number of violations that you want to fix:

A horizontal slider is shown with a blue bar and a blue knob positioned at approximately 93.61%. Below the slider, the text reads: "Improve Security Compliance (in %) from 92 to 93.61". Below this, there is a red-bordered box containing the text "Remediate 1 violations with an approximate estimation of 0.1 person days effort". The number "1" is in a small box with up/down arrows, and "0.1" is in another small box.

- When the Action Plan Recommendation is first opened, the box will indicate a default initial remediation target to correct one target will be set to correct one additional violation.
- You can manually change the number of violations in the box using the up/down buttons or by manually entering the number you want to correct:



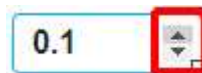
- The Action Plan Recommendation will recalculate the suggested Action Plan each time you change the value in the box.

Effort manual entry

This option indicates the amount of effort in man/days you would like to "spend" on fixing the violations:

A horizontal slider is shown with a blue bar and a blue knob positioned at approximately 93.61%. Below the slider, the text reads: "Improve Security Compliance (in %) from 92 to 93.61". Below this, there is a red-bordered box containing the text "Remediate 1 violations, with an approximate estimation of 0.1 person days effort". The number "1" is in a small box, and "0.1" is in another small box.

- When the Action Plan Recommendation is first opened, the box will indicate a target effort in man/days based on the default i Action Plan, this initial remediation target will be set to correct one additional violation.
- You can manually change the amount of effort in the box using the up/down buttons or by manually entering the number - this like to "spend" on fixing the violations:



- The Action Plan Recommendation will recalculate the suggested Action Plan each time you change the value in the box.

FINALIZE

The FINALIZE button will add all the violations for selected rules into the Action Plan. In the following example, 7 violations have

Click to enlarge

A screenshot of the interface showing a "FINALIZE" button and a table of violations. The table has columns: CRITERIA, RULE, CRITICAL, EFFORT(MIN), VIOLATION, and TOTAL. One row is checked, and a red arrow points to the "1" in the VIOLATION column with the text "One violation added to the APR".

CRITERIA	RULE	CRITICAL	EFFORT(MIN)	VIOLATION	TOTAL
<input checked="" type="checkbox"/> One rule ticked	Architecture - Multi-Layers and Data Access	Avoid having multiple artifacts upd...n the same SQL Table	60	1	1 h
<input type="checkbox"/>	Programming Practices - Error and Exception Handling	Avoid raising an exception in a Web...by a Supply Function	60	1	1 h

Note that the Comment in the Action Plan will be populated automatically and will describe the target remediation, for example:

A screenshot of the "ACTIONS" tab in the Action Plan, showing a table with columns: PRIORITY, STATUS, COMMENT, RULE, OBJECT NAME LOCATION, and LAST UPDATE. Two rows are visible, both with a status of "Added".

PRIORITY	STATUS	COMMENT	RULE	OBJECT NAME LOCATION	LAST UPDATE
High	Added	All Modules - R...ovement from 92 to 93.77	Avoid having multiple artifacts updating data on the same SQL Table		01-08-2021
High	Added	All Modules - R...ovement from 92 to 93.61	Avoid raising an exception in a Web Dynpro Supply Function or in a Method...		01-08-2021

Action Plan Recommendation list

This section lists the rules that the Action Plan Recommendation algorithm thinks are the **best match** for the target remediation. You can select or deselect rules from this list. The **best match** header.

Check boxes

The check boxes enable you to choose whether you want the violations for a specific rule to be added to the Action Plan. If you do not want to fix violations for a specific rule, de-select the associated rule.

In the following example, we do not want to fix the violations of the rule **Avoid using javascript or expression in CSS**.

Click to enlarge

<input type="checkbox"/>	CRITERIA	RULE	CRITICAL	EFFORT(MIN)	VIOLATIONS	TOTAL
<input checked="" type="checkbox"/>	Efficiency - SQL and Data Handling Performance	Use dedicated stored procedures where possible (ASCPEN-PRF-10)	●	120	4	1 d
<input checked="" type="checkbox"/>	Architecture - Reuse	Avoid defining singleton or factory when using Spring	●	180	3	1 d
<input checked="" type="checkbox"/>	Efficiency - SQL and Data Handling Performance	Avoid SQL queries that no index can support	●	120	2	4 h
<input checked="" type="checkbox"/>	Secure Coding - Input Validation	Avoid using javascript or expression in the CSS file	●	60	1	1 h

- When you deselect a rule, the Action Plan Recommendation will recalculate the suggested Action Plan, therefore the algorithm may decide that a different combination of violations will match the chosen remediation target.
- If violations of a particular rule are already present in the Action Plan, the check box will be **unselected and disabled**.

<input type="checkbox"/>	CRITERIA
<input type="checkbox"/>	Efficiency - SQL and Data Handling Performance
<input checked="" type="checkbox"/>	Efficiency - Memory, Network and Disk Space Management
<input type="checkbox"/>	Architecture - Reuse
<input type="checkbox"/>	Efficiency - SQL and Data Handling Performance
<input type="checkbox"/>	Secure Coding - Input Validation

Criteria	The name of the parent Technical Criterion for the violated rule.
Rule	The name of the violated rule .
Critical	Indicates whether the rule is critical or not (a red dot indicates a critical rule).
Effort (min)	Indicates the suggested time in minutes required to fix one single violation .
Violations	Number of violations of the rule that will be added to the Action Plan.
Total	Total effort in man/days required to fix all the violations of the selected rule. This value is calculated by multiplying the effort by the number of violations.