Security Dashboard - Action Plan Recommendation

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**.

Calculation of the remediation effort

The remediation effort of a rule is determined as follows:

- For ISO rules the remediation effort applied is deduced from its **ISO characteristic**
- For CISQ rules, the remediation effort applied is deduced from its **CISQ characteristic**
- For other rules, the remediation effort applied is deduced from the **technical criterion of the rule** (see the table below)

For a rule, the **total remediation effort proposed by the Action Plan Remediation feature is: (the remediation effort) x (average number of occurrences of violations) x (number of violations to be corrected).**

The total remediation effort

The remediation effort is an estimate to be used to select an action plan. It cannot claim to have a predictive value. In reality, it is necessary to take into account the technology (a C++ remediation effort will be different from a COBOL remediation), the development practices (unit tests, integration tests, etc.), the level of competence of the teams, the functional or technical complexity (backend, frontend).

Default efforts by technical criterion:

	Technical Criteria	**Evaluation**	**Impact**
Low effort	Documentation - Naming Convention Conformity Documentation - Style Conformity Complexity - Empty Code Documentation - Bad Comments Documentation - Automated Documentation	12 minutes (0.2 x 60 minutes)	Local impact
Low Effort	Documentation - Volume of Comments Dead code (static) Programming Practices - Structuredness'	24 minutes (0.4 x 60 minutes)	Local impact
Intermediate Effort	Complexity - Dynamic Instantiation Secure Coding - Weak Security Features Secure Coding - API Abuse,	30 minutes = (0.5 x 60 minutes)	Local Impact & Sensitive changes
Intermediate Effort	Programming Practices - Unexpected Behavior' Programming Practices - Error and Exception Handling Volume - Number of LOC Programming Practices - File Organization Conformity Programming Practices - OO Inheritance and Polymorphism Architecture - Multi-Layers and Data Access Programming Practices - Modularity and OO Encapsulation Conformity Complexity - Algorithmic and Control Structure Complexity Complexity - Technical Complexity Secure Coding - Encapsulation Secure Coding - Input Validation Secure Coding - Time and State Architecture - OS and Platform Independence Volume - Number of Components Efficiency - Memory, Network and Disk Space Management	1 hour = (1 x 60 minutes)	Global Impact & Sensitive Change
High Effort	Efficiency - SQL and Data Handling Performance Complexity - SQL Queries Efficiency - Expensive Calls in Loops Complexity - Functional Evolvability	2 hours = (2 x 60 minutes)	Very Sensitive changes
High Effort	Complexity - OO Inheritance and Polymorphism Volume - Number of Components Architecture - Object-level Dependencies Architecture - Reuse Efficiency - Memory, Network and Disk Space Management	3 hours= (3 x 60 minutes)	

The difference with the OMG Technical Debt calculation is as follows:

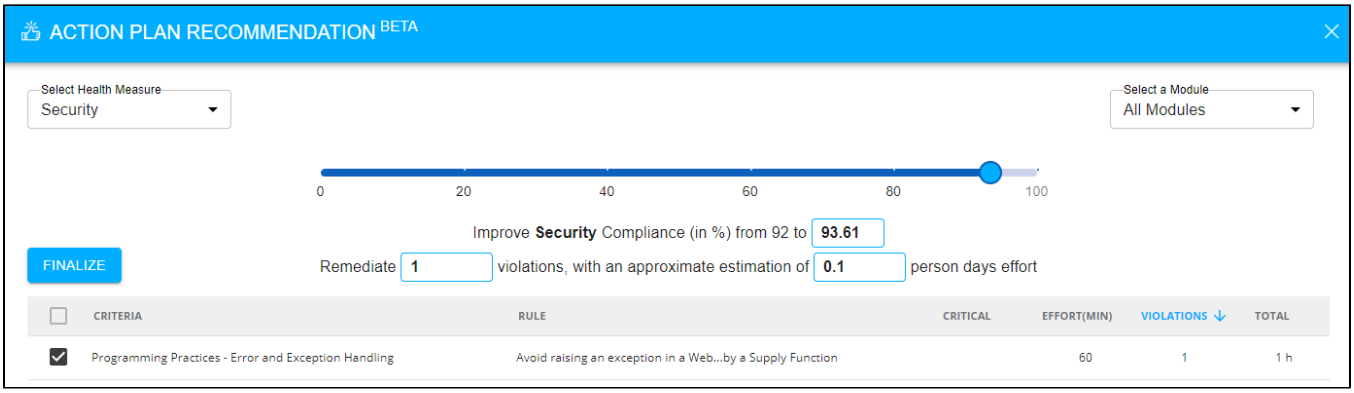
- OMG Technical Debt is limited to CISQ, while the Action Plan Remediation feature makes a calculation for all CISQ and non-CISQ rules (except if one explicitly selects the CISQ scope).
- OMG Technical Debt is adjusted for each object according to its characteristics (e.g. cyclomatic complexity) - the Action Plan Remediation feature does not make this adjustment due to calculation time.
- OMG Technical Debt is adjusted as close as possible to the number of occurrences of violations - the Action Plan Remediation feature i s based on an average of occurrences of violations for reasons of calculation time.

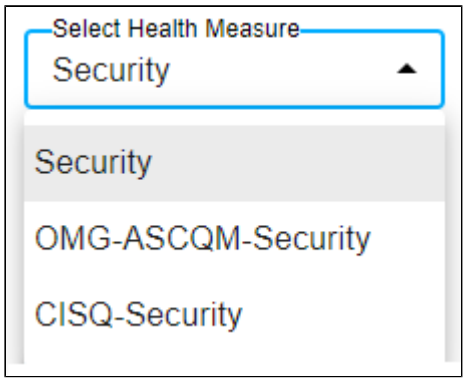
Accessing the Action Plan Recommendation

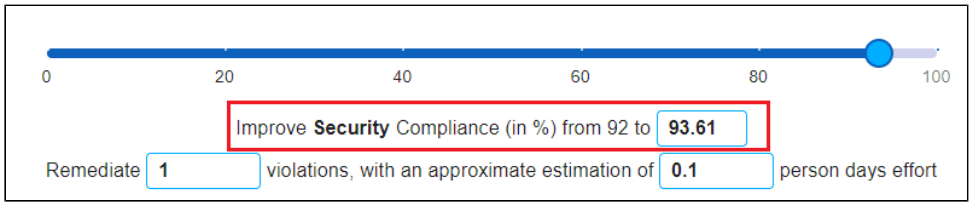
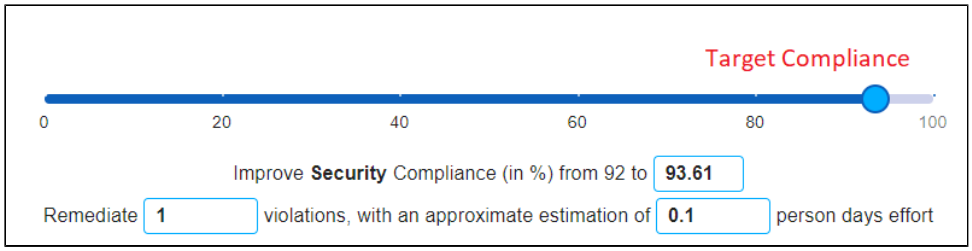
The Action Plan Recommendation feature can be accessed from the **Action Plan** using the icon in the top right corner:

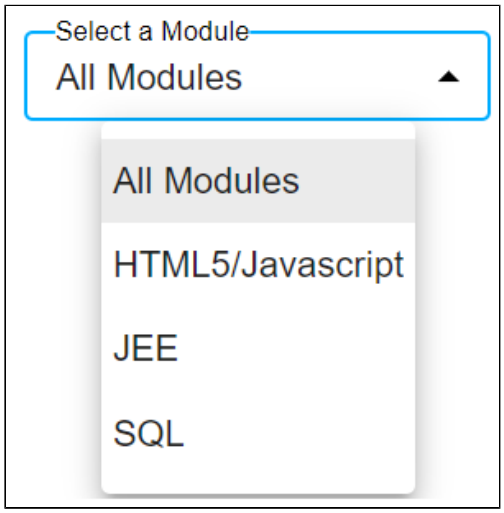
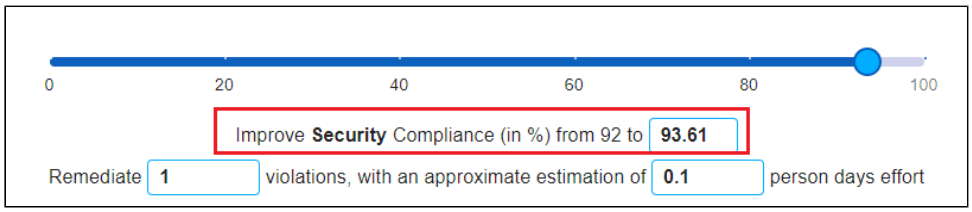
Action Plan Recommendation interface

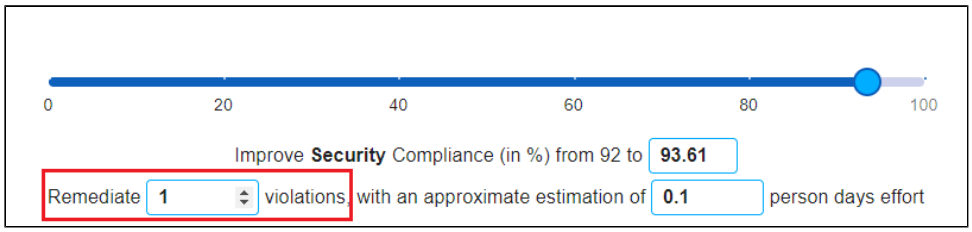
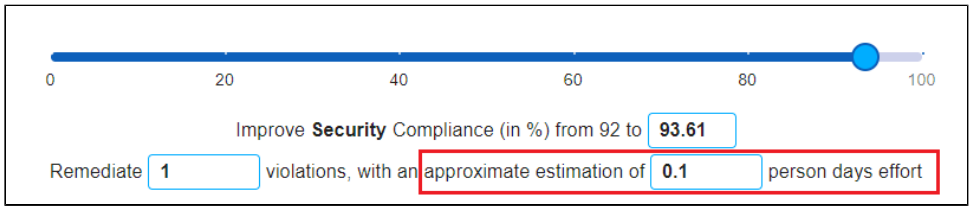
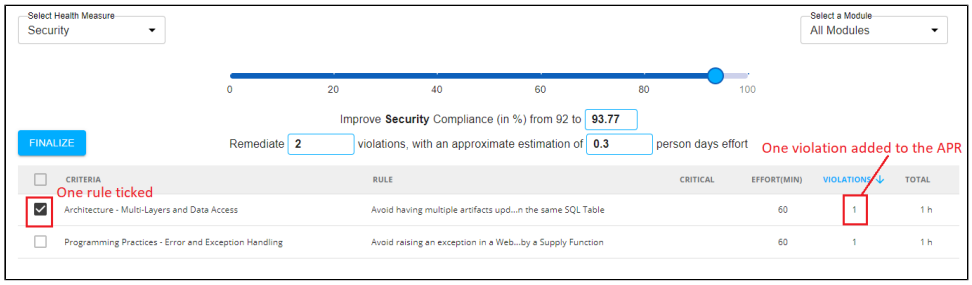
Click to enlarge



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**
	 
	• 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 a • 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 remediati 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).

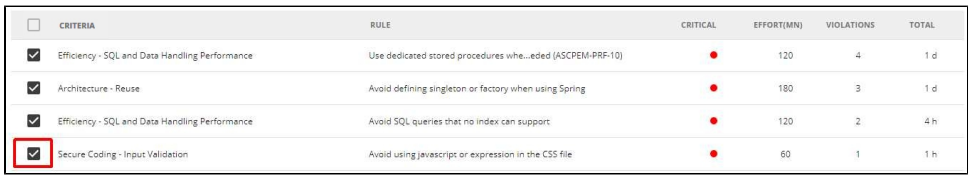
Violation manual entry	This option indicates **the number of violations that you want to fix**:  • When the Action Plan Recommendation is first opened, the box will indicate a default initial remediation target to **correct one** target will be set to **correct one additional violation**. • You can manually 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**:  • 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*  Note that the **Comment** in the Action Plan will be populated automatically and will describe the target remediation, for example: 

<table>
<tr><td>Action Plan Recommendation list</td><td>This section lists the rules that the Action Plan Recommendation algorithm thinks are the best match for the target remediation. Y
header.

<table>
<tr><td>Check boxes</td><td>The check boxes enable you to choose whether you want the violations for a specific rule to be added to the Actic
all rules will be added to the Action Plan. If you do not want to fix violations for a specific rule, de-select the associ

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

Click to enlarge

When you deselect a rule, the Action Plan Recommendation will recalculate the suggested Action Plan, there 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

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