**OBJECTIVES**

GENERAL

* Identify, analyze and evaluate the risks that can compromise the security for the assets, that are critical in the execution of a business process.

SPECIFIC:

* Apply the OWASP Risk Rating Methodology to analyze and evaluate security risks.
* Identify security controls/countermeasures/safeguards that can be needed to mitigate critical security risks.

OWASP Risk Rating Methodology can be found in the link:

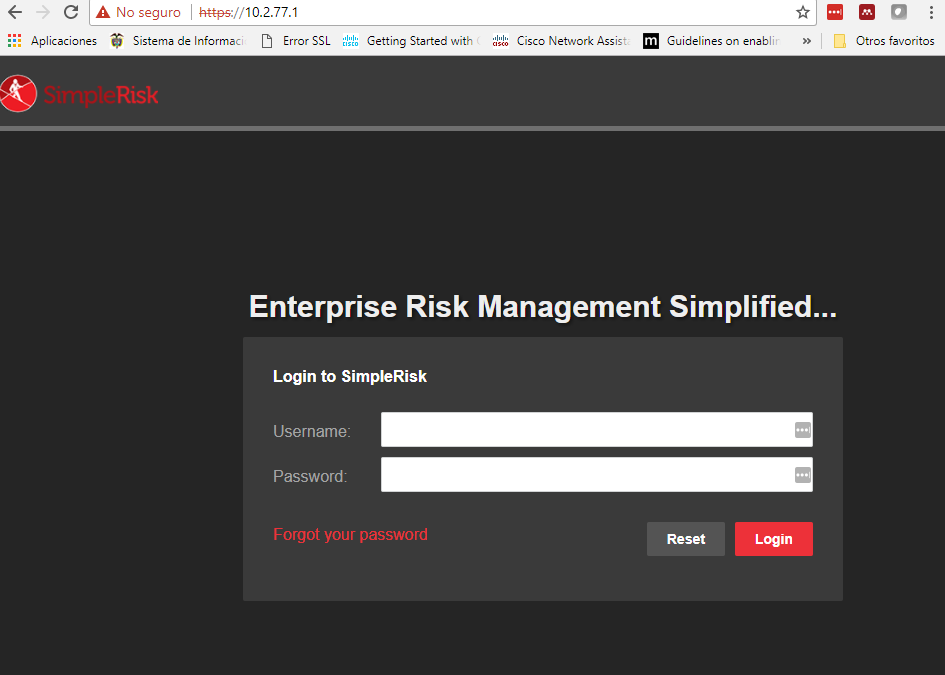
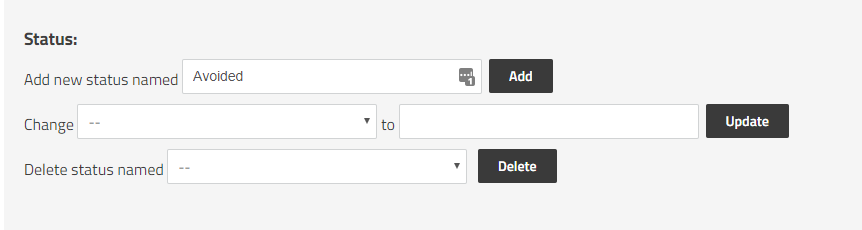
<https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>

Make groups of three students and make the following activities:

**SECTION ONE – SIMPLE RISK CONFIGURATION**

1. Start a local instance of SimpleRisk following instructions in Laboratory I and log in using credentials admin/admin.

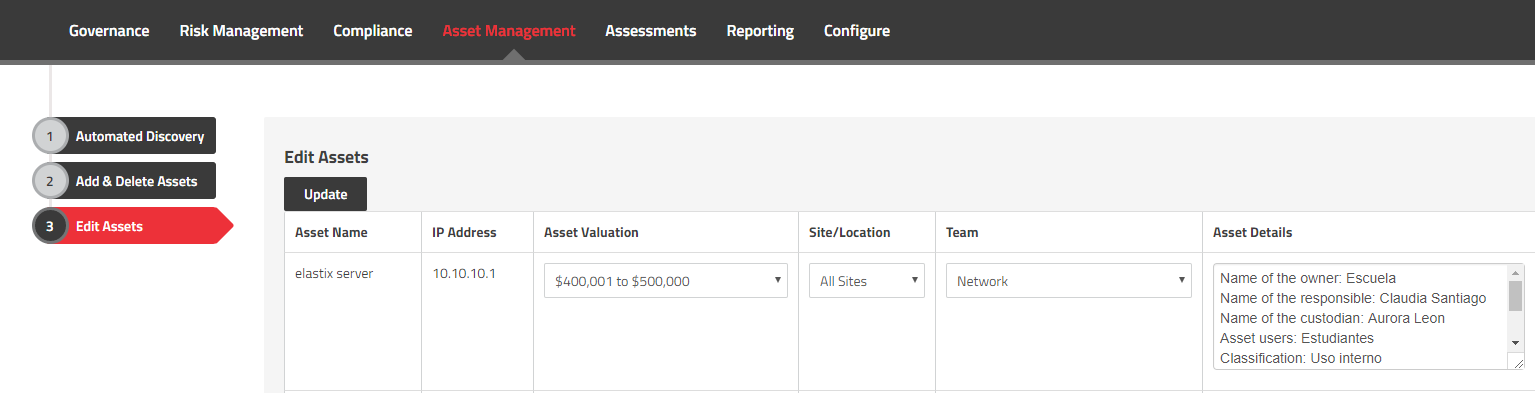
* In configure, go to “Add and remove values” and in status delete all existing status and create the followings: Accepted, Avoided, Mitigated and Transferred.



**SECTION TWO – ASSET INVENTORY**

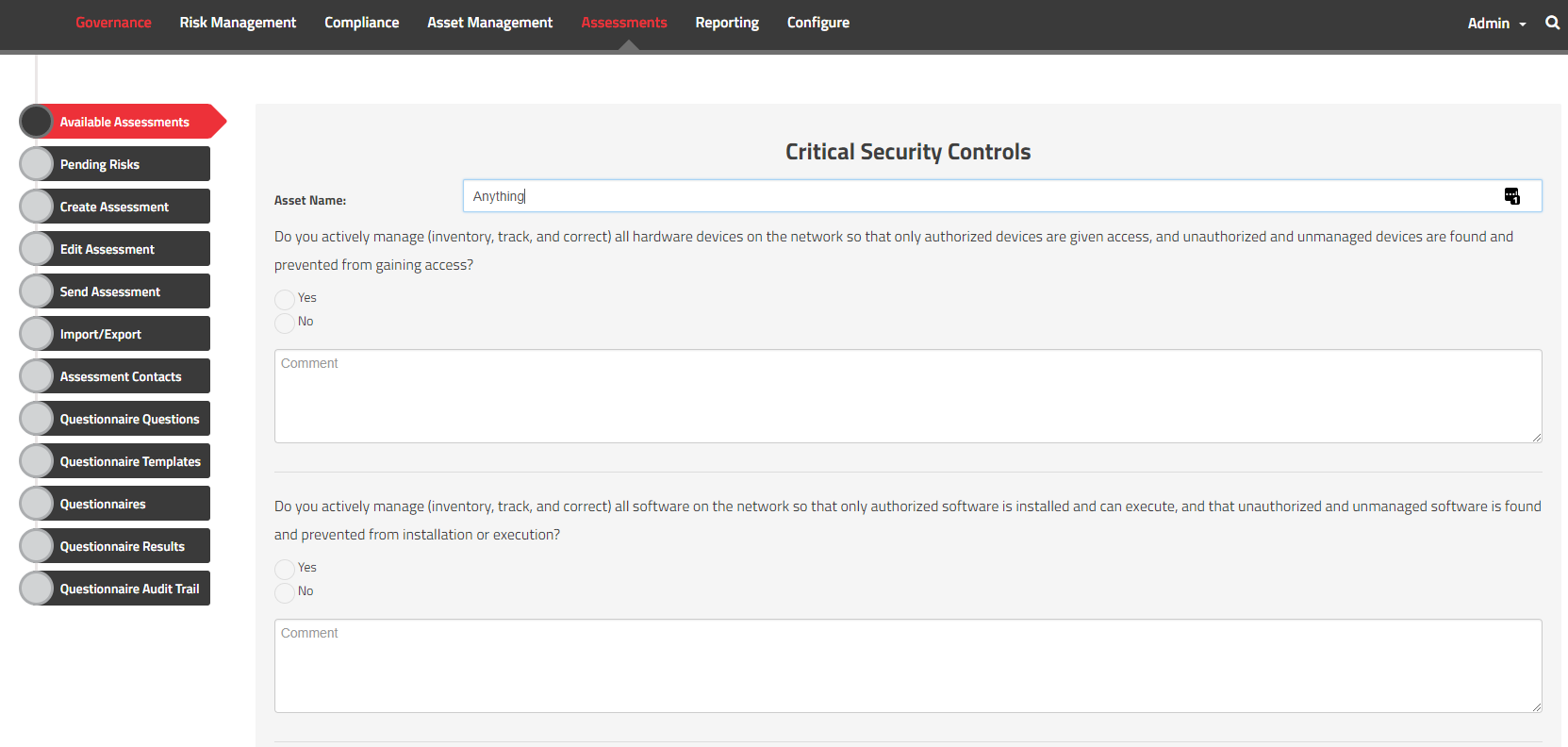
Verify the asset information filled out in the “Asset Management” section in SimpleRisk. For each asset fill: Asset name, IP Address, Site/location, Team and Asset Details. In Asset Details you must place the following information:

* Name of the owner
* Name of the responsible
* Name of the custodian
* Asset users
* Classification
* Impact to availability
* Impact to confidentiality
* Impact to Integrity
* Total Impact

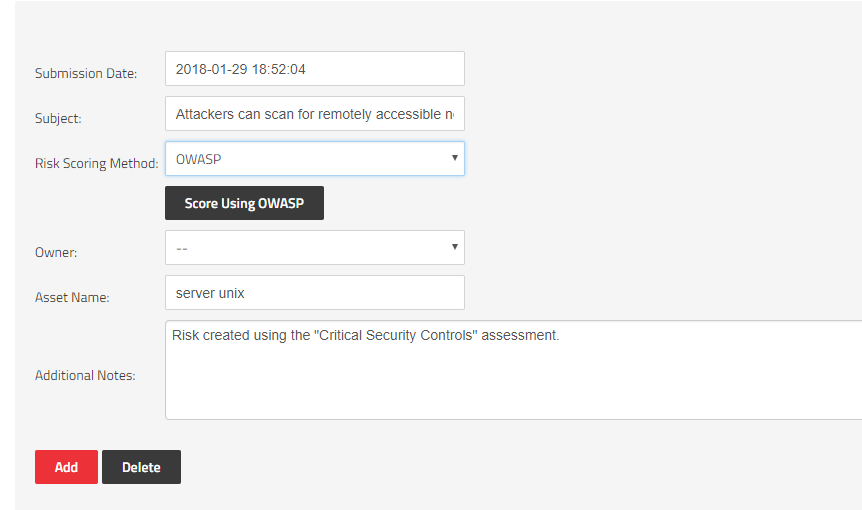


**SECTION THREE – RISK ASSESSMENT**

In the “Assessment” section in Simple Risk start the “Critical Security Controls” and fill out and submit the questionnaire composed of 21 questions without thinking in an asset but the area or the process:

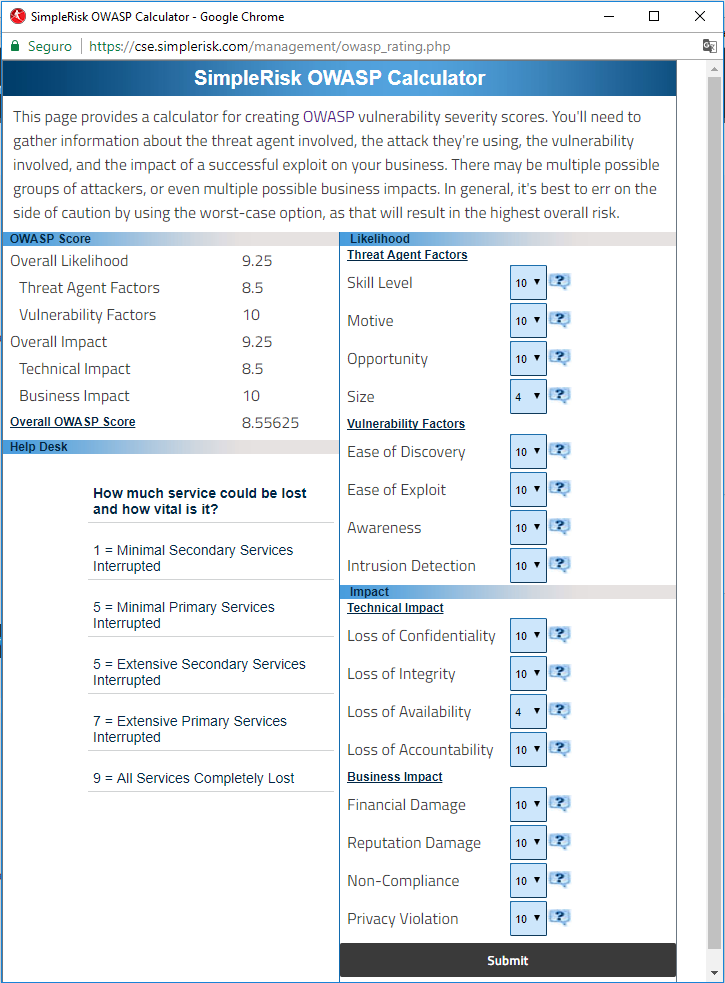


After submit the questionnaire, all the suggested risk will appear in the “Pending risks” section.

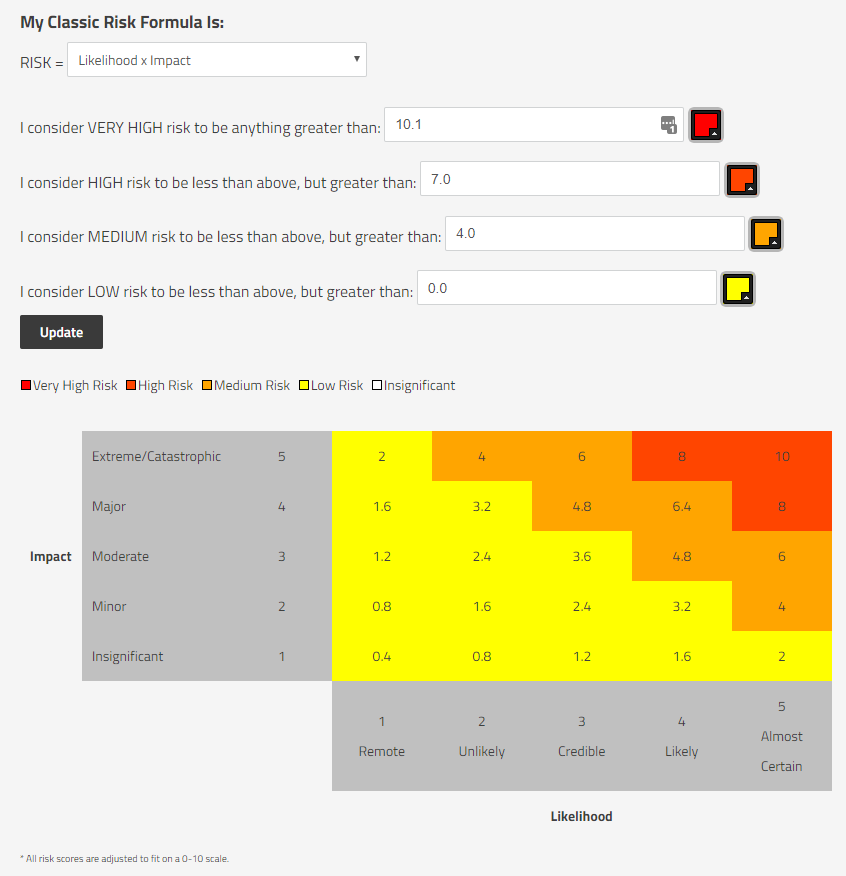


Analyze each risk reviewing: 1) The asset over which the risk applies and 2) The risk score using a Risk Scoring Methodology. SimpleRisk can use 4 Risk Scoring Methodology: OWASP, CVSS, DREAD and Classic.

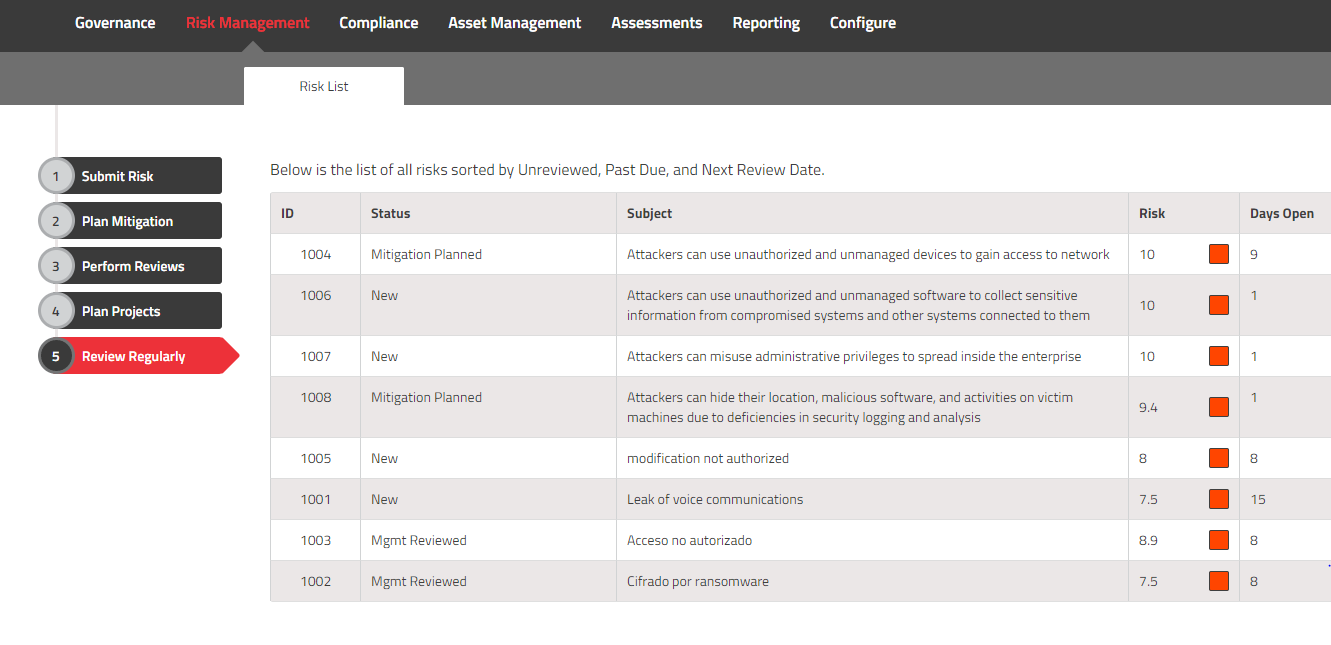
OWASP Risk Rating Methodology [[1]](#footnote-1)calculates the Overall OWASP risk score using the Likelihood and the Impact. The Likelihood depends on the Threat agent and the Vulnerability Factors, and Impact depends on the Technical Impact and the Business Impact. You can click on the interrogation symbol to understand the meaning of the scale values:



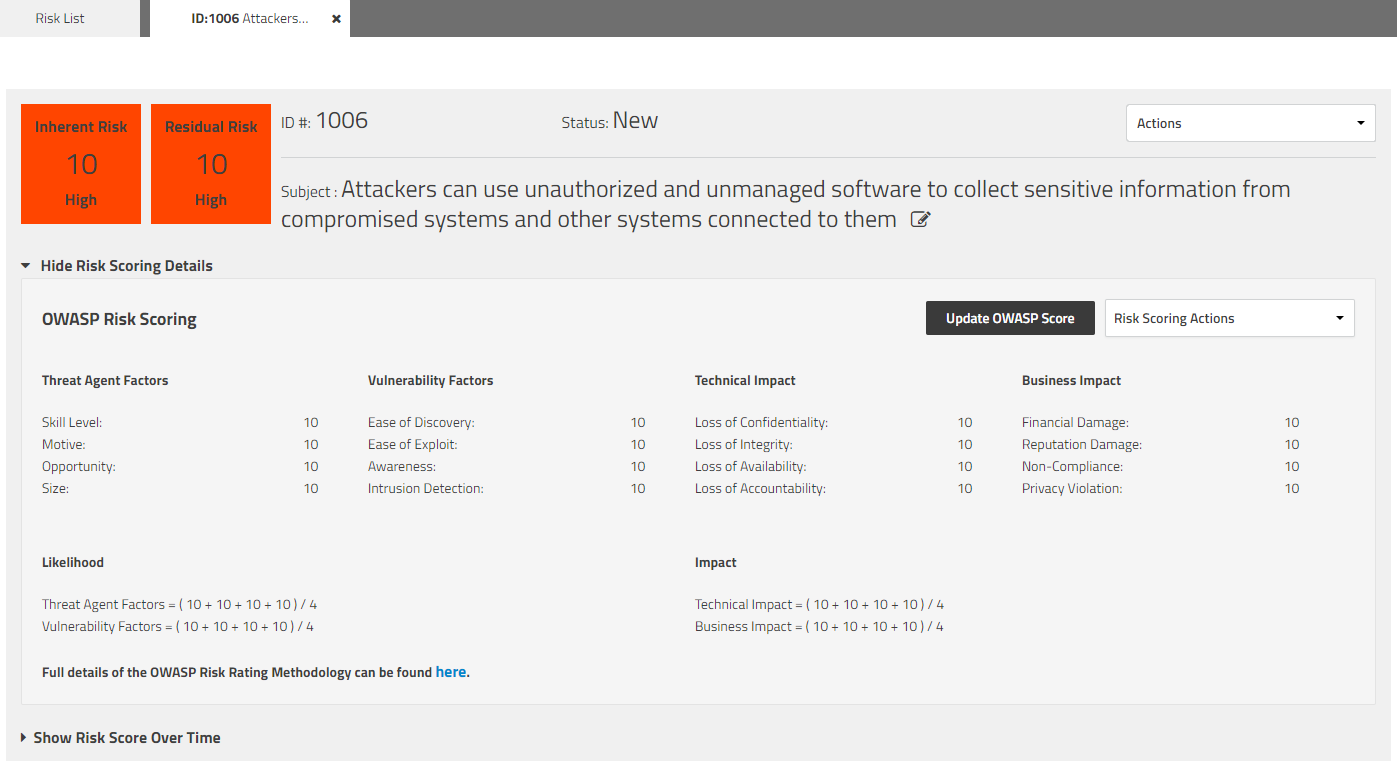
This Overall Owasp Score (8.55) correspond to a High risk according to the heat map:



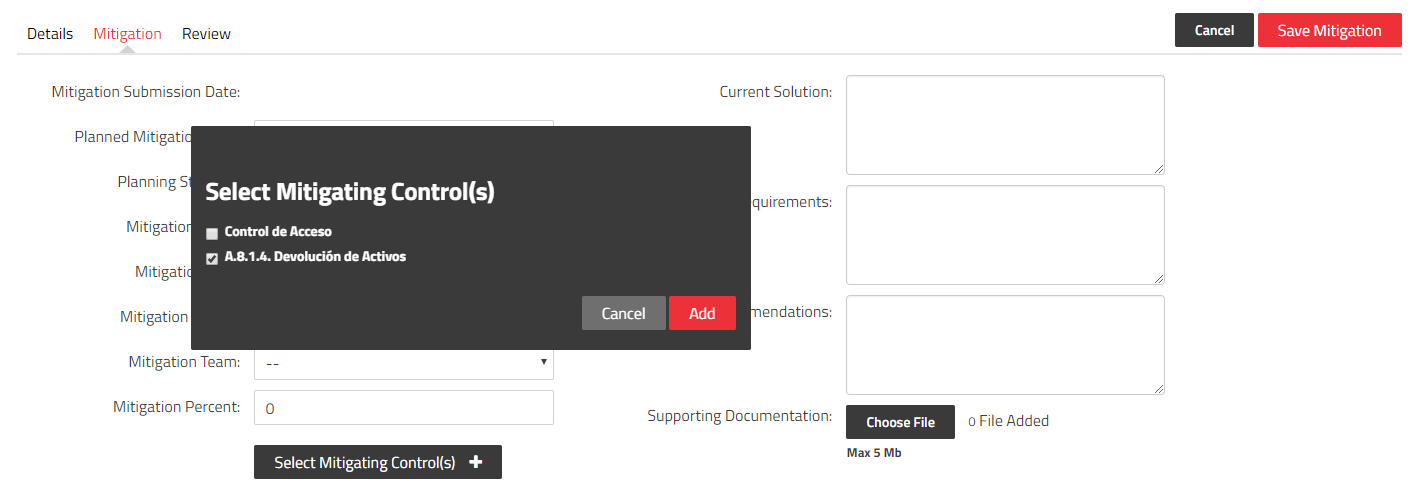
After setting the Owasp Risk score you can add the risk. In the Risk Management tab you can view the available risks:



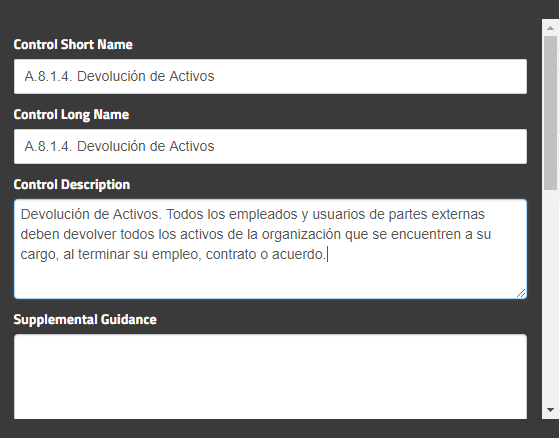
Get in on of the risk and you will see the most important information:



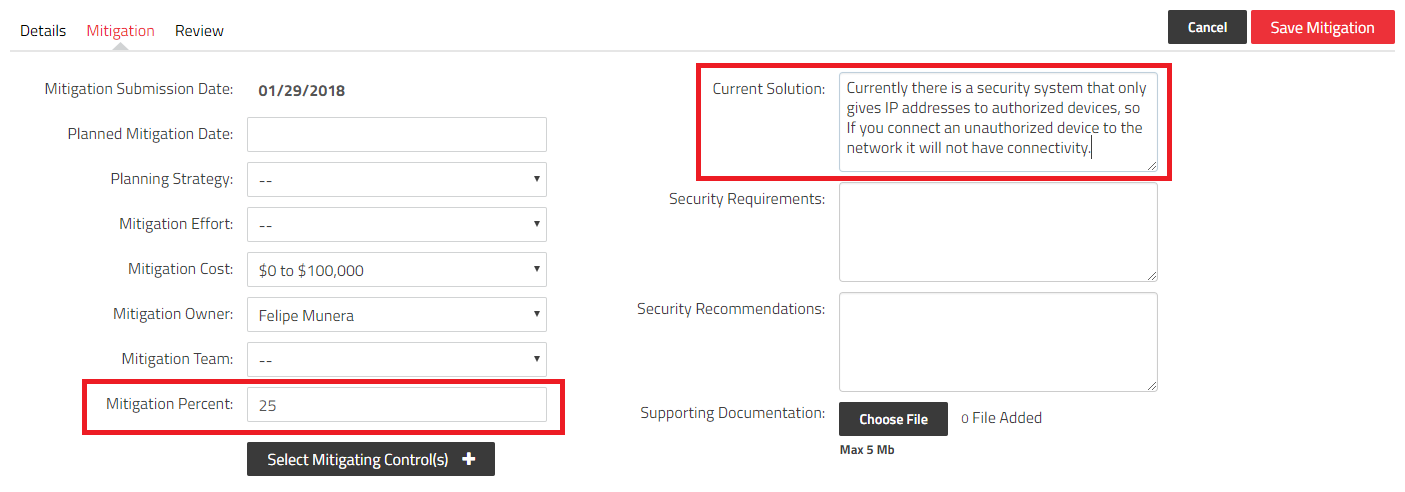
In mitigation tab you can select edit mitigation and select the controls that currently apply to the asset (the existing controls):



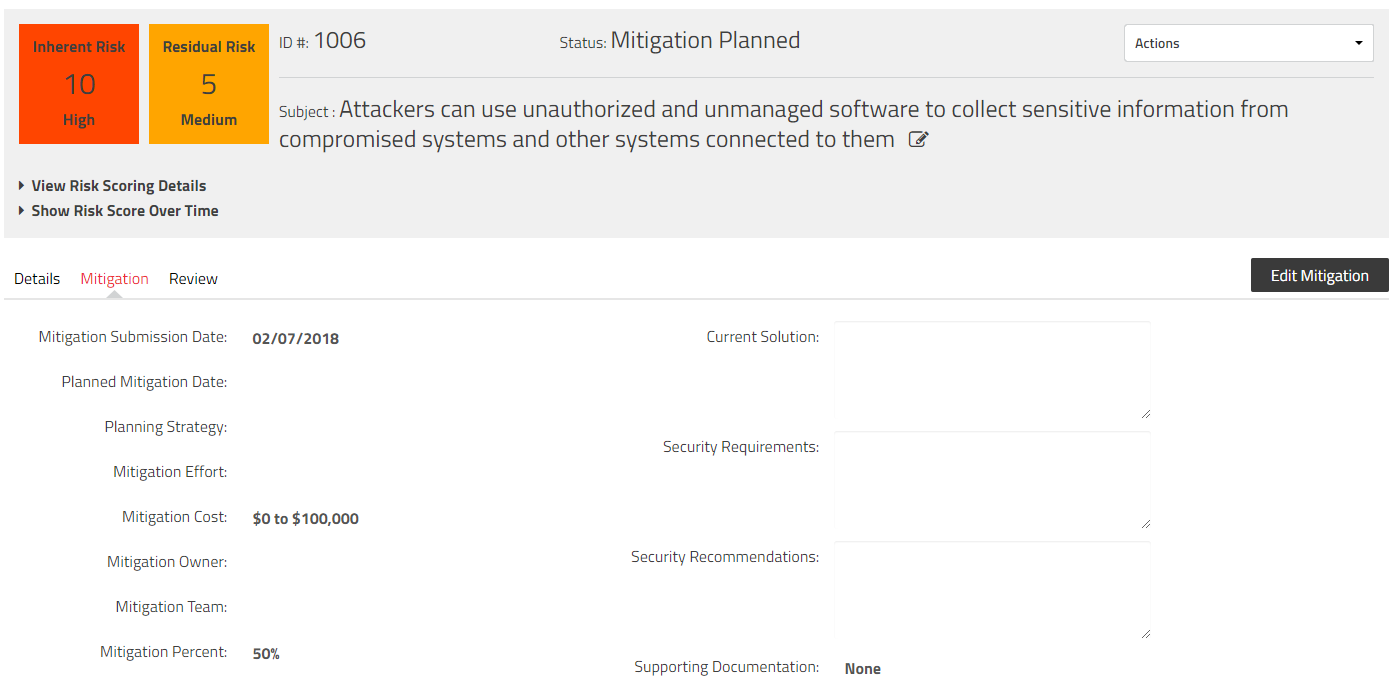
Before selecting a control, you must create it in the tab Governance, going to controls and pressing the plus (+) button:



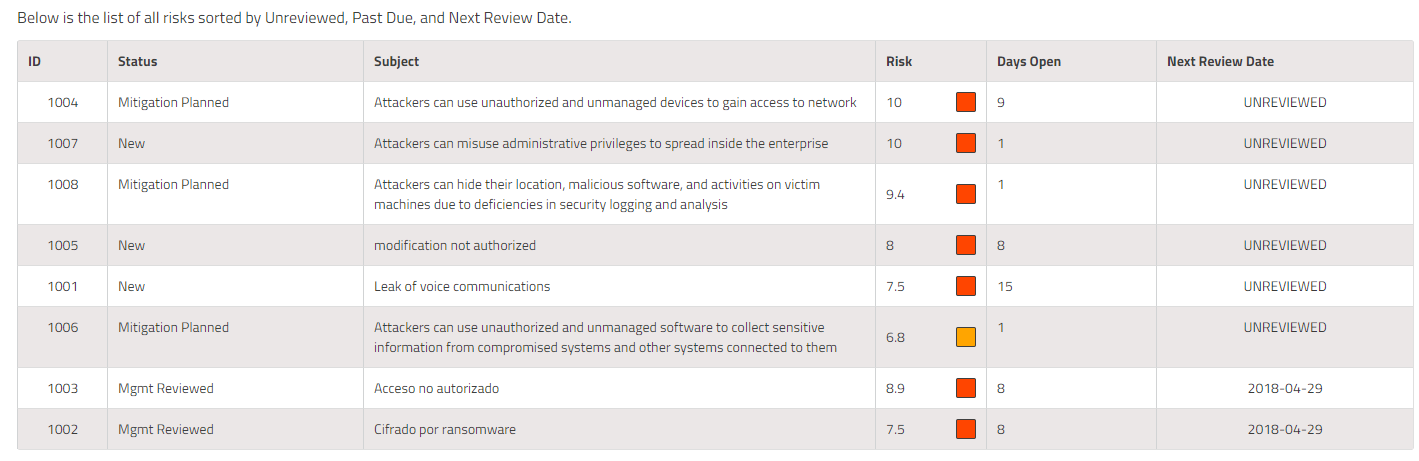
After selecting the controls, yu must choose the “Mitigation percent” [0-100%] which represent how much the selected control reduce the risk. Additionally you must fill out the “current solution”.



After refreshing the page, you will see that residual risk gets reduce:



After all risks have been set you should be able to see the resume in the “review regularly” section:



Then you must review all the risks to decide what to do next. The treatment option can be:

* Mitigate: Apply an additional control to reduce the Residual Risk.
* Accept: Accept the risk because the Residual Risk is under the Acceptable Risk Threshold, or because the cost of implementing the control is more expensive that the asset value.
* Avoid: Eliminate the origin of the Risk (for example replace the asset for a new one with the vulnerability and in this way, eliminate the origin of the risk).
* Transfer: Pass the Residual Risk to a third party (for example an insurance company).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Option** | **Residual risks** | **Status** | **What to to in SimpleRisk?** | |
| **Mitigate the risk** | i) When 10 > Residual risks > 4  AND  ii) It is possible to implement a control to mitigate it | Mitigated | Add additional controls in the “Mitigation Tab” or/and adjust the “Mitigation Percent” so the Residual Risk can be < 4 | Change risk status to **Mitigated** |
| **Accept the risk** | i) When 4 > Residual risks > 0  OR  ii) When the cost of implementing the control is more expensive that the asset value. | Accepted | Do nothing because the risk is low | Change risk status to **Accepted** |
| **Transfer the risk** | i) When 10 > Residual risks > 4  AND  ii) It is NOT possible to implement a control to mitigate it | Transferred | In “Security Recommendations” explain how to transfer the risk | Change risk status to **Transferred** |
| **Avoid the risk** | i) When 10 > Residual risks > 4  AND  ii) It is NOT possible to implement a control to mitigate it | Avoided | In “Security Recommendations” explain how to avoid the risk | Change risk status to **Avoided** |

**SECTION FOUR**

**Executive Summary:** Prepare an Executive Summary where you can resume the most important aspect of the risk analysis that you have just done. You can use graphs, tables, figures or any other element obtained from SimpleRisk. The executive summary must help help to explain to the manager: the higher risks in the company, how many risks where transferred/avoided/accepted/mitigated and the change in the risk value before controls (total risk) and after controls (residual risk).

Some interesting figures can be obtained from the “Reporting” Tab in SimpleRisk:

* Mitigated vs unmitigated
* Level of risks [Very High, High, Medium, Low] from the Risk Dashboard
* Risk status [Accepted, Avoided, Mitigated, Transferred] from the Risk Dashboard
* Risk source [External, People, Process, System] from the Risk Dashboard
* Risk by Asset
* High Risk Report

Prepare the following two documents to deliver:

1. A zip folder with the following HTML files:
   1. Asset management -> Edit Assets
   2. Risk management -> Review Regularly
   3. For each risk
      1. Details tab with expand of the “View Risk Scoring Details”
      2. Mitigation tab
   4. Reporting -> Overview -> Mitigated vs unmitigated
   5. Reporting -> Risk Dashboard
   6. Reporting -> Risk advice
   7. Reporting -> Risk and assets (Report: Risks by Asset)
   8. Reporting -> High Risk Report
2. PDF with the Executive Summary about the company risks.

The files must be named in the following way:

* **Lab2-Name1LastName1Name2Lastname2Name3Lastname3.zip**
* **ExecutiveSummary-Name1LastName1Name2Lastname2Name3Lastname3.pdf**

1. <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology> [↑](#footnote-ref-1)