RITA

RITA is designed to assess the security state of the NG-SOC infrastructure based on a **dynamic risk analysis methodology** that incorporates a new **modelling approach**. This methodology is inspired by existing methodologies that are commonly used by security practitioners and consultants for risk assessment, but was tailored for the field of cybersecurity, based on the identified security requirements in the scope of the project.

The model is based on the identification of:

a) **basic assets** and their exposure to threat,
b) **system (composite) assets**, their decomposition to basic assets and their relationships, as well as list of threats for each basic asset, the threat likelihood and associated countermeasures mapped to CIS Controls classification,
c) **threats** that can harm the system and their association with the system asset types,
d) **vulnerabilities** and their association with the identified threats,
e) **countermeasures** and their association with the threat that it mitigates.

RITA functions include:

a) an automated framework for **assets identification**,
b) the **iterative risk and impact assessments** on existing cybersecurity assets, depending on the assets, their interconnections and their operational environment,
c) the **estimation of threats cascading mechanisms**, with the extraction of risk scores leading to the timely identification and warning on vulnerabilities and attack entry points.

In summary, RITA engine:

1) provides an environment for the hierarchical system modelling that can be performed from a system user or architect without required security knowledge;
2) provides an updatable and upgradable knowledgebase with assets, threats, vulnerabilities, countermeasures and their relationships;
3) consumes information from other architectural components regarding vulnerabilities and threats;

4) dynamically evaluates the cybersecurity risk and impact of the successful exploitation of a vulnerability in the NG-SOC ecosystem, with automatic re-evaluation of risks and impacts upon an event or a change;
5) incorporates an inference engine taking into account cascading threats, risks and impacts by exploiting the interconnections and interdependencies between assets, entities and services.

RITA produces the risk and impact assessment results which will be used for selecting and configuring the required countermeasures. In fact, the outcome of the risk and impact assessment process will be exploited by NG-SOC in order to create new security configurations for the organization, each one being characterized by a different set of applied countermeasures.

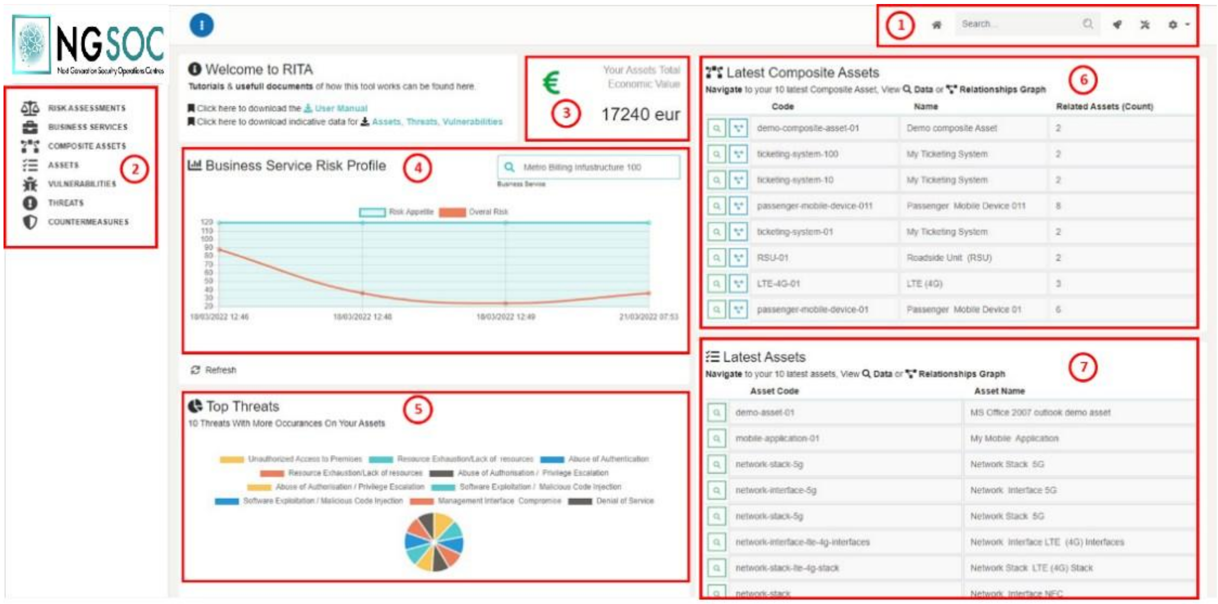
RITA Guide

Dashboard

Users are presented with the RITA main screen, which essentially serves as the tools dashboard and consists of the following:

- **Application toolbar** ①, which is always visible, containing links to the following pages: home, Search Input, allowing to search for entities (such as assets, threats, vulnerabilities, countermeasures, services and risk assessments) depending on the currently accessed dashboard.
- **Navigation panel** ②, offering an easy way to navigate around the different elements of the tool's knowledge base and inventories, namely the assets, composite assets, threats, vulnerabilities, and countermeasures as well as the risk assessments and business services.
- **Economic Value** dashlet ③ that presents the common economic value of all composite assets.
- **Business Service Risk Profile** dashlet ④ that provides a quick visualisation of the business process risk evolution, by presenting the results of the risk assessments executed by the user.

- **Top Threats** dashlet ⑤ that presents the top-10 threats with more occurrences on the assets.
- **Latest Composite Assets** dashlet ⑥ that presents the 10 latest composite assets, allowing for easy access to material.
- **Latest Assets** dashlet ⑦ that presents the 10 latest assets.


NGSOC
Next Generation Security Operations Centres
RISK ASSESSMENTS
BUSINESS SERVICES
COMPOSITE ASSETS
ASSETS
VULNERABILITIES
THREATS
COUNTERMEASURES
1
2
3
4
5
6
7
Search...
Your Assets Total Economic Value
€
Metro Billing Infustructure 100
Business Service
Risk Appetite
Overal Risk
120
110
100
90
80
70
60
50
40
30
20
18/03/2022 12:46
18/03/2022 12:48
18/03/2022 12:49
21/03/2022 07:53
Refresh
Unauthorized Access to Premises
Resource Exhaustion/Lack of resources
Abuse of Authentication
Resource Exhaustion/Lack of resources
Abuse of Authorisation / Privilege Escalation
Abuse of Authorisation / Privilege Escalation
Software Exploitation / Malicious Code Injection
Software Exploitation / Malicious Code Injection
Management Interface Compromise
Denial of Service

Welcome to RITA

Tutorials & **usefull documents** of how this tool works can be found here.

Click here to download the User Manual

Click here to download indicative data for Assets, Threats, Vulnerabilities

17240 eur

Business Service Risk Profile

Top Threats

10 Threats With More Occurances On Your Assets

Latest Composite Assets

Navigate to your 10 latest Composite Asset, View **Data** or **Relationships Graph**

Code	Name	Related Assets (Count)
demo-composite-asset-01	Demo composite Asset	2
ticketing-system-100	My Ticketing System	2
ticketing-system-10	My Ticketing System	2
passenger-mobile-device-011	Passenger Mobile Device 011	8
ticketing-system-01	My Ticketing System	2
RSU-01	Roadside Unit (RSU)	2
LTE-4G-01	LTE (4G)	3
passenger-mobile-device-01	Passenger Mobile Device 01	6

Latest Assets

Navigate to your 10 latest assets, View **Data** or **Relationships Graph**

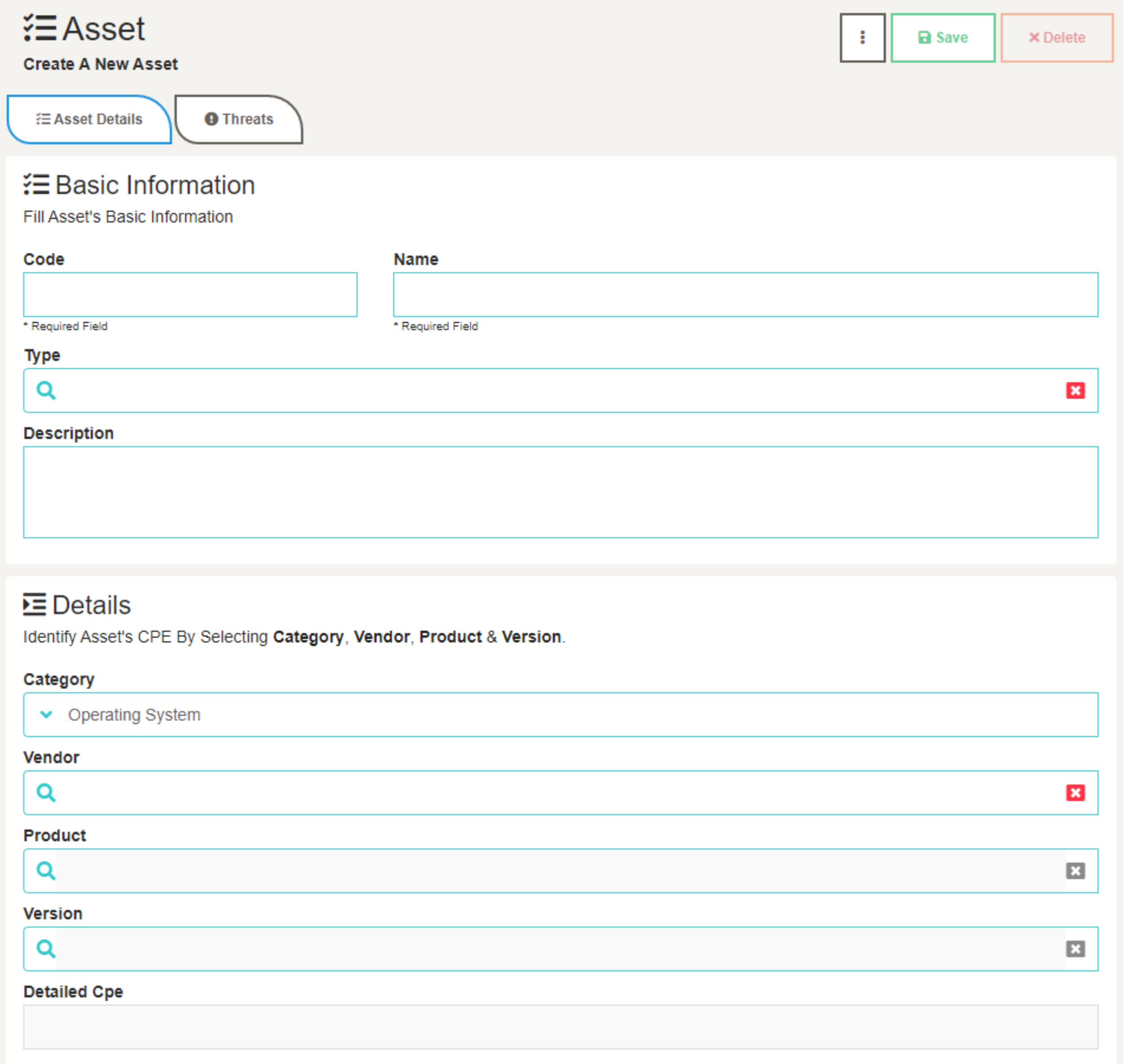
Asset Code	Asset Name
demo-asset-01	MS Office 2007 outlook demo asset
mobile-application-01	My Mobile Application
network-stack-5g	Network Stack 5G
network-interface-5g	Network Interface 5G
network-stack-5g	Network Stack 5G
network-interface-lte-4g-interfaces	Network Interface LTE (4G) Interfaces
network-stack-lte-4g-stack	Network Stack LTE (4G) Stack
network-stack	Network Interface NFC

RITA can visualize information graphically on the web browser through an interactive user interface that presents and organizes information on **dashlets** that sit on their personal **dashboard**. Dashlets provide access to information in simple and clear fashion.

Assets

1. Login to RITA
2. Click on the “**Assets**” menu item on the **Navigation panel**.
3. Click on the “New” button and populate the required information that is grouped into two tabs, namely: the “Asset Details” and “Threats” tabs. The “Asset Details” tab groups information into logical areas, namely “Basic Information” and “Details”:

- In the “Basic Information” area provide the asset’s code, name, type and description.
- In the “Details” area select the Category, Vendor, Product & Version in order for the tool to automatically generate the asset CPE value.
- Finally click the “Save” button.
- Navigating to the “Threats” tab we are presented with the threats that have been successfully mapped/associated to the selected asset type of the newly created basic asset.



Asset

Create A New Asset

Basic Information

Fill Asset's Basic Information

Code:

* Required Field

Name:

* Required Field

Type:

Description:

Details

Identify Asset's CPE By Selecting **Category**, **Vendor**, **Product** & **Version**.

Category: Operating System

Vendor:

Product:

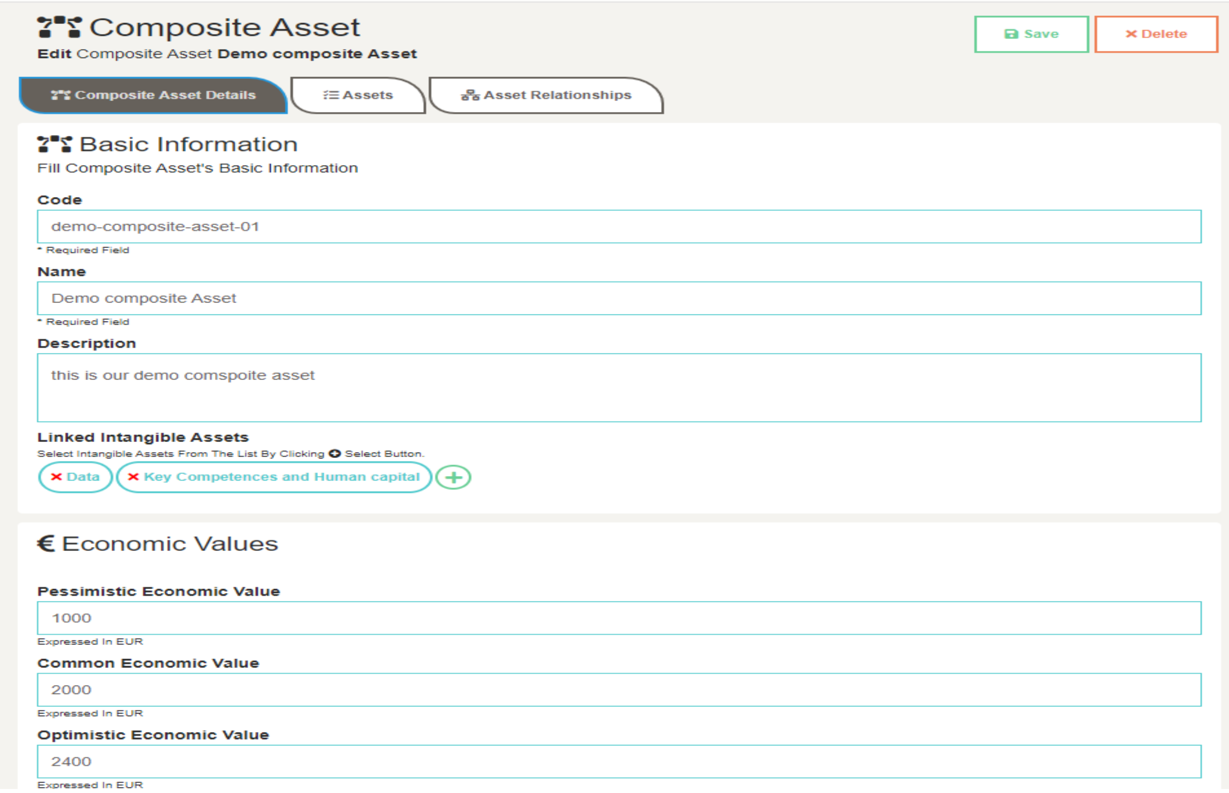
Version:

Detailed Cpe:

Asset repository, is populated with new entries (basic assets) as the system is used, enabling the NG-SOC platform users to maintain a dynamic and up-to-date **asset inventory.**

Composite Assets

1. Login to RITA
2. Click on the "**Composite Assets**" menu item on the **Navigation panel**.
3. Click on the "New" button and populate the required information that is grouped into logical tabs, namely the "Composite Asset Details", "Assets" and "Asset relationships":
   - In the "Composite Asset Details" tab group provide the composite asset's code, name, description, economic values and links to intangible assets.
   - In the "Assets" tab select the list of basic assets that are used to make up the composite asset including their priority in terms of economic value.
   - For each asset, select whether an identified threat is active, set its likelihood and set applicable counter measures.
   - In the "Asset relationships" tab define the assets relationships.
   - Finally click the "Save" button.



Composite Asset

Edit Composite Asset **Demo composite Asset**

Basic Information

Fill Composite Asset's Basic Information

Code

demo-composite-asset-01

* Required Field

Name

Demo composite Asset

* Required Field

Description

this is our demo comspoite asset

Linked Intangible Assets

Select Intangible Assets From The List By Clicking ⊕ Select Button.

✕ Data ✕ Key Competences and Human capital ⊕

€ Economic Values

Pessimistic Economic Value

1000

Expressed In EUR

Common Economic Value

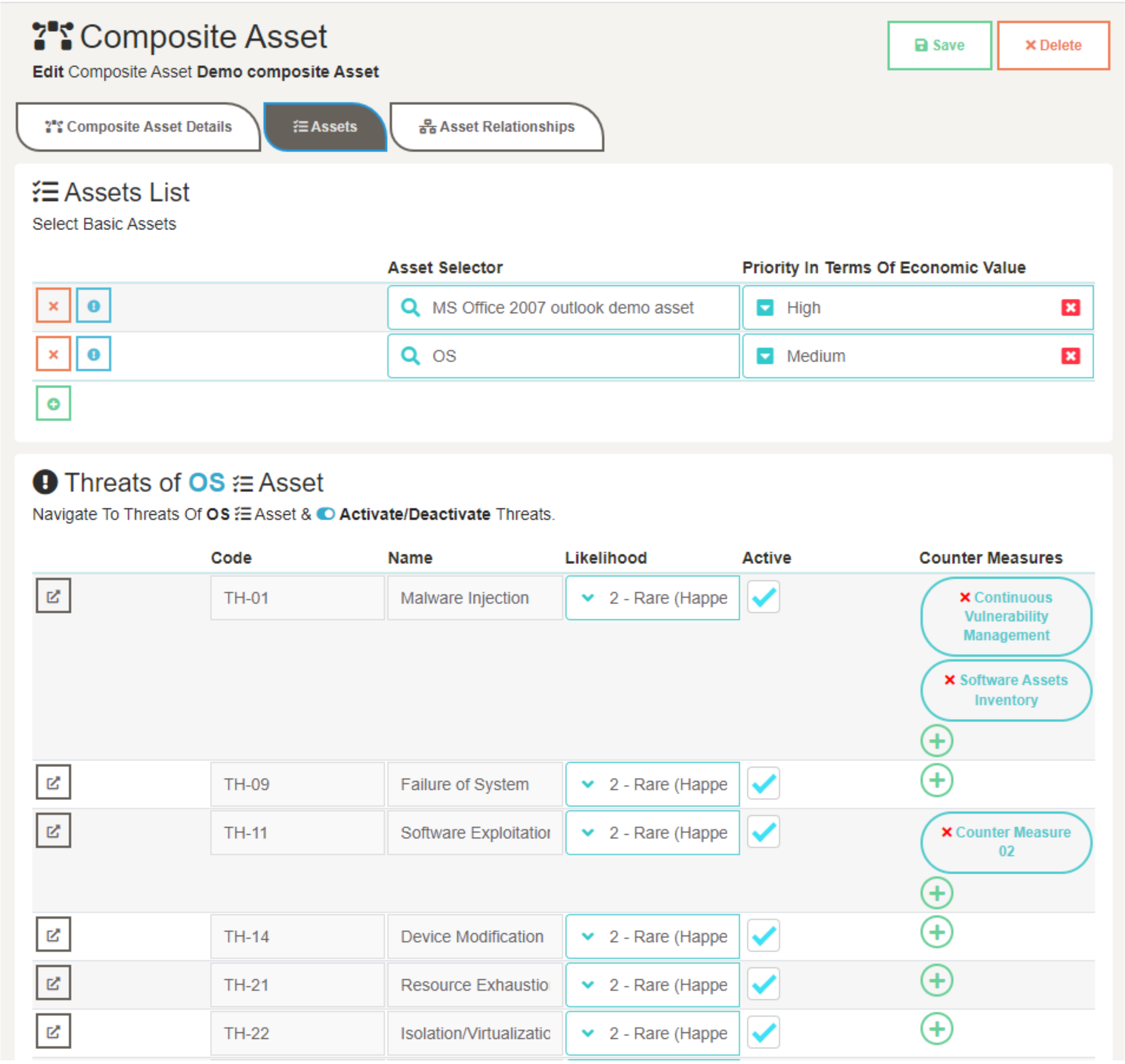
2000

Expressed In EUR

Optimistic Economic Value

2400

Expressed In EUR



Composite Asset

Edit Composite Asset **Demo composite Asset**

Assets List

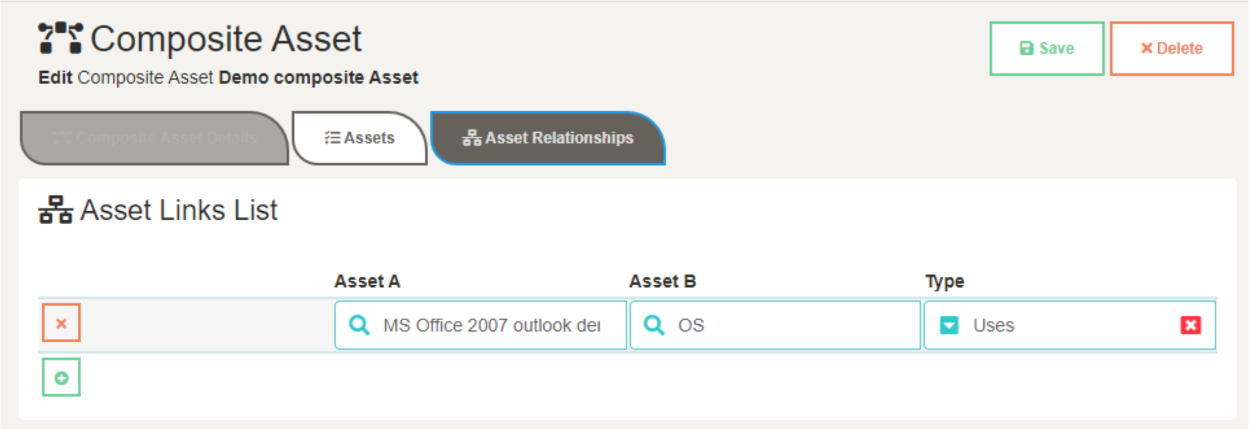
Select Basic Assets

Asset Selector	Priority In Terms Of Economic Value
MS Office 2007 outlook demo asset	High
OS	Medium

Threats of OS Asset

Navigate To Threats Of **OS** Asset & **Activate/Deactivate** Threats.

Code	Name	Likelihood	Active	Counter Measures
TH-01	Malware Injection	2 - Rare (Happe	✓	Continuous Vulnerability Management Software Assets Inventory
TH-09	Failure of System	2 - Rare (Happe	✓	
TH-11	Software Exploitatior	2 - Rare (Happe	✓	Counter Measure 02
TH-14	Device Modification	2 - Rare (Happe	✓	
TH-21	Resource Exhaustio	2 - Rare (Happe	✓	
TH-22	Isolation/Virtualizatic	2 - Rare (Happe	✓	



Composite Asset

Edit Composite Asset **Demo composite Asset**

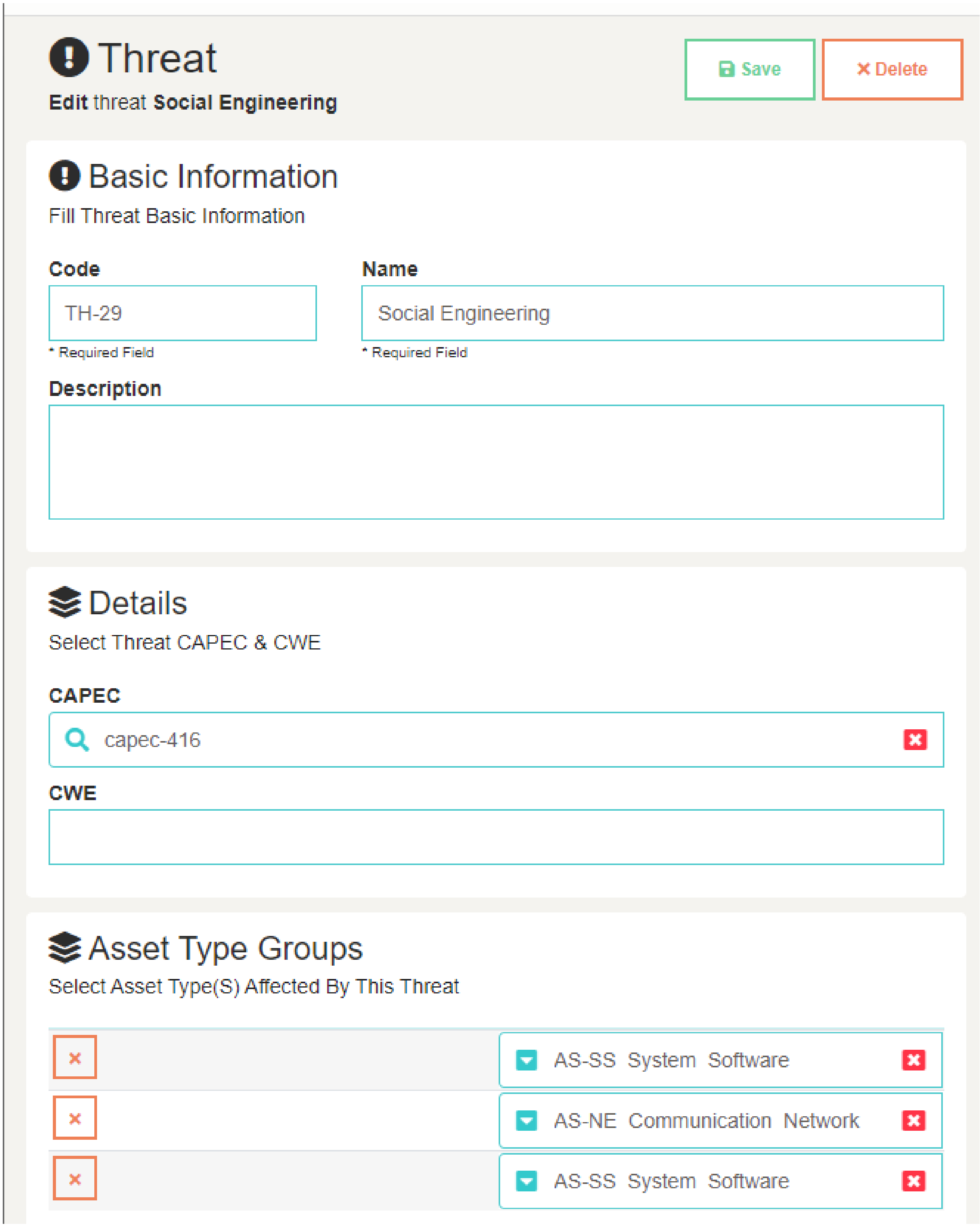
Asset Links List

Asset A	Asset B	Type
MS Office 2007 outlook de	OS	Uses

Asset repository, is populated with new entries as the system is used, enabling the NG-SOC platform users to maintain a dynamic and up-to-date **asset inventory**.

Threats

1. Login to RITA
2. Click on the “**Threats**” menu item on the **navigation panel**
3. Click on the “New” button and populate the required information that is grouped into logical areas, namely Basic Information, Details, Asset Type Groups and Impact:
    - In the “Basic information” area provide the threat code, name and description.
    - In the “Details” area select the CAPEC entry/value and optionally type the CWE value.
    - In the “Asset Type Groups” area select the asset type(s) that are affected by this threat.
    - In the “Impact” area select the security objectives (Confidentiality, Integrity and Availability) that are affected by this threat.
    - Finally click the “Save” button.



Threat

Edit threat **Social Engineering**

Basic Information

Fill Threat Basic Information

Code	**Name**
TH-29	Social Engineering
* Required Field	* Required Field

Description

Details

Select Threat CAPEC & CWE

CAPEC

capec-416

CWE

Asset Type Groups

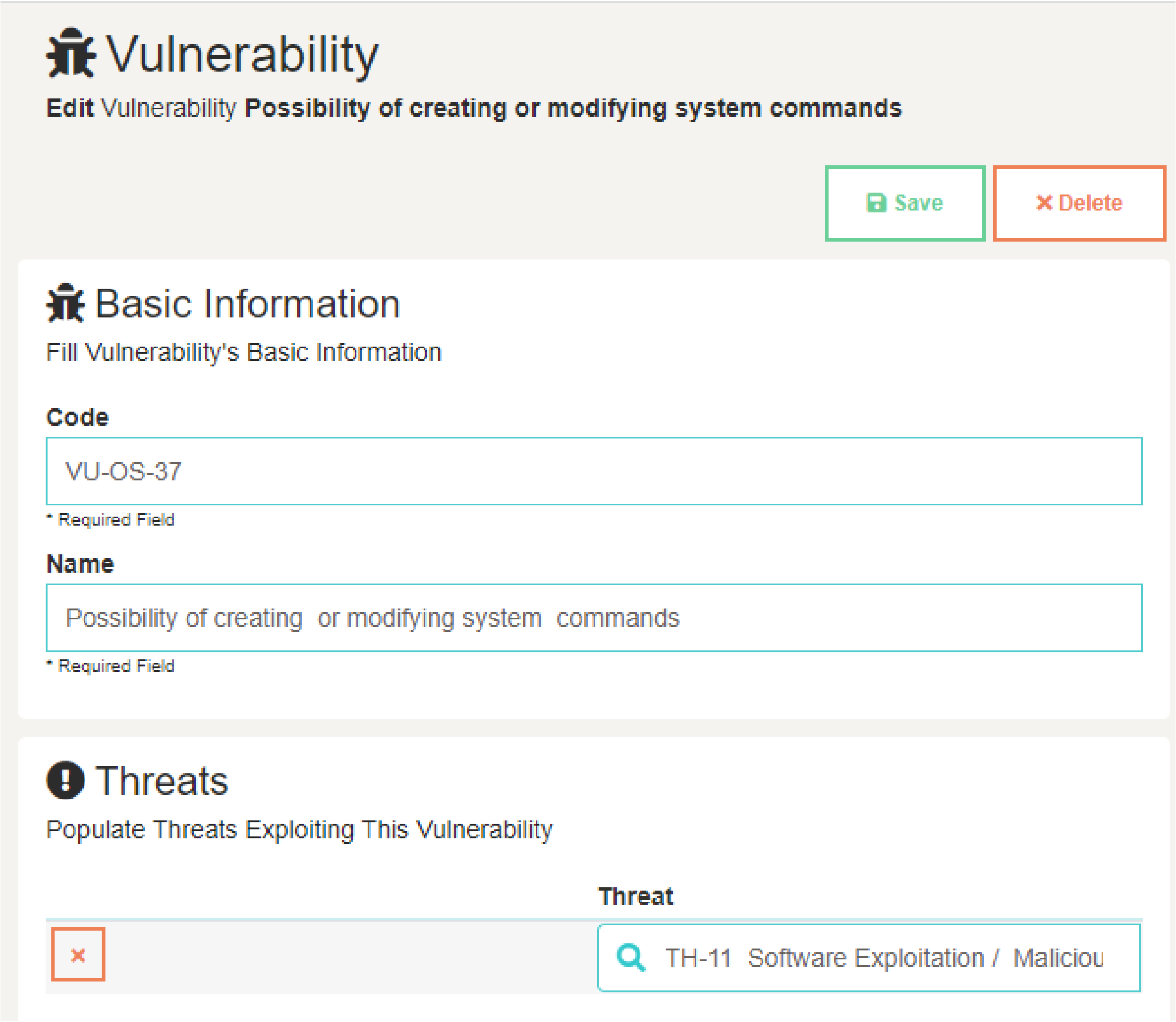
Select Asset Type(S) Affected By This Threat

×	AS-SS System Software
×	AS-NE Communication Network
×	AS-SS System Software

Threats repository, is populated with new entries as the system is used, enabling the NG-SOC platform users to maintain a dynamic and up-to-date **threats inventory**.

Vulnerabilities

1. Login to RITA
2. Click on the "**Vulnerabilities**" menu item on the **navigation panel**
3. Click on the "New" button and populate the required information that is grouped into logical areas, namely "Basic Information", and "Threats":
   - In the "Basic information" area provide the code and a name for the vulnerability.
   - In the "Threats" area select the threats that are exploiting this vulnerability.
   - Finally, click the "Save" button.


Vulnerability

Edit Vulnerability **Possibility of creating or modifying system commands**

Basic Information

Fill Vulnerability's Basic Information

Code

VU-OS-37

* Required Field

Name

Possibility of creating or modifying system commands

* Required Field

Threats

Populate Threats Exploiting This Vulnerability

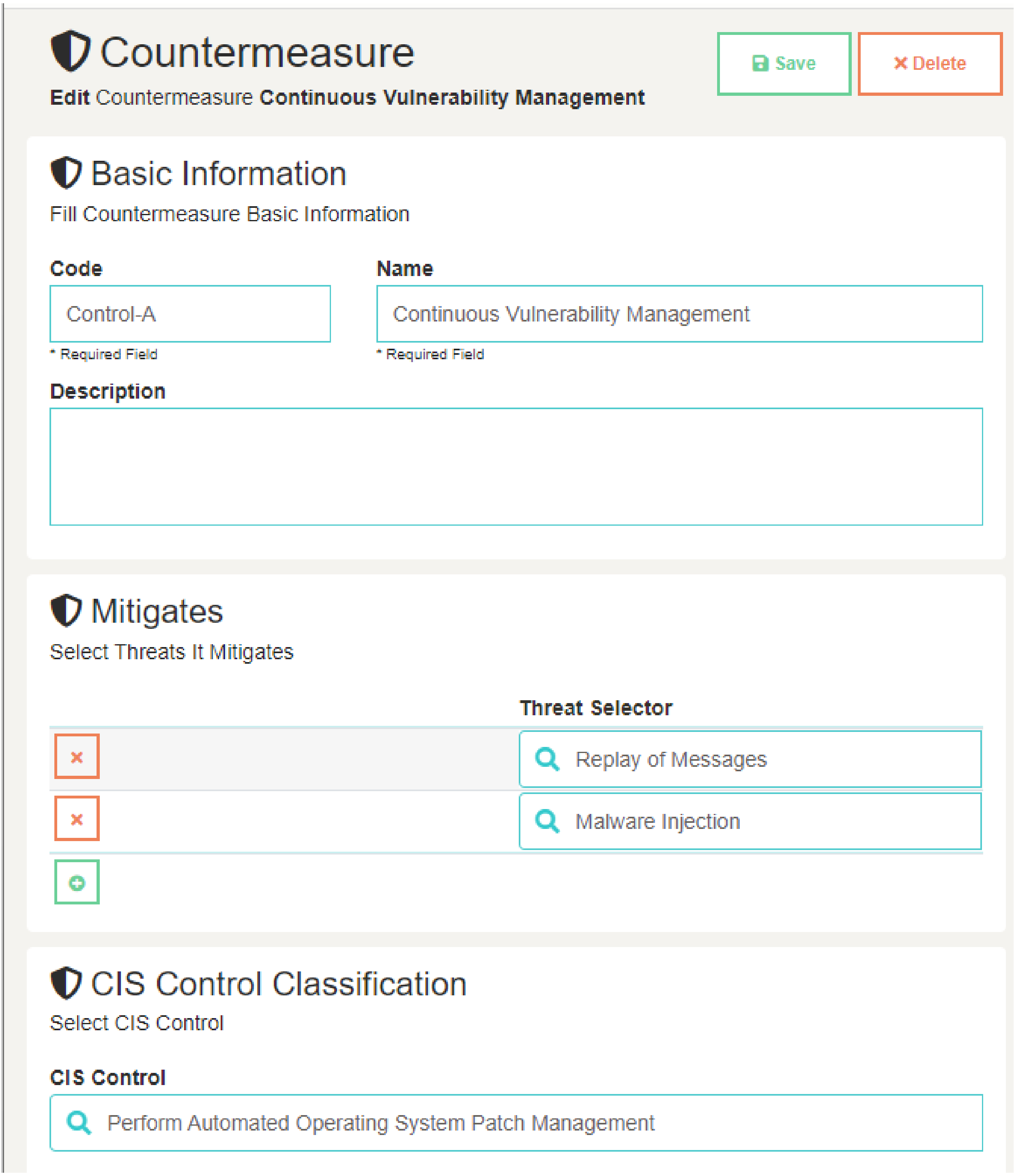
Threat

TH-11 Software Exploitation / Maliciou

Vulnerability repository, is populated with new entries as the system is used, enabling the NG-SOC platform users to maintain a dynamic and up-to-date **vulnerability inventory**.

Countermeasures

1. Login to RITA
2. Click on the “**Countermeasures**” menu item on the **navigation panel**
3. Click on the “New” button and populate the required information that is grouped into logical areas, namely “Basic Information”, “Mitigates” and “CIS Control Classification”:
    - In the “Basic information” area provide the code, name and description of the countermeasure.
    - In the “Mitigates” area select the threats that are mitigated by the countermeasure, using the “threat selector”.
    - Finally, in the “CIS Control Classification” area select the CIS control that are mapped to this countermeasure.
    - Finally, click the “Save” button.



Countermeasure

Edit Countermeasure **Continuous Vulnerability Management**

Basic Information

Fill Countermeasure Basic Information

Code: Control-A

* Required Field

Name: Continuous Vulnerability Management

* Required Field

Description

Mitigates

Select Threats It Mitigates

	Threat Selector
×	Replay of Messages
×	Malware Injection

CIS Control Classification

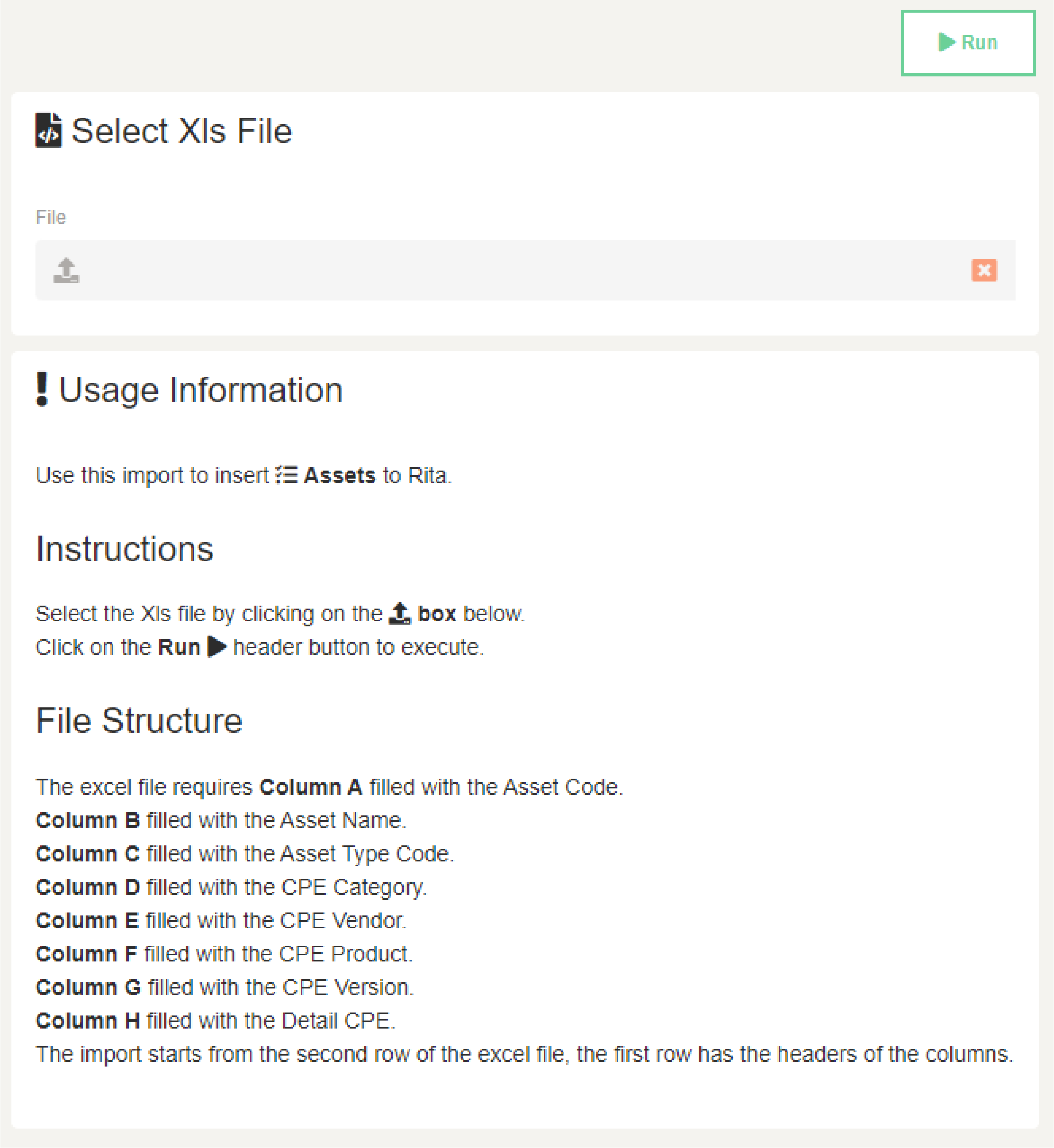
Select CIS Control

CIS Control: Perform Automated Operating System Patch Management

Countermeasure repository, is populated with new entries as the system is used, enabling the NG-SOC platform users to maintain a dynamic and up-to-date **countermeasure inventory**.

Import Assets

1. Login to RITA
2. Click the "**Assets**" menu item on the **Navigation panel**.
3. Click on the "Import" button, select the MS Office Excel file to upload, and then click the "Run" button.



Select Xls File

File

Usage Information

Use this import to insert **Assets** to Rita.

Instructions

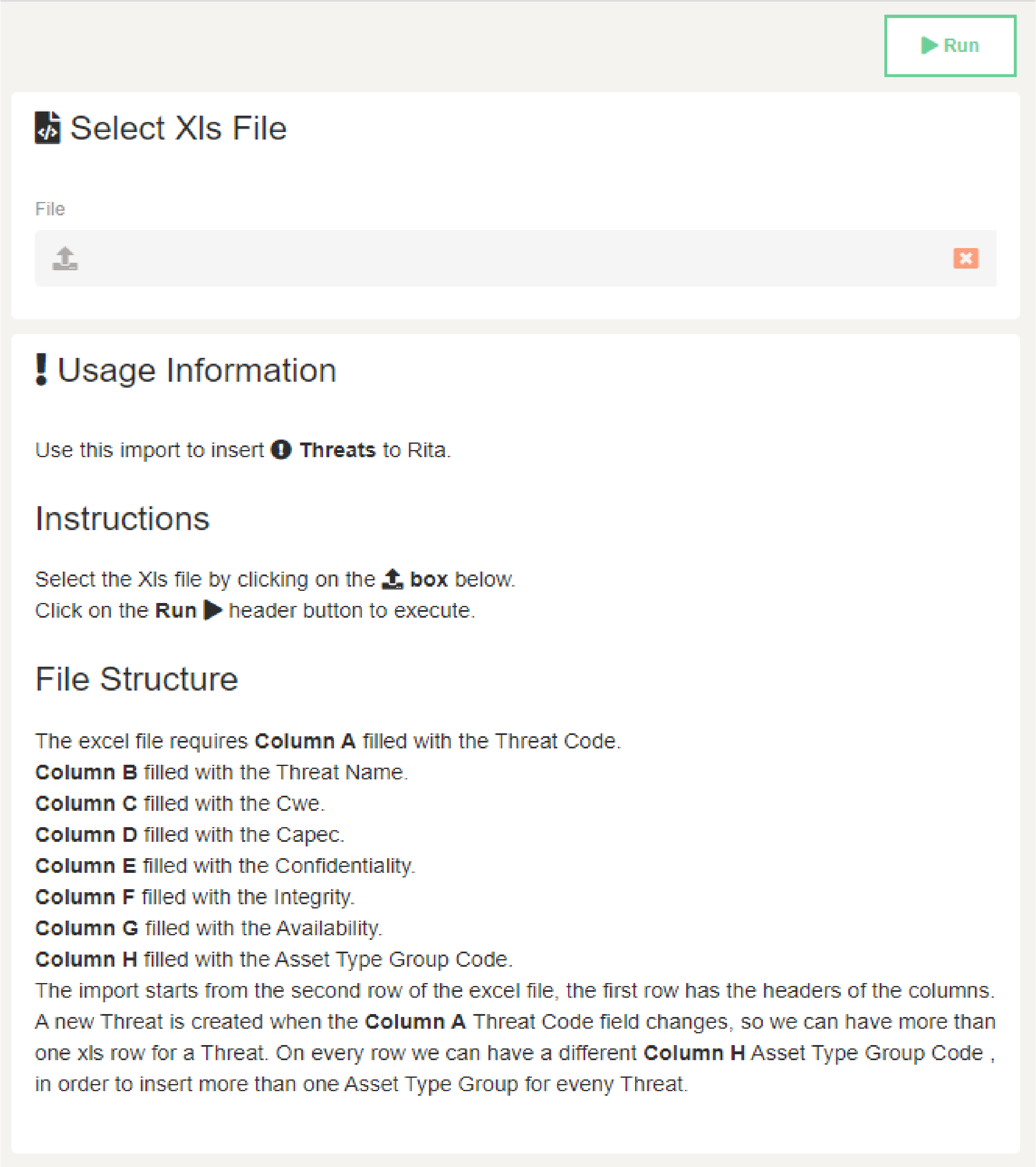
Select the Xls file by clicking on the **box** below.
Click on the **Run** ▶ header button to execute.

File Structure

The excel file requires **Column A** filled with the Asset Code.
Column B filled with the Asset Name.
Column C filled with the Asset Type Code.
Column D filled with the CPE Category.
Column E filled with the CPE Vendor.
Column F filled with the CPE Product.
Column G filled with the CPE Version.
Column H filled with the Detail CPE.
The import starts from the second row of the excel file, the first row has the headers of the columns.

Import Composite Assets

1. Login to RITA
2. Click the "**Composite Assets**" menu item on the **Navigation panel**.
3. Click on the "Import" button, select the MS Office Excel file to upload, and then click the "Run" button.



Select Xls File

File

Usage Information

Use this import to insert **Threats** to Rita.

Instructions

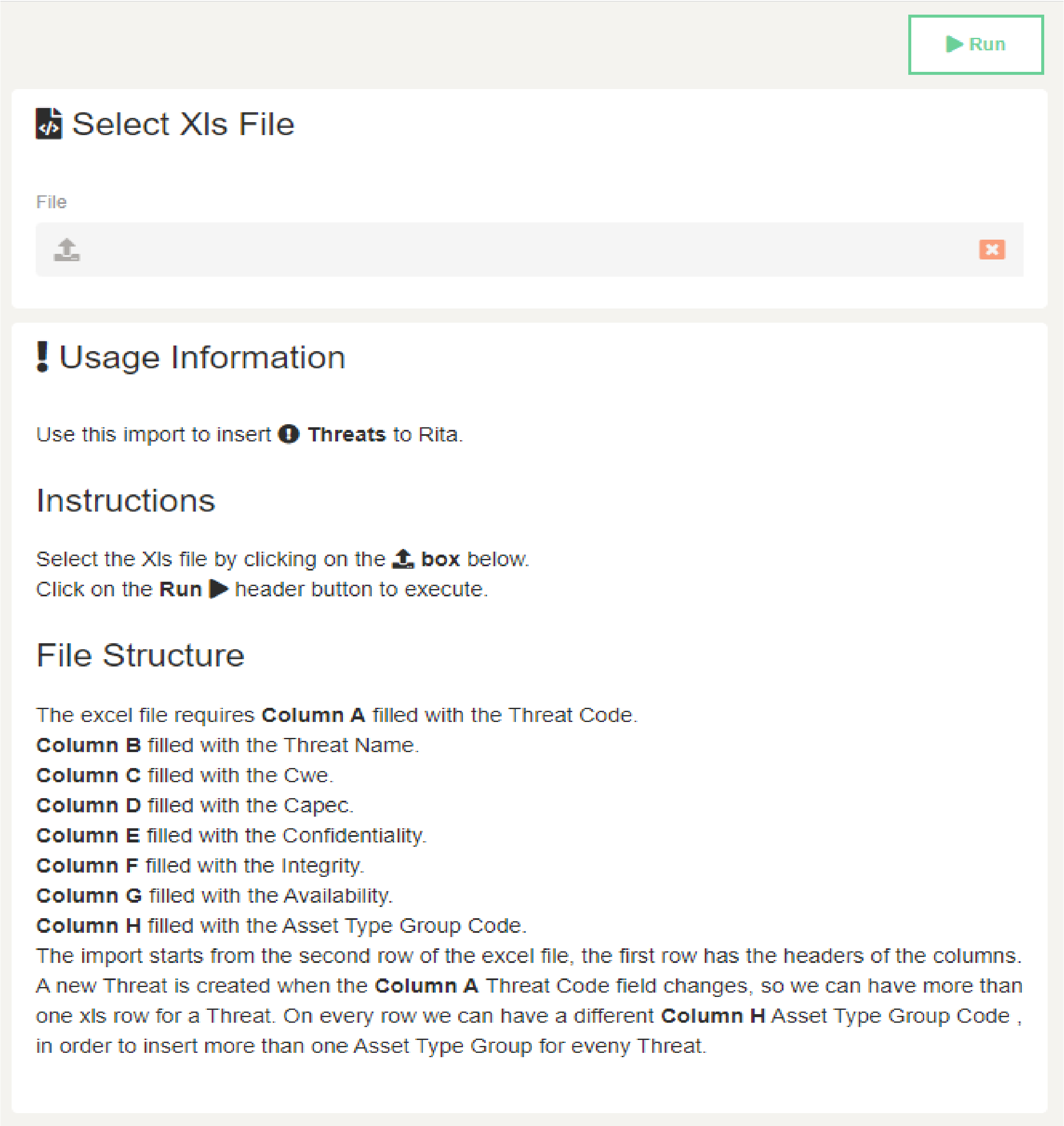
Select the Xls file by clicking on the **box** below.
Click on the **Run** ▶ header button to execute.

File Structure

The excel file requires **Column A** filled with the Threat Code.
Column B filled with the Threat Name.
Column C filled with the Cwe.
Column D filled with the Capec.
Column E filled with the Confidentiality.
Column F filled with the Integrity.
Column G filled with the Availability.
Column H filled with the Asset Type Group Code.
The import starts from the second row of the excel file, the first row has the headers of the columns.
A new Threat is created when the **Column A** Threat Code field changes, so we can have more than one xls row for a Threat. On every row we can have a different **Column H** Asset Type Group Code , in order to insert more than one Asset Type Group for eveny Threat.

Import Threats

1. Login to RITA
2. Click the “**Threats**” menu item on the **Navigation panel**.
3. Click on the “Import” button, select the MS Office Excel file to upload, and then click the “Run” button



Select Xls File

File

! Usage Information

Use this import to insert ❗ **Threats** to Rita.

Instructions

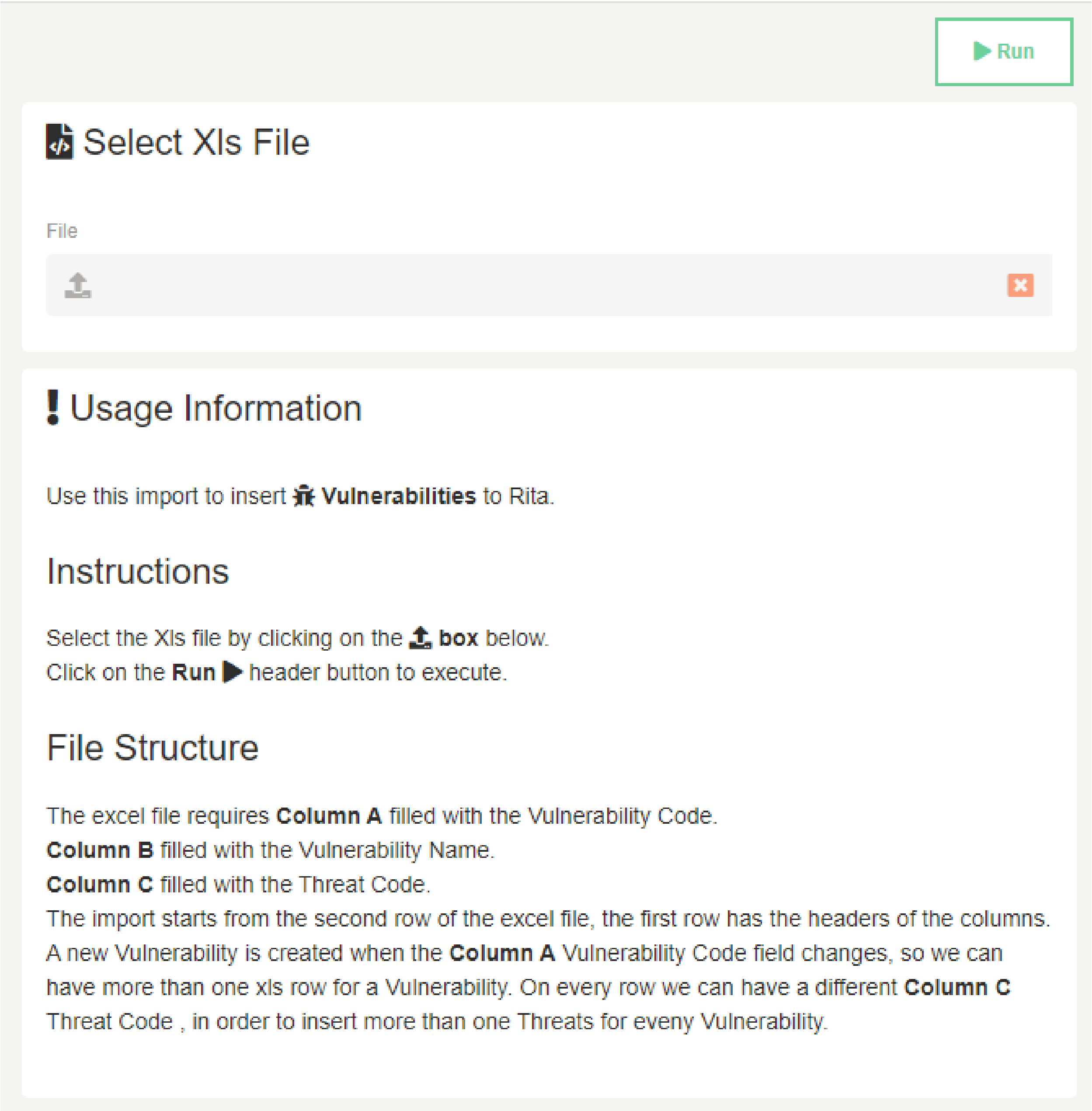
Select the Xls file by clicking on the ⬆ **box** below.
Click on the **Run** ▶ header button to execute.

File Structure

The excel file requires **Column A** filled with the Threat Code.
Column B filled with the Threat Name.
Column C filled with the Cwe.
Column D filled with the Capec.
Column E filled with the Confidentiality.
Column F filled with the Integrity.
Column G filled with the Availability.
Column H filled with the Asset Type Group Code.
The import starts from the second row of the excel file, the first row has the headers of the columns.
A new Threat is created when the **Column A** Threat Code field changes, so we can have more than one xls row for a Threat. On every row we can have a different **Column H** Asset Type Group Code , in order to insert more than one Asset Type Group for eveny Threat.

Import Vulnerabilities

1. Login to RITA
2. Click the “**Vulnerabilities**” menu item on the **Navigation panel**.
3. Click on the “Import” button, select the MS Office Excel file to upload, and then click the “Run” button.



Select Xls File

Usage Information

Use this import to insert 🐞 **Vulnerabilities** to Rita.

Instructions

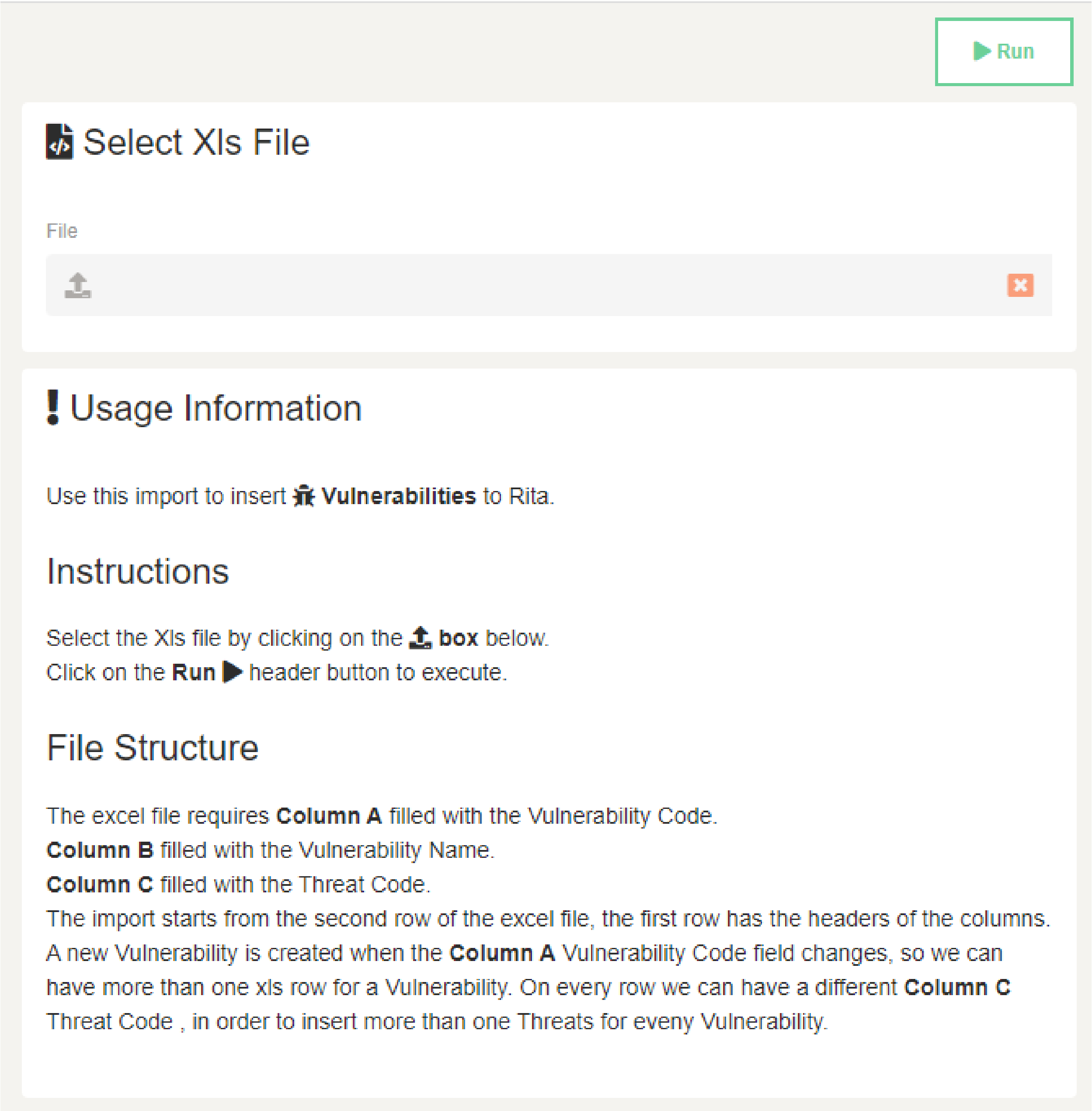
Select the Xls file by clicking on the ⬆ **box** below.
Click on the **Run** ▶ header button to execute.

File Structure

The excel file requires **Column A** filled with the Vulnerability Code.
Column B filled with the Vulnerability Name.
Column C filled with the Threat Code.
The import starts from the second row of the excel file, the first row has the headers of the columns. A new Vulnerability is created when the **Column A** Vulnerability Code field changes, so we can have more than one xls row for a Vulnerability. On every row we can have a different **Column C** Threat Code , in order to insert more than one Threats for eveny Vulnerability.

Import Countermeasures

1. Login to RITA
2. Click the "**Countermeasures**" menu item on the **Navigation panel**.
3. Click on the "Import" button, select the MS Office Excel file to upload, and then click the "Run" button.



Select Xls File

File

Usage Information

Use this import to insert **Vulnerabilities** to Rita.

Instructions

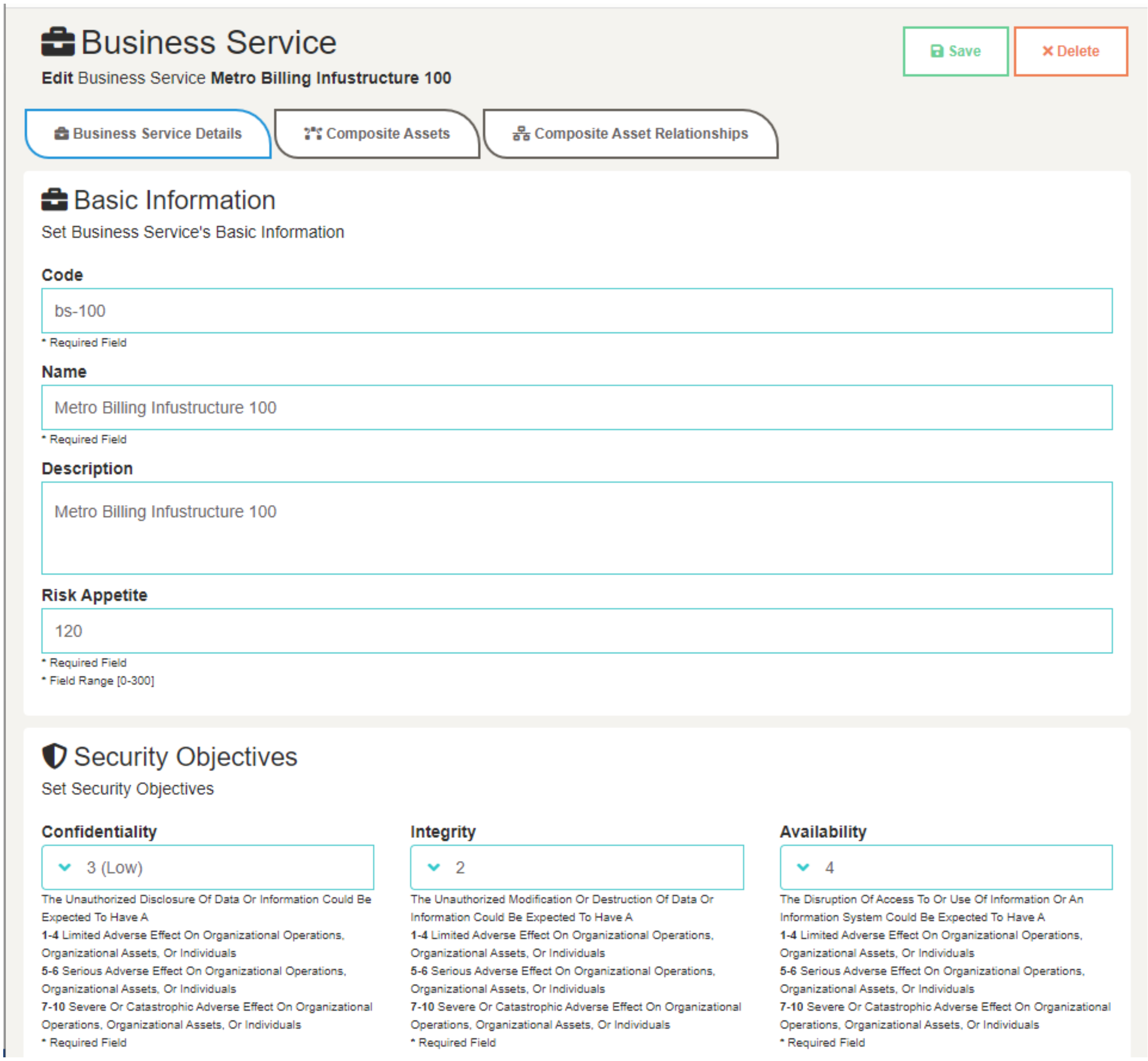
Select the Xls file by clicking on the ⬆ **box** below.
Click on the **Run** ▶ header button to execute.

File Structure

The excel file requires **Column A** filled with the Vulnerability Code.
Column B filled with the Vulnerability Name.
Column C filled with the Threat Code.
The import starts from the second row of the excel file, the first row has the headers of the columns.
A new Vulnerability is created when the **Column A** Vulnerability Code field changes, so we can have more than one xls row for a Vulnerability. On every row we can have a different **Column C** Threat Code , in order to insert more than one Threats for eveny Vulnerability.

Business Services

1. Login to RITA
2. Click the “**Business Services**” menu item on the **Navigation panel**.
3. Click on the “New” button and populate the required information that is grouped into two tabs, namely: the “Asset Details” and “Threats” tabs. The “Asset Details” tab groups’ information into logical tabs, namely the “Business Service Details”, “Composite Assets” and “Composite Asset Relationships”:
   - In the “Business Service Details” tab provide the business service information (code, name, description and risk appetite) and the service security objectives.
   - In the “Composite Assets” tab select the list of composite assets that are used to support the business service.
   - In the “Composite Asset Relationships” tab, as its name suggests, define the composite assets relationships.
   - Finally click the “Save” button
4. Click the “Play” icon that is shown next to the business service entry in the list of business services.
5. Click the “Run Assessment” button to execute the risk assessment.
6. Click the “chart-bar” icon, to obtain the details of the risk assessment.



Business Service

Edit Business Service **Metro Billing Infustructure 100**

Basic Information

Set Business Service's Basic Information

Code

bs-100

* Required Field

Name

Metro Billing Infustructure 100

* Required Field

Description

Metro Billing Infustructure 100

Risk Appetite

120

* Required Field
* Field Range [0-300]

Security Objectives

Set Security Objectives

Confidentiality

3 (Low)

The Unauthorized Disclosure Of Data Or Information Could Be Expected To Have A
1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
* Required Field

Integrity

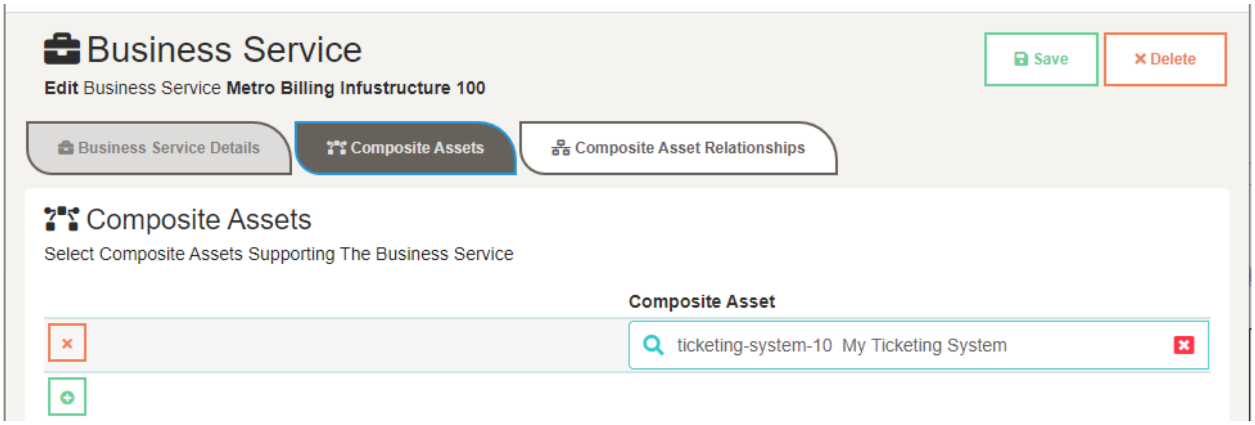
2

The Unauthorized Modification Or Destruction Of Data Or Information Could Be Expected To Have A
1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
* Required Field

Availability

4

The Disruption Of Access To Or Use Of Information Or An Information System Could Be Expected To Have A
1-4 Limited Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
5-6 Serious Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
7-10 Severe Or Catastrophic Adverse Effect On Organizational Operations, Organizational Assets, Or Individuals
* Required Field



Business Service

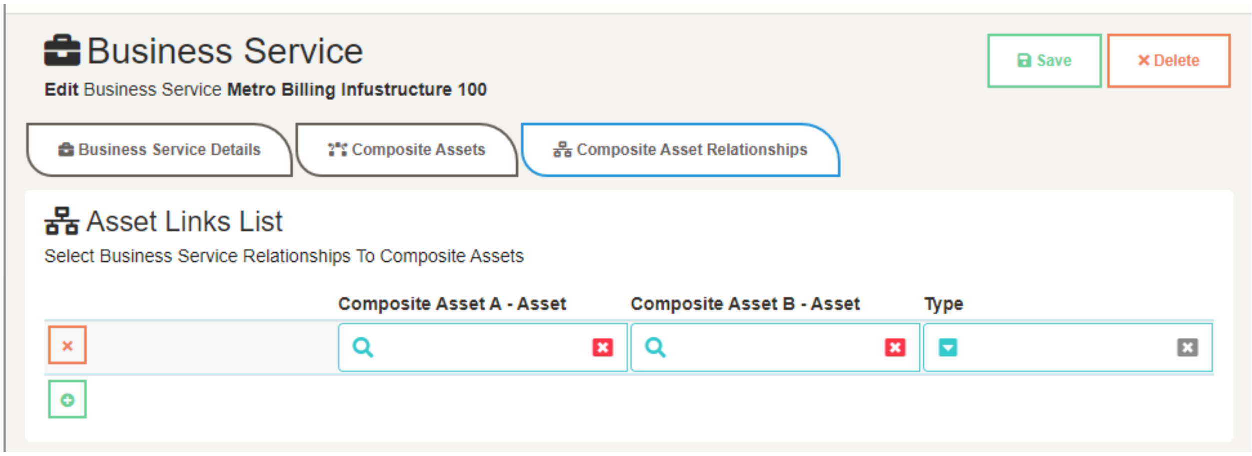
Edit Business Service **Metro Billing Infustructure 100**

Composite Assets

Select Composite Assets Supporting The Business Service

Composite Asset

ticketing-system-10 My Ticketing System



Business Service

Edit Business Service **Metro Billing Infustructure 100**

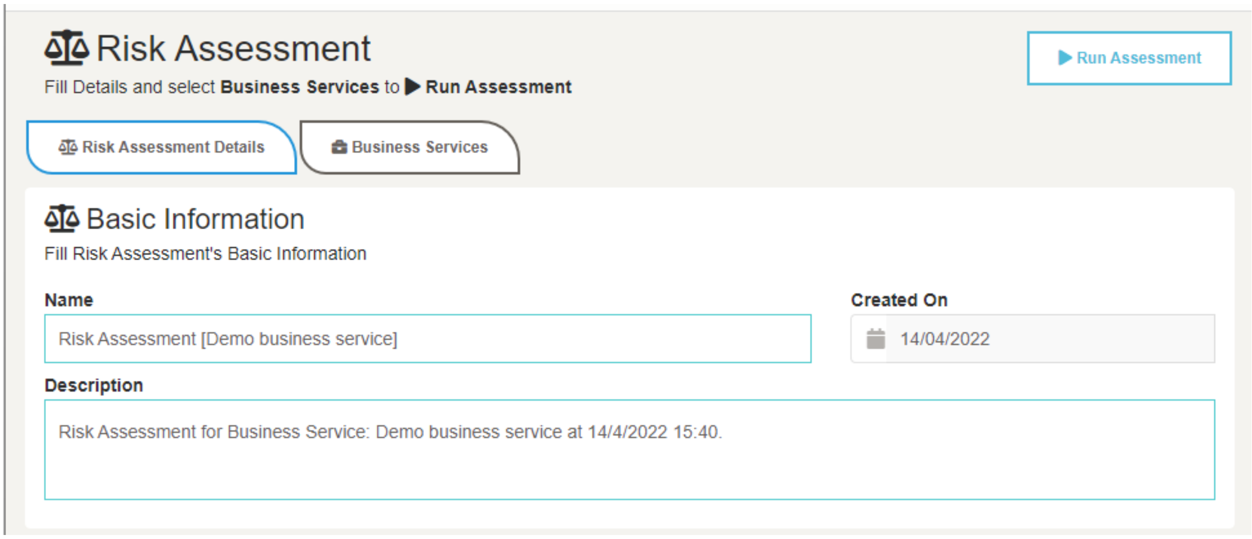
Asset Links List

Select Business Service Relationships To Composite Assets

Composite Asset A - Asset	Composite Asset B - Asset	Type

NG-SOC platform users can define the core business processes of the infrastructure that will be used for risk analysis based on:

- the business service security objectives,
- the threat likelihood for each identified/selected threat of each basic asset,
- vulnerability level for each identified vulnerability.



Risk Assessment

Fill Details and select **Business Services** to ▶ **Run Assessment**

Basic Information

Fill Risk Assessment's Basic Information

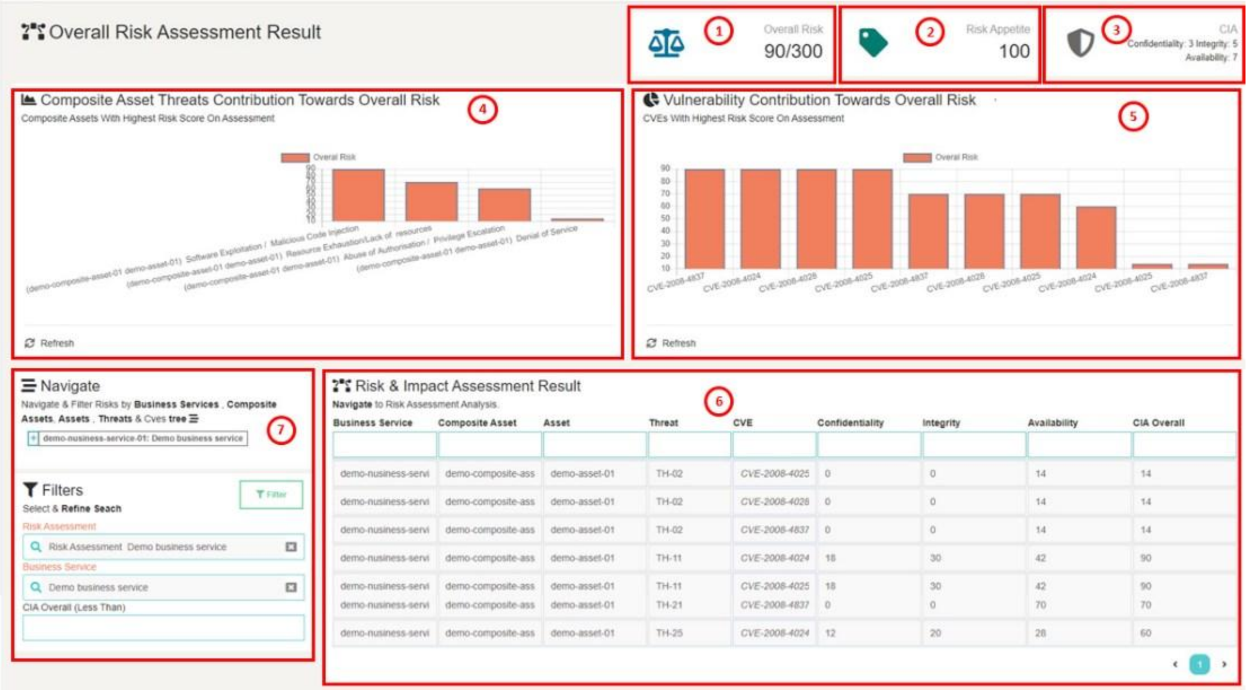
Name: Risk Assessment [Demo business service]

Created On: 14/04/2022

Description: Risk Assessment for Business Service: Demo business service at 14/4/2022 15:40.

1. As this is an asynchronous activity its progress is displayed on the **application toolbar**. When the risk modelling and analysis is done and risk values are calculated the user is presented with the new risk value result.
2. User is presented with the “Overall Risk Assessment Result” form that is organised into the following **dashlets**:

- **Overall risk** dashlet ① that presents the over risk value for the business service.
- The service **Risk Appetite** dashlet ② that presents the risk appetite that we have configured for that instance of the business service risk assessment.
- The service **Security Objectives (CIA)** dashlet ③ that presents the CIA values that we have configured for that instance of the business service risk assessment.
- Below, we are presented with two interactive bar-chart graphs:
  - The one on the left ④ presents the composite assets with the highest threat contribution towards the overall risk and
  - On the right ⑤ presents the vulnerabilities with the highest contribution towards the overall risk
- At the bottom of the page ⑥ we are presented with the full details of the risk assessment, based on the decomposition of a business service, to its composite assets, the assets that comprise the composite asset, the threats exposed, the identified vulnerabilities and their individual risk values per security objective.
  - Considering that this detailed report contains a lot of information, to ease navigation, we can use the quick filter functionality ⑦.


①
②
③
④
⑤
⑥
⑦
Overal Risk
90
80
70
60
50
40
30
20
10
(demo-composite-asset-01 demo-asset-01) Software Exploitation / Malicious Code Injection
(demo-composite-asset-01 demo-asset-01) Resource Exhaustion/Lack of resources
(demo-composite-asset-01 demo-asset-01) Abuse of Authorisation / Privilege Escalation
(demo-composite-asset-01 demo-asset-01) Denial of Service
Refresh
Overal Risk
90
80
70
60
50
40
30
20
10
CVE-2008-4837
CVE-2008-4024
CVE-2008-4028
CVE-2008-4025
CVE-2008-4837
CVE-2008-4028
CVE-2008-4025
CVE-2008-4024
CVE-2008-4025
CVE-2008-4837
Refresh
Filter
‹ 1 ›

Overall Risk Assessment Result

Overall Risk 90/300

Risk Appetite 100

CIA Confidentiality: 3 Integrity: 5 Availability: 7

Composite Asset Threats Contribution Towards Overall Risk

Composite Assets With Highest Risk Score On Assessment

Vulnerability Contribution Towards Overall Risk

CVEs With Highest Risk Score On Assessment

Navigate

Navigate & Filter Risks by **Business Services** , **Composite Assets**, **Assets** , **Threats** & Cves **tree**

+ demo-nusiness-service-01: Demo business service

Filters

Select & **Refine Seach**

Risk Assessment

Risk Assessment Demo business service

Business Service

Demo business service

CIA Overall (Less Than)

Risk & Impact Assessment Result

Navigate to Risk Assessment Analysis.

Business Service	Composite Asset	Asset	Threat	CVE	Confidentiality	Integrity	Availability	CIA Overall
demo-nusiness-servi	demo-composite-ass	demo-asset-01	TH-02	*CVE-2008-4025*	0	0	14	14
demo-nusiness-servi	demo-composite-ass	demo-asset-01	TH-02	*CVE-2008-4028*	0	0	14	14
demo-nusiness-servi	demo-composite-ass	demo-asset-01	TH-02	*CVE-2008-4837*	0	0	14	14
demo-nusiness-servi	demo-composite-ass	demo-asset-01	TH-11	*CVE-2008-4024*	18	30	42	90
demo-nusiness-servi	demo-composite-ass	demo-asset-01	TH-11	*CVE-2008-4025*	18	30	42	90
demo-nusiness-servi	demo-composite-ass	demo-asset-01	TH-21	*CVE-2008-4837*	0	0	70	70
demo-nusiness-servi	demo-composite-ass	demo-asset-01	TH-25	*CVE-2008-4024*	12	20	28	60

The NG-SOC platform users can visualize risk assessment information graphically on the web browser through an interactive user interface that presents and organizes information on **dashlets** that sit on their personal **dashboard**. Dashlets provide access to information in simple and clear fashion.