NISTIR 8272

Impact Analysis Tool for Interdependent Cyber Supply Chain Risks

Celia Paulsen
Jon Boyens
Jeffrey Ng
Kris Winkler
James Gimbi

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8272

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8272

Impact Analysis Tool for Interdependent Cyber Supply Chain Risks

Celia Paulsen
Jon Boyens
Computer Security Division
Information Technology Laboratory

Jeffrey Ng
Kris Winkler
James Gimbi
Boston Consulting Group
New York, NY

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8272

August 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8272
63 pages (August 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8272

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: scrm-nist@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

As awareness of cybersecurity supply chain risks grows among federal agencies, there is a greater need for tools that evaluate the impacts of a supply chain-related cyber event. This can be a difficult activity, especially for those organizations with complex operational environments and supply chains. A publicly available tool to support supply chain risk analysis that specifically takes into account the potential impact of an event does not currently exist. This publication describes how to use the Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool that has been developed to help federal agencies identify and assess the potential impact of cybersecurity events in their interconnected supply chains.

Keywords

C-SCRM; cyber supply chain risk management; risk management; secure supply chain; supply chain; supply chain assurance; supply chain dependencies; supply chain risk; supply chain risk management; supply chain security.

Acknowledgments

The authors, Jon Boyens (NIST), Celia Paulsen (NIST), Jeffrey Ng (Boston Consulting Group), Kris Winkler (Boston Consulting Group), and James Gimbi (Boston Consulting Group), would like to acknowledge and thank a number of individuals who provided valuable insights and helped to improve this publication. We would especially like to thank Nadya Bartol (Boston Consulting Group) for her contribution to the content during the document development and review, and Stuart Roth (Boston Consulting Group), David Bishop (Boston Consulting Group), and Kent Vasko (Boston Consulting Group) for their work on the design and development of the C-SCRM Interdependency Tool described in this document.

Document Conventions

Several of the terms used in this document are not intended to be definitive. Organizations may use different terms for the concepts described herein. For example, the term "projects" as used in this document may be better described as "missions" for some organizations or "business units" for others; "suppliers" may be called "partners," etc. Readers are encouraged to view these terms as flexible and descriptive rather than limiting. These terms can be customized in the Tool based on the preferred nomenclature (see Sec. 4.8).

When referencing any specific button, field, or text in the Tool, the text is displayed in `Courier New` font**.**

Supplemental Content

The source code for the tool described in this document, along with sample data and multiple installer packages are available on the project webpage at: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management/interdependency-tool.

The source code, sample data, and a windows installer are also available in the NIST GitHub library at https://github.com/usnistgov/supply-chain-interdependency-tool.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Relationship to Other Publications 1
1.3 Audience 2
1.4 Location of files 2
2 Tool Overview 3
2.1 Licensing 4
2.2 Use Case 4
2.3 Data Requirements 5
2.3.1 Sample Data 5
2.4 Security Advisory 5
3 Getting Started 6
3.1 System Requirements 6
3.2 Installing the Tool 6
3.3 Running the Tool 7
3.4 Uninstalling the Tool 8
3.5 Creating CSV Files 8
3.5.1 CSV File Requirements 8
3.5.2 CSV File Optional Fields 9
3.6 Importing CSV Files 9
3.6.1 Importing Updated CSV Files 10
3.6.2 Handling Import Errors 11
3.7 Completing Questionnaires 12
3.7.1 Using the Artificial Answer Generator 14
4 User Interface 16
4.1 Interface Overview 16
4.2 Dashboard 17
4.3 Suppliers 18
4.4 Products 20
4.5 Projects 22
4.6 Suppliers, Products, and Projects Questionnaires 24
4.7 Visualizations 25

4.7.1 Hierarchy 25
4.7.2 Candlestick 26
4.7.3 Scatterplots 27
4.8 Tool Menu 28
5 Results 30
5.1 Overview 30
5.2 Significant Nodes 30
5.3 *Impact Score*s 30
5.4 *Interdependence Scores* 31
5.5 *Assurance Score*s 31
6 Advanced Configuration 32
6.1 Overview 32
6.2 Question 32
6.3 Question Info Text 33
6.4 Weight 33
6.5 Answers 33
References 34

List of Appendices

Appendix A – Calculation 35
Appendix B – Question Categories 39
Appendix C – Calculation Example 45

List of Figures

Figure 1: Node relationship diagram 3
Figure 2: macOS Installation Window 6
Figure 3: Ubuntu Linux Install Message 7
Figure 4: Importing CSV files 9
Figure 5: Choosing file to import 10
Figure 6: Example of inactive supplier entry 11
Figure 7: Sample import error message 11

Figure 8: Accessing questionnaires 13
Figure 9: Accessing random answer generator 14
Figure 10: Generate random answers dialog box 14
Figure 11: Top navigation bar 16
Figure 12: Dashboard view 17
Figure 13: Suppliers detail view 18
Figure 14: Products detail view 20
Figure 15: Projects detail view 22
Figure 16: Questionnaire user interface 24
Figure 17: Hierarchy visualization 25
Figure 18: Candlestick visualization 26
Figure 19: Scatterplots visualization 27
Figure 20: Tool menu button 28
Figure 21: Tool menu 28
Figure 22: User preferences window 29
Figure 23: Calculation flow 35
Figure 24: Supply chain diagram for example scenario 46

List of Tables

Table 1: Import error codes 12
Table 2: Supplier Questions, Category, and Logic 39
Table 3: Product Questions, Category, and Logic 42
Table 4: Project Questions, Category, and Logic 44
Table 5: Suppliers CSV File Structure and Contents 45
Table 6: Products CSV File Structure and Contents 45
Table 7: Projects CSV File Structure and Contents 45
Table 8: Supplier Supply Line Breakdown 47
Table 9: Products Supply Line Breakdown 47
Table 10: Project Supply Line Breakdown 47

1 Introduction

1.1 Purpose

More organizations are becoming aware of the importance of identifying cybersecurity risks associated with extensive, complicated supply chains. Several solutions have been developed to help manage supply chains; most focus on contract management or compliance. There is a need to provide organizations with a systematic and more usable way to evaluate the potential impacts of cyber supply chain risks relative to an organization's risk appetite. This is especially important for organizations with complex supply chains and highly interdependent products and suppliers.

This publication describes one potential way to visualize and measure these impacts: a Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool (hereafter "Tool"), which is designed to provide a basic measurement of the potential impact of a cyber supply chain event. The Tool is not intended to measure the risk of an event, where risk is defined as a function of threat, vulnerability, likelihood, and impact. Research conducted by the authors of this publication found that, at the time of publication, existing cybersecurity risk tools and research focused on threats, vulnerabilities, and likelihood, but impact was frequently overlooked. Thus, this Tool is intended to bridge that gap and enable users and tool developers to create a more complete understanding of an organization's risk by measuring impact in their specific environments.

The Tool also provides the user greater visibility over the supply chain and the relative importance of particular projects, products, and suppliers (hereafter referred to as "nodes") compared to others. This can be determined by examining the metrics that contribute to a node's importance, such as the amount of access a node has to the acquiring organization's IT network, physical facilities, and data. By understanding which nodes are the most important in their organization's supply chain, the user can begin to understand the potential impact a disruption of that node may cause on business operations. The user can then prioritize the completion of risk mitigating actions to reduce the impact a disruption would cause to the organization's supply chain and overall business.

1.2 Relationship to Other Publications

NIST has published multiple documents regarding supply chain risk management.

- The criticality calculations used in this Tool are based on the methodology detailed in NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components* [NISTIR 8179].
- The Tool can be used to provide input relevant to NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [SP 800-161], to support supply chain risk assessment and mitigation activities.
- The Cybersecurity Framework Version 1.1 [NIST CSF] may be used to communicate an organization's risk profile, which can be used in conjunction with this tool to add *likelihood* and *vulnerability* information for a more holistic view of third-party risks.
- This project extends the work performed with the University of Maryland's Supply Chain Management Center to create the Cyber Risk Portal [UMD1] [UMD2].

1.3 Audience

The Tool is intended for organizations that are exploring ways to improve their supply chain risk management or third-party risk programs. It may be used by organizations to supplement their existing supply chain or third-party risk management capabilities or as a means to understand where to invest in more comprehensive risk management activities. It is not intended to be a stand-alone tool for the holistic management of supply chain risk.

Intended users of this Tool are individuals involved in supply chain management or corporate risk management functions. This includes cyber and supply chain/procurement practitioners who wish to analyze and assess cybersecurity risks in their organization's supply chain. The Tool may also be used by developers and researchers looking at ways supply chain cybersecurity impacts can be measured.

1.4 Location of files

The latest version of all files related to the Tool described in this IR document are located on the project webpage at: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management/interdependency-tool as well as in the NIST GitHub library, which can be found at: https://github.com/usnistgov/supply-chain-interdependency-tool.

2 Tool Overview

Cyber risk is commonly defined as a function of threat, vulnerability, likelihood, and impact, but current cybersecurity risk tools mainly focus on threats, vulnerabilities, and likelihood. The Tool measures the relative impact of potential supply chain disruptions, allowing the user to identify highly impactful and interdependent nodes where focused risk-mitigating controls may need to be applied.

For the purposes of this publication, the terms suppliers, products, and projects were chosen to characterize a simple supply chain. Projects are individual functions, missions, or lines of business in an organization. Each project may utilize one or more information technology or operational technology (IT/OT) products. Products are provided by one or more suppliers. This relationship is depicted in Figure 1.

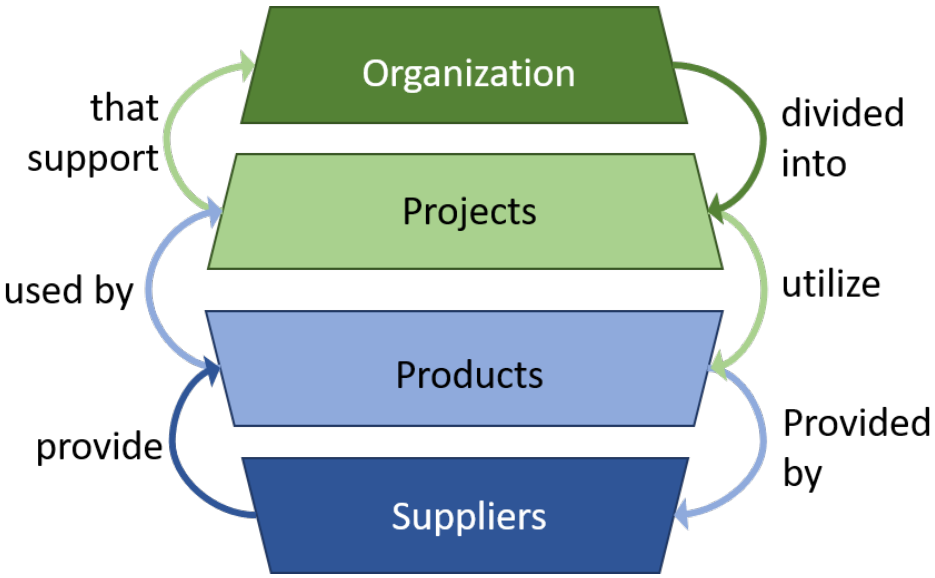

Figure 1: Node relationship diagram

To measure the relative impact of potential supply chain disruptions, the Tool analyzes:

- basic information about the structure of an organization's supply chain;
- the degree of access that products and suppliers have to the organization's assets;
- the organization's dependence on particular first-tier suppliers, and
- the criticality level of the products and projects.

Each node is given an *Impact Score*, an *Interdependence Score*, and an *Assurance Score* (see Sec. 5 for more information) with illustrative visualizations to assist in the identification of high-impact nodes. The Tool runs locally on the user's machine, granting the user complete control over the data and algorithms used by the Tool.

2.1 Licensing

The software associated with this publication was developed at the National Institute of Standards and Technology (NIST) in whole or in part by employees of the Federal Government in the course of their official duties and is being made available as a public service. For portions not authored by NIST employees, NIST has been granted unlimited rights. Pursuant to title 17 United States Code Section 105, works of NIST employees are not subject to copyright protection in the United States. This software may be subject to foreign copyright. Permission in the United States and in foreign countries, to the extent that NIST may hold copyright, to use, copy, modify, create derivative works, and distribute this software and its documentation without fee is hereby granted on a non-exclusive basis, provided that this notice and disclaimer of warranty appears in all copies.

THE SOFTWARE ASSOCIATED WITH THIS PUBLICATION IS PROVIDED 'AS IS' WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THE SOFTWARE WILL CONFORM TO SPECIFICATIONS, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND FREEDOM FROM INFRINGEMENT, AND ANY WARRANTY THAT THE DOCUMENTATION WILL CONFORM TO THE SOFTWARE, OR ANY WARRANTY THAT THE SOFTWARE WILL BE ERROR FREE. IN NO EVENT SHALL NIST BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THIS SOFTWARE, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE SOFTWARE OR SERVICES PROVIDED HEREUNDER.

2.2 Use Case

The Tool can be used in conjunction with existing risk tools used by the organization. For example, once highly impactful and interdependent nodes are identified, risk modelling tools can be used to more closely examine the threat, vulnerability, and likelihood components of cyber supply chain risk. This Tool can be used with other tools that map the supply chain to create a more accurate picture of the risk of sub-suppliers. It can also be used to complement governance, risk, and compliance (GRC) tools used by the organization.

Users (e.g., organizations and developers) are encouraged to modify this Tool as they see fit to integrate information from existing sources such as an accounting system or supplier management portal. Users may also integrate the concepts and ideas presented herein or portions of the source code of this Tool into their existing systems.

2.3 Data Requirements

The Tool requires two types of user input:

1. **CSV files:** The user is required to import three comma-separated value (CSV) files into the Tool, each detailing relationships between nodes. Sec. 3.5 provides information on creating and using these CSV files.
2. **Questionnaires:** The user is required to complete a questionnaire for each node within the Tool. Sec. 3.7 provides information about completing the questionnaires, and Sec. 4.6 provides information about the questionnaire user interface.

2.3.1 Sample Data

Users may test the Tool with sample data sets available here: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management/interdependency-tool or here: https://github.com/usnistgov/supply-chain-interdependency-tool. The sample data sets include:

1. **Sample Data Set – Basic:** Three CSV files that provide a good starting point for trying out the Tool. This data set contains a single project and a series of simple product and supplier supply lines.
2. **Sample Data Set – Interconnected:** Three CSV files that provide more complicated supply lines. This data set contains four projects and more complex node relationships.

2.4 Security Advisory

The Tool does not contain any security mechanisms (e.g., password protection) to protect the data contained within. All data imported and created during the use of this Tool is stored locally on the user's file system and is not encrypted or otherwise protected by the Tool. The Tool and related data need to be treated with care as supply chain data may be sensitive for an organization.

3 Getting Started

This section describes how to install, run, and uninstall the Tool.

3.1 System Requirements

The Tool was developed for use on Microsoft Windows 10, Apple macOS Mojave, or Ubuntu. The Tool may function on other versions of Windows, Mac, and Linux operating systems, but other versions have not been tested. Updates to the tool to ensure continued compatibility with various operating systems is not guaranteed.

The user is required to create CSV files as input to the Tool and may require a spreadsheet editor, such as Microsoft Excel, or a text editor, such as Notepad, nano, or vi. The user is advised to have at least 200 MB of available space on the file system.

3.2 Installing the Tool

The latest stable version of the Tool is v1.0.0. Binary releases for each platform and other information related to the Tool can be found at the following sites: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management/interdependency-tool or https://github.com/usnistgov/supply-chain-interdependency-tool. Select the appropriate download for the computer's operating system.

On Microsoft Windows systems, double click the file "`C-SCRM-Installer.exe`" downloaded either from the project webpage or GitHub.

On Apple Macintosh systems, double click the .dmg file, and drag the C-SCRM application icon to the "Applications" folder as shown in Figure 2.

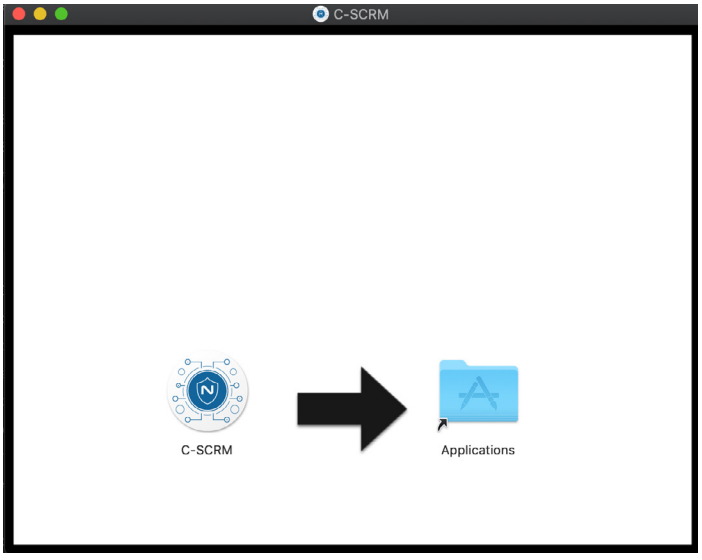

Figure 2: macOS Installation Window

On Linux systems, exact installation steps vary based on distribution and configuration. The binary distributions located on the project webpage include both a Debian package file for Ubuntu (`c-scrm_1.0.0_amd64.deb`) and a tar (`.tar.gz`) file for use with other distributions. When downloading and running the Debian package on Ubuntu, a window similar to that in Figure 3 may appear. Click the "`Install`" button to install the Tool.

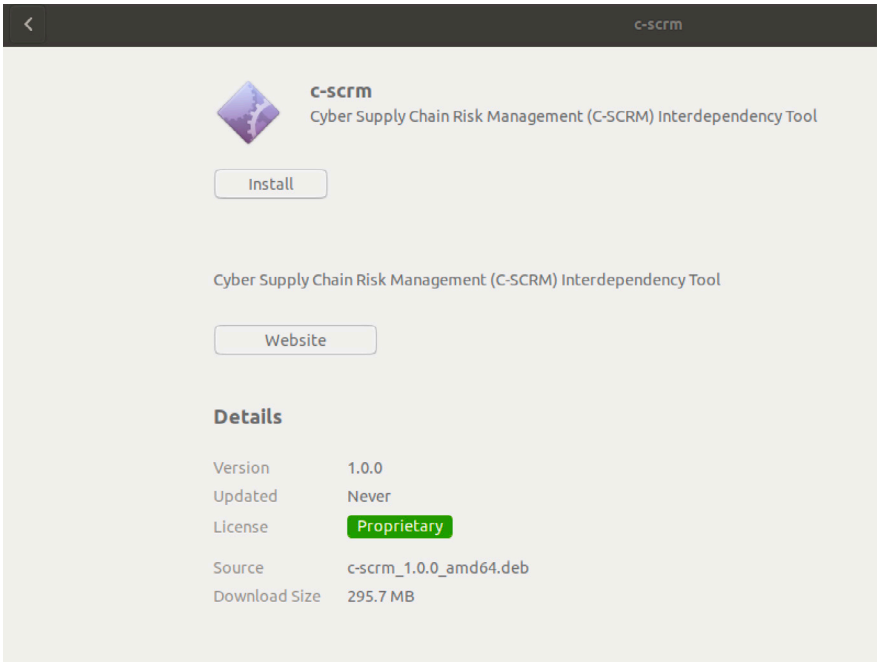

Figure 3: Ubuntu Linux Install Message

3.3 Running the Tool

On Microsoft Windows systems, the user can access the Tool by searching for "`C-SCRM`" in All Applications. All Applications can be accessed by clicking the Windows icon in the toolbar, which is located on the far left of the toolbar. The Tool can then be run by double-clicking the "`C-SCRM`" result. The Tool can also be run directly by double-clicking the "`C-SCRM`" shortcut added by the installer to the desktop. Files used to run the Tool are stored at `C:\Users\[Your User Name]\AppData\Local\C-SCRM`.

On Apple Macintosh systems, the Tool can be accessed by searching for "`C-SCRM`" in Spotlight (located in the upper right corner), or locating "`C-SCRM`" in the Applications folder. The Tool can then be run by double-clicking the "`C-SCRM`" search result in Spotlight or the "`C-SCRM`" row or icon in the Applications folder.

On Ubuntu Linux systems, the Tool can be accessed in the `/usr/share/applications` folder. The Tool can then be run by double-clicking the "`C-SCRM`" application in the folder or directly from the desktop when "`Show Applications`" is selected.

3.4 Uninstalling the Tool

On Microsoft Windows systems, uninstall the Tool by navigating to `Settings > Apps & Features`, finding "`C-SCRM`", and choosing Uninstall. If running Windows in a domain environment, the data will be associated with the roaming profile and is required to be deleted manually. Navigate to `C:\Users\[Your User Name]\AppData\Local\C-SCRM` or `C:\Users\[Your User Name]\AppData\Roaming\C-SCRM`, move this directory to the `Recycle Bin`, and empty the `Recycle Bin`.

On Apple Macintosh systems, drag the installed Tool into the Trash. The folder containing the Tool's data can be found at `/Users/[Your User Name]/Library/Application Support/C-SCRM` and also needs to be deleted by right-clicking on the folder and selecting `Move to Trash` or dragging the directory into the `Trash`.

On Ubuntu Linux systems, if the Debian package is installed, uninstall the Tool from the terminal by running "`sudo dpkg -r c-scrm`." If installed from the tar file, remove the unarchived directory. The directory location when using Ubuntu is `/home/USERNAME/.config/C-SCRM`, but the exact location of the application data files may vary based on configuration and Linux version used.

3.5 Creating CSV Files

The tool is initially populated using comma-separated (CSV) files created by the user. Data in these files may come from a variety of sources, including accounting systems and vendor management tools, or be manually created by leveraging institutional knowledge. This section provides details on the three CSV files that are required to be imported. Sample template files are available (see Sec. 2.3.1) to provide an example of an acceptable file format based on the requirements described in Sec. 3.5.1.

3.5.1 CSV File Requirements

Three separate CSV files are required: one containing supplier information, one containing product information, and one containing project information. While any file name may be used, including the appropriate designation (e.g., "supplier," "product," or "project") in the file name may simplify the import process.

The CSV files are required to contain the required fields (also known as "column headings") outlined below. These fields are required to be included in the first row of each CSV file and spelled exactly as shown within the quotations:

1. **Required fields for Supplier CSV file**
   a. "`ID`" – Supplier ID, user's choice of alphanumeric value
   b. "`Name`" – Supplier Name
2. **Required fields for Product CSV file**
   a. "`ID`" – Product ID, user's choice of alphanumeric value
   b. "`Name`" – Product name

c. "`Supplier ID`" – ID of suppliers that supply this product. These values must match "`ID`" in the Supplier CSV file. If there are multiple suppliers, each entry is required to be separated by a semicolon (;).
d. "`Project ID`" – ID of projects that utilize this product. These values must match "`ID`" in the Project CSV file. If there are multiple projects, each entry is required to be separated by a semicolon (;).

3. **Required fields for Project CSV file**
   a. "`ID`" – Project ID, user's choice of alphanumeric value
   b. "`Level`" – Recommend assigning organizational unit value 'x', e.g. = '1', with associated projects assigned value = '1.x' where x is the project number (1.1, 1.2, 2.2, 2.3, etc.)
   c. "`Name`" – Project Name

Note: The `Product CSV` file is the only file that establishes the interrelationships for the supply chain (see 2c and 2d). It also defines the product nodes. The `Supplier CSV` and `Project CSV` files are only used to define the supplier and project nodes.

3.5.2 CSV File Optional Fields

Users may include arbitrary additional fields aside from those required above. These fields may contain additional node attributes, such as supplier phone and address. Sec. 4.6 details how these fields are displayed in the Tool.

3.6 Importing CSV Files

This section details how to import the CSV files into the Tool.

1. Start the Tool (see Sec. 3.3). Note the `IMPORT...` buttons, as shown in Figure 4

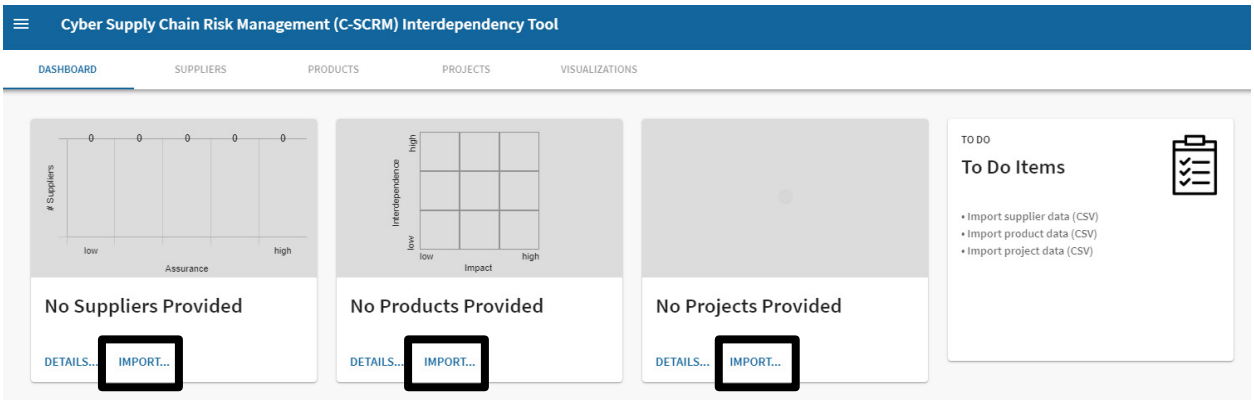

Figure 4: Importing CSV files

2. Click the `IMPORT...` buttons to import the CSV files for each node type (*Suppliers*, *Products*, and *Projects*). CSV files may be imported in any order.
   a. **Note**: Future versions of this Tool may support importing a single file that includes all node data.

3. For each node type (*Suppliers*, *Products*, and *Projects*), click `CHOOSE FILE...` as shown in Figure 5, and select the appropriate CSV file on the file system.

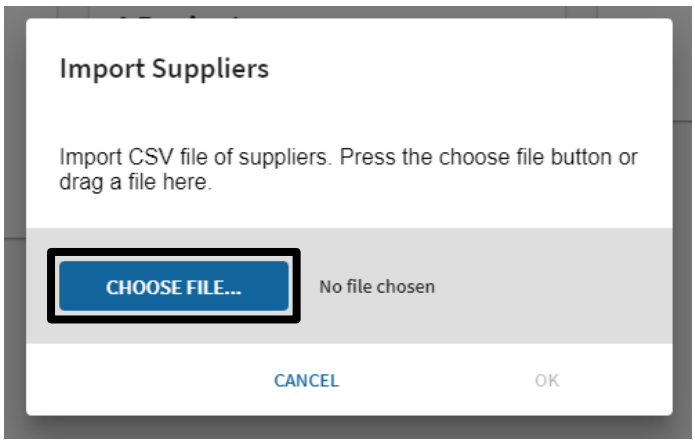

Figure 5: Choosing file to import

3.6.1 Importing Updated CSV Files

CSV files can be re-imported if updates are made to a data file (e.g., adding new nodes or changing column values in an existing node). To re-import an updated CSV file, click the `IMPORT...` button and select the new data file.

If updates are made to the name of an existing node and/or product connections, the visualizations and metrics can be updated to reflect this updated data. If a node is deleted, the entry is moved to "`inactive`" as shown in Figure 6. If, at a later point, a new CSV file is imported that contains the same ID as that of the previously deleted node, the table entry and the questionnaire data associated with that entry will be activated.

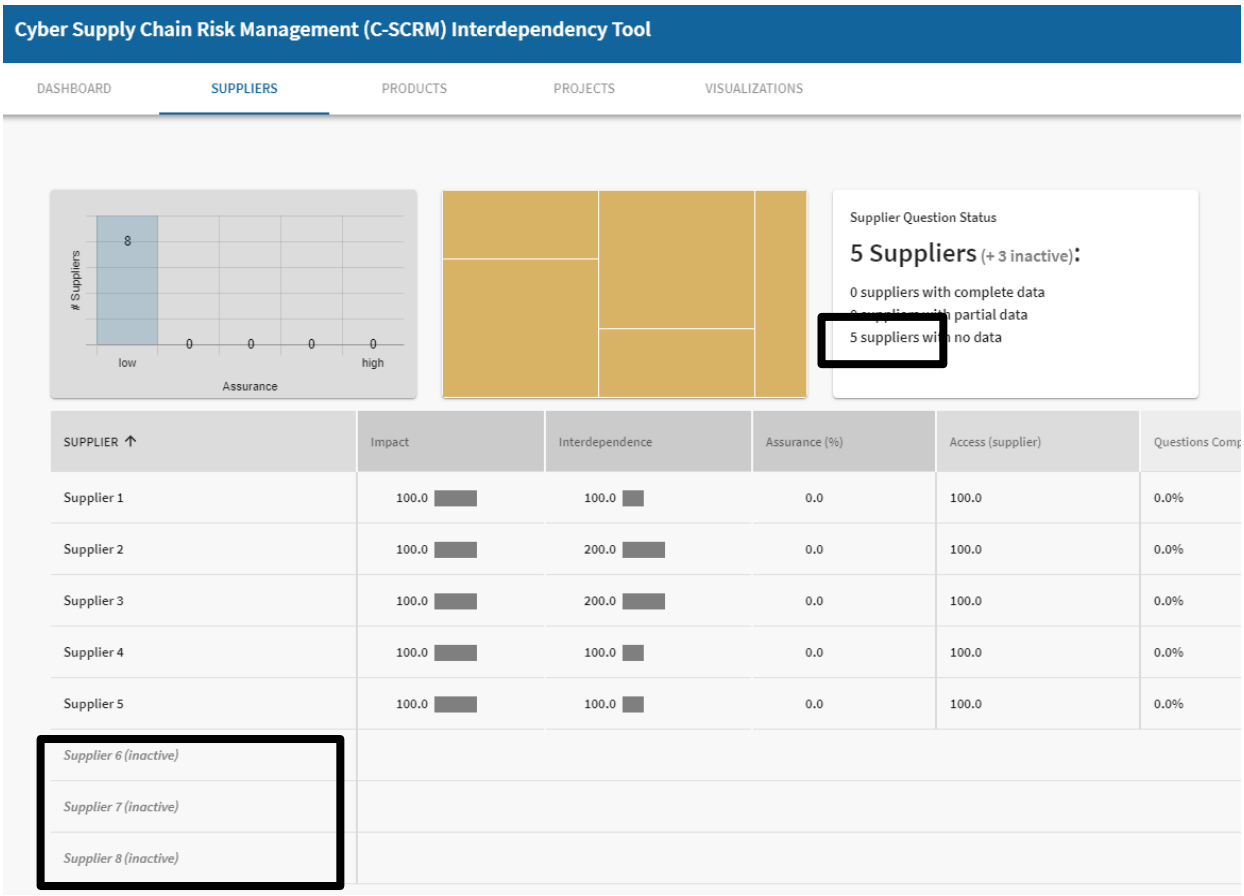

Figure 6: Example of inactive supplier entry

If a new node needs to be added, it must have a unique ID that has not been previously used to avoid inadvertent use of old data from an "`inactive`" entry.

3.6.2 Handling Import Errors

Data validation is performed on all imported files to ensure they meet the requirements outlined above in Sec. 3.5.1. Figure 7 shows a sample import error message.

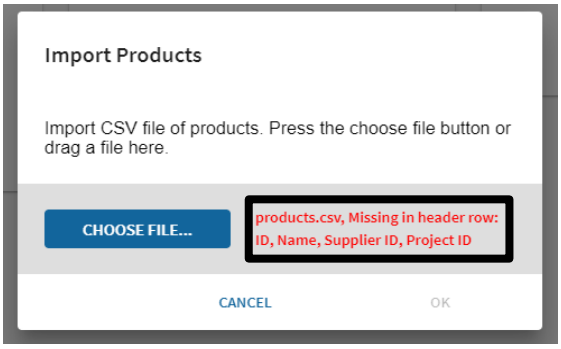

Figure 7: Sample import error message

Table 1 lists potential error messages and provides a description of how to interpret each error.

Table 1: Import error codes

Import Error Message Text	Import Error Description
`Missing in header row: [Missing column headings listed here]`	The first row is missing one or more of the required column headings. Check that all required fields are included in the first row of the file and spelled exactly as shown in Sec. 3.5.1.
`One or more rows missing these fields: [Column headings with missing fields listed here]`	One or more rows are missing data for the required columns listed above in Sec. 3.5.1. Check that there are no blank cells for any required columns in the spreadsheet selected for import.
`Import file rows cannot have duplicate IDs`	One or more rows have the same ID value in the ID column. Check the ID field to ensure that each row has a unique value in the ID field.
`IDs cannot contain the characters "|" or ";"`	Values in the ID column are best kept alphanumeric and specifically cannot contain the restricted characters "|" or ";". Check to ensure these characters are not in the ID column.
`One or more rows have duplicate relations in Supplier ID`	One or more rows have a duplicate ID separated by a semicolon in the Supplier ID field. For example, a value of "2;2" is invalid. The values separated by a semicolon are required to be unique.
`One or more rows have duplicate relations in Project ID`	One or more rows have a duplicate ID separated by a semicolon in the Project ID field. For example, a value of "2;2" is invalid. The values separated by a semicolon are required to be unique.

3.7 Completing Questionnaires

After importing the CSV files, the user must complete questionnaires for each individual node as shown in Figure 8. Currently, the questionnaire must be completed manually. Appendix B lists the questions in the questionnaire.

Note: In future versions, it may be possible to import answers to the questionnaires.

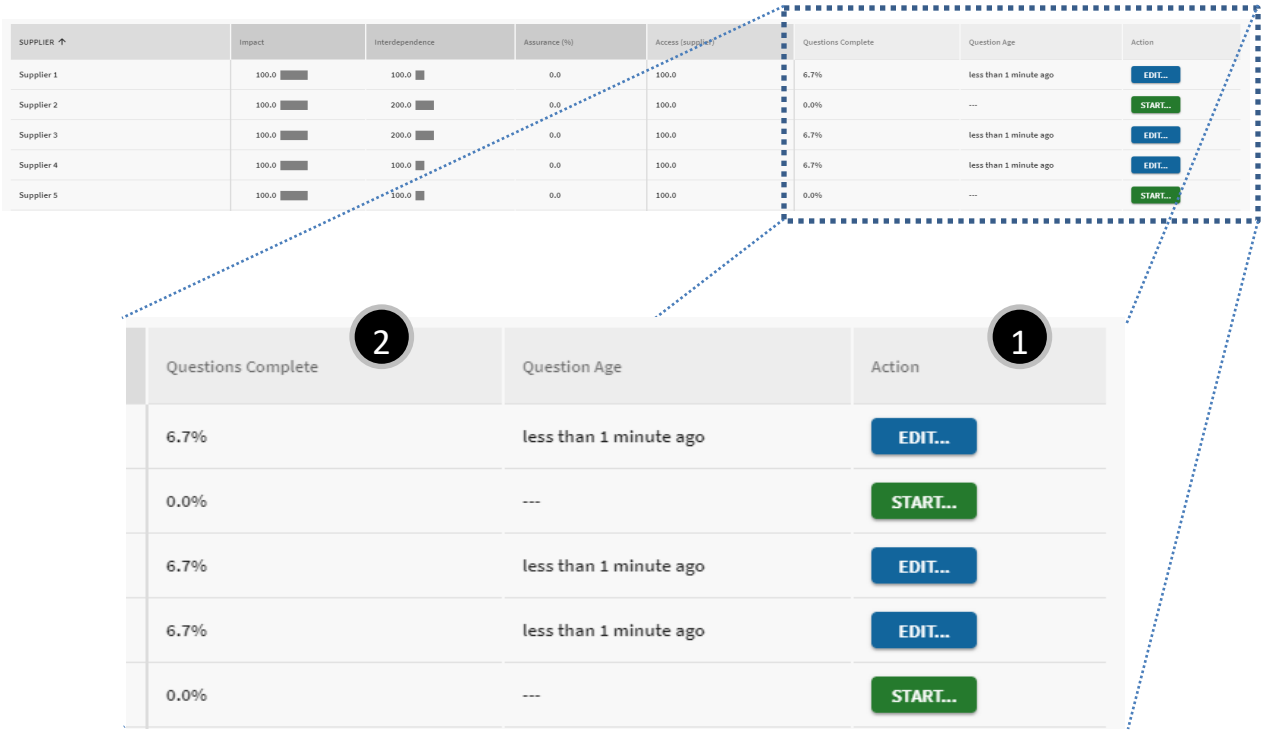

Figure 8: Accessing questionnaires

To access the questionnaires, click the *SUPPLIERS*, *PRODUCTS*, or *PROJECTS* view (see Sec. 4 below) towards the top of the Tool, and then click the START… button (see #1 in Figure 8). After completing the questionnaire to the extent possible, click SAVE…. The questionnaire does not need to be completed in order to produce results. However, the more complete the questionnaire is, the more accurate the calculated metrics are.

Once saved, the button in the *Action* column will now display EDIT… instead of START… (see Figure 8). The *Questions Complete* column indicates the percentage of questions that have been answered in the questionnaire. Any rows that do not contain the value "100%" in this column indicate the questionnaire is incomplete (see #2 in Figure 8). After all questionnaires are completed to the extent possible, the results are ready to be analyzed.

This questionnaire was developed based on subject matter experts' opinions and advice as well as existing supplier risk questionnaires. The questions in the questionnaire have been selected as the minimum information an organization needs to know about their suppliers, products, and processes in order to gain an understanding of the potential impact that a node may have. Many organizations have existing supplier questionnaires that differ from the questionnaire in this Tool. Those organizations are encouraged to compare their questionnaires with the one in this Tool and, where appropriate, update their questionnaire or modify this Tool to support their questionnaire. Instructions for how to modify the questionnaire contents and question weightings are in Sec. 6.

3.7.1 Using the Artificial Answer Generator

The Tool features a configurable artificial answer generator for testing purposes. This can simulate completion of the questionnaires and give the user an idea of a sample output from the Tool. Using this feature is only recommended when first learning to use this Tool. Once the user is familiar with the Tool, use of this feature is not recommended.

To generate random sample data for the questionnaires, click on the bottom right of the question status box (see #1 in Figure 9).

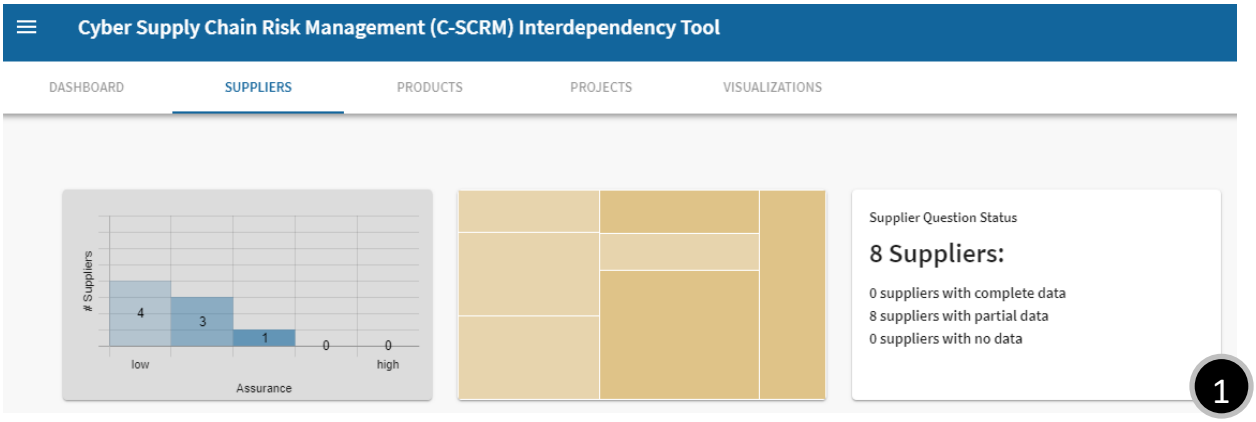

Figure 9: Accessing random answer generator

Clicking the question status box at this location allows the user to access the *Generate Random Answers* feature, as shown in Figure 10.

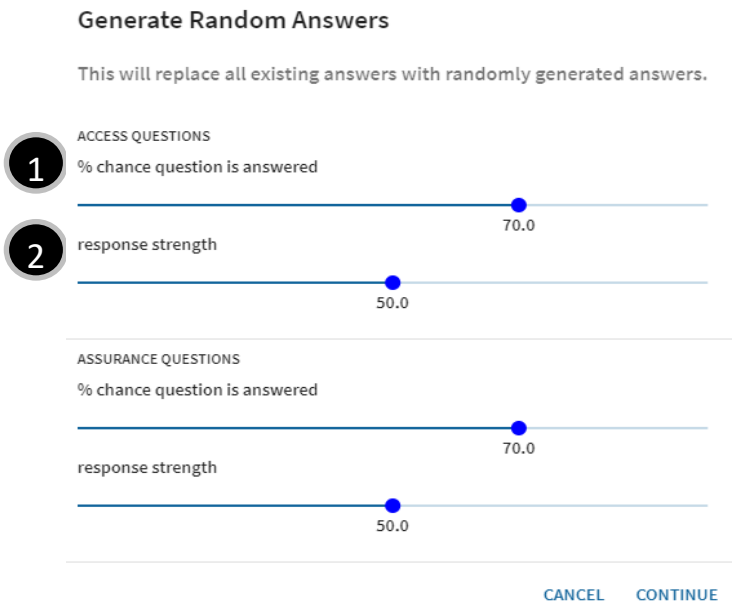

Figure 10: Generate random answers dialog box

The box is organized by question categories: *ACCESS*, *ASSURANCE*, *CRITICALITY*, and *DEPENDENCY* (see Appendix B for a listing of questions in each category). The following options are provided to generate random answers:

1. *% chance question is answered:* Drag the slider to set the average percentage of questions to be completed in a given questionnaire. For example, a value of 70.0 means approximately 70 % of questions in each questionnaire are answered (30 % of questions are left blank). Unanswered questions do not impact the score. Specifically, this means that the default assumption of the "worst-case scenario" applies to the unanswered question (e.g., highest criticality, access, dependency, and lowest assurance). See Sec. 5 for more information about how scores are calculated and this default assumption.

2. *Response strength*: Drag the slider to set the "strength" of the answer choices. A higher response strength translates to a better score. For example, a higher response strength value in the criticality category translates to a lower criticality score (indicating that the product or project is less critical); a higher response strength in the access category translates to a lower access score (indicating that the supplier/product has less access to acquirer's environment); a higher response strength in the dependency category translates to a lower dependency score (indicating that the acquirer has low dependency on the product); and a higher response strength in the assurance category translates to a higher assurance score (indicating that the acquirer has a high number of implemented mitigations for the supplier).

See Sec. 4 for more information about the questionnaire interface. See Sec. 5 for more information about how to analyze the results generated.

4 User Interface

This section describes how to identify, use, and interpret all components of the Tool.

4.1 Interface Overview

Figure 11 provides a screenshot of the top navigation bar in the user interface.

Figure 11: Top navigation bar

The Tool has five main views:

1. ***DASHBOARD*** – The dashboard provides a visual summary of the available Supplier, Product, and Project data. It also summarizes activities that need to be completed to provide more accurate information for the Tool to analyze.
2. ***SUPPLIERS*** – The *Suppliers* view shows information about the suppliers that provide products to the organization.
3. ***PRODUCTS*** – The *Products* view shows information about the products that the suppliers provide to the organization.
4. ***PROJECTS*** – The *Projects* view shows information about the projects or business units that utilize one or more products.
5. ***VISUALIZATIONS*** – The *Visualizations* view shows the interconnections between nodes as well as the significance and Interdependence of each node.

Please see Secs. 4.2 through 4.8 for more details about the user interface of each of these views.

4.2 Dashboard

Figure 12 provides a screenshot of the *Dashboard* view.

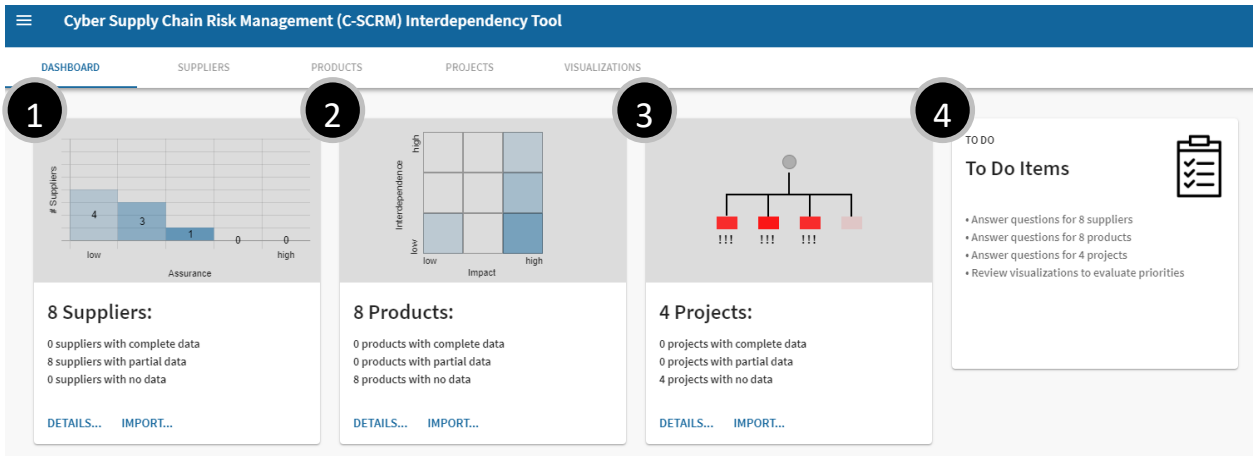

Figure 12: Dashboard view

There are four tiles on the Dashboard:

1. ***SUPPLIERS*** – The bar chart shows the distribution of the supplier *Assurance Scores* (see Sec. 5.5 for a description of *Assurance Scores*). Click the DETAILS... button to navigate to the *Suppliers* view. Click the IMPORT... button to import a Supplier CSV file.
2. ***Products*** – The heat map plots *Interdependence* on the *y-axis* and *Impact* on the *x-axis*. Products with the highest impact and exposure are located in the top right of the diagram. The darker colors indicate the number of products in a given category. In the example above, the bottom left-most box has a dark blue color, which means there are a large number of products that have low *Interdependence* and low *Impact* compared to other impact-interdependence combinations. Click the DETAILS... button to navigate to the *Products* view. Click the IMPORT... to import a Products CSV file.
3. ***Projects*** – The tree diagram represents each project as a rectangular box, and each box is colored by degree of *Impact* with the darker red colors indicating higher *Impact*. Click the DETAILS... button to navigate to the *Projects* view. Click the IMPORT... button to import a Projects CSV file.
4. ***To Do Items*** – The list of items in this box is populated based on the completeness of the information in the *Suppliers*, *Products*, and *Projects* views. Example tasks that may appear include importing node CSV files and completing node questionnaires.

4.3 Suppliers

Figure 13 provides a screenshot of the *Suppliers* detail view.

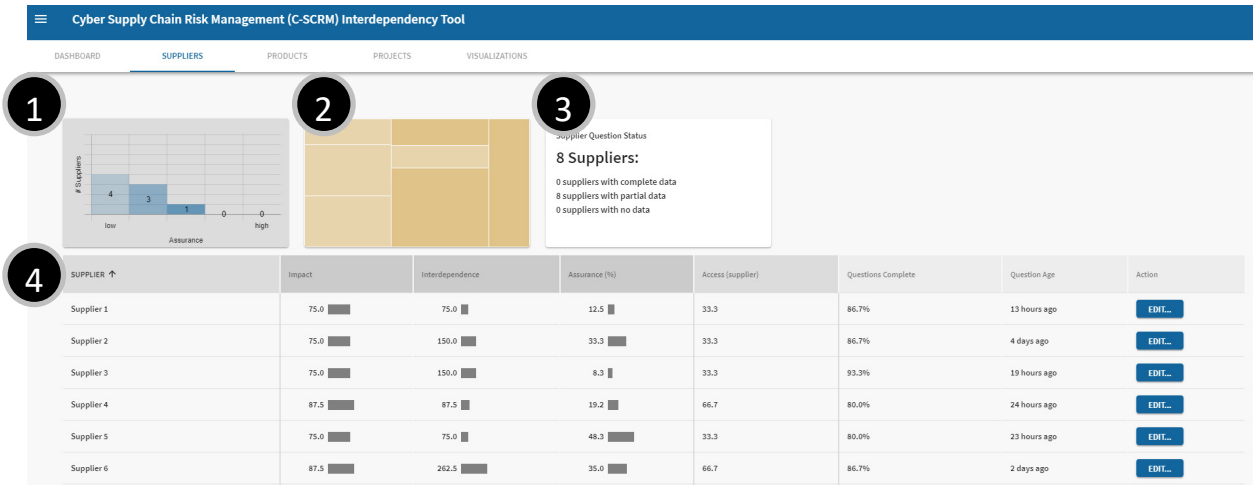

Figure 13: Suppliers detail view

The *Suppliers* view provides additional details about the suppliers that have been imported into the Tool and related metrics that have been calculated:

1. **Supplier Visualization** – Bar chart shows the distribution of supplier *Assurance Scores*.
2. **Heat Map** – Each box in the heat map is colored based on supplier *Impact* with red/purple/pink/brown denoting higher *Impact* and green/orange/blue denoting lower *Impact* (depending on the color scheme selected). See Sec. 4.8 for more information on how to modify the color scheme. The size of the box denotes supplier *Interdependence* with larger boxes indicating larger *Interdependence*.
    a. Get *Interdependence* and *Impact* values for each box in the heat map by hovering over a rectangle.
3. **Status Box –** Shows the total number of suppliers imported into the Tool and their statuses based on the number of questions answered in the supplier questionnaire (see #4f below).
4. **Supplier Table –** Lists suppliers and key metrics. Click on the column header to sort the table by that column's values in ascending or descending order. The dark gray columns (`Impact`, `Interdependence` and `Assurance`) are calculated columns, which means they are calculated based on information provided in the questionnaires across nodes. The light grey column (`Access (supplier)`) is derived directly from the associated supplier questionnaire and is not calculated from data in the *Product* or *Project* views.
    a. `Supplier` – Supplier name from imported data file.
    b. `Impact` – Indicates potential impact if supplier faces disruption. An *Impact* score ranges from 0 to 100, with a score of 100 translating to devastating impact and 0 translating to no impact. An *Impact* score is calculated by taking the maximum *Access* and *Dependency* scores for all supply lines the node is a part of (see Appendix A for calculation details).

c. `Interdependence` – Indicates influence of the supplier in the supply chain. *Interdependence Scores* are unbounded and are calculated by adding the `Dependency` and access scores for each supply line that node is a part of (see Appendix A for calculation details). Higher scores indicate greater *Interdependence*.
d. `Assurance (%)` – Indicates degree of supply chain risk management security mitigating actions/controls implemented by supplier. *Assurance Scores* range from 0 to 100 with 0 translating to the absence of any mitigating controls implemented. An *Assurance* score is calculated by averaging the *Assurance Scores* of each supplier that a node is related to (e.g., any supplier contained in a supply line that the node is a part of) (see Appendix A for calculation details).
e. `Access (supplier)` – *Supplier Access* scores indicates degree of access supplier has to the acquirer's sensitive assets (specifically systems, information and physical location). This score is calculated by taking the average score of the questions in the access Sec. of the questionnaire. *Access* scores range from 0 to 100 with 100 translating to complete access.
f. `Questions Complete` – Percentage of questions answered in supplier questionnaire.
g. `Question Age` – Length of time elapsed since product questionnaire has been edited.
h. `Action` – Contains the `SHOW...` or `EDIT...` button, which can be used to view/edit the questionnaire responses for a given project.

4.4 Products

Figure 14 provides a screenshot of *Products* detail view.

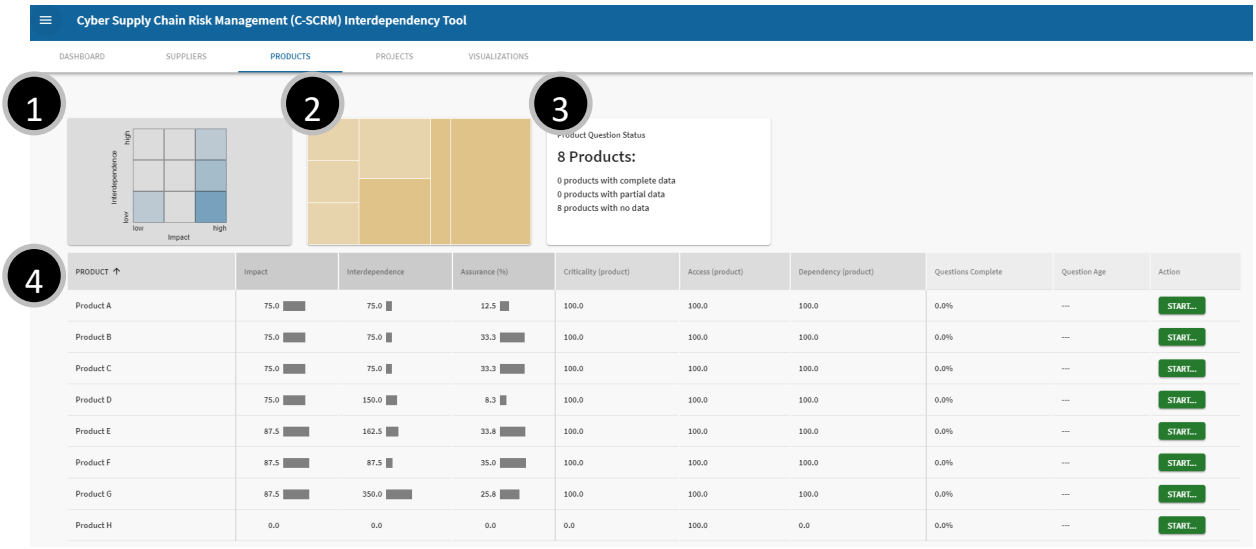

Figure 14: Products detail view

The *Products* view provides additional details about the products that have been imported into the Tool and related metrics that have been calculated:

1. **Products Visualization** – Matrix shows distribution of products' *Impact Score* and *Interdependence Score* with darker colors indicating more products in a given category. In the example above, the bottom right-most box has a dark blue color which means there are a large number of products that have low *Interdependence* and high *impact* compared to other impact-interdependence combinations
2. **Heat Map** - Each box is colored based on product *impact* with red/purple/pink/brown denoting higher *Impact* and green/orange/blue denoting lower *Impact* (depending on the color scheme selected). The size of the box denotes product *Interdependence* with larger boxes indicating larger *Interdependence*.
    a. Get *Interdependence* and *Impact* values for each box in the heat map by hovering over a rectangle.
3. **Status Box –** Shows the total number of products imported into the Tool and their statuses based on the number of questions answered in the products questionnaire (see #4h below).
4. **Products Table –** Lists products and key metrics. Click on the column header to sort the table by that column's value in ascending or descending order. The dark grey columns (`Impact`, `Interdependence`, and `Assurance`) are calculated based on information provided in the node questionnaires. The light grey columns (`Criticality (product)`, `Access (product)`, and `Dependency (product)`) are derived directly from the associated supplier questionnaire and is not calculated from data in the *Suppliers* or *Project* views.
    a. `Product` – Product name from imported data file.

b. `Impact` – Indicates potential impact to acquirer if supplier faces disruption. An *Impact Score* ranges from 0 to 100, with a score of 100 translating to devastating impact and 0 translating to no impact. An *Impact* score is calculated by taking the maximum *Access* and *Dependency* scores for all supply lines the node is a part of (see Appendix A for calculation details).
c. `Interdependence` – Indicates influence of the product in the supply chain. *Interdependence* scores are unbounded and are calculated by adding the *Dependency* and *Access* scores for each supply line that node is a part of (see Appendix A for calculation details). Higher scores indicate greater `Interdependence`.
d. `Assurance (%)` – Indicates degree of supply chain risk management security mitigating actions/controls implemented by suppliers providing a product. *Assurance* scores range from 0 to 100 with 0 translating to the absence of any mitigating controls implemented. *Assurance* scores are calculated by averaging the *Assurance* scores of each supplier that a node is related to (e.g., any supplier contained in a supply line that the node is a part of) (see Appendix A for calculation details).
e. `Criticality (product)` – Indicates how important product is to its associated projects. If the product is connected to more than one project, the project with the highest *criticality* value is displayed.
f. `Access (product)` – Indicates degree of access product has to the acquirer's sensitive assets (specifically, information and physical location). This score is calculated by taking the average score of the questions in the *access* category of the questionnaire. Scores range from 0 to 100 with 100 translating to complete access.
g. `Dependency (product)` – This column is equivalent to *Supplier Dependency* and indicates degree of dependence acquirer has on a supplier to supply the project with a given product. If the product is connected to more than one supplier, the supplier with the highest dependency value is displayed.
h. `Questions Complete` – Percentage of questions answered in product questionnaire.
i. `Question Age` – Length of time elapsed since product questionnaire has been edited.
j. `Action` – Contains the `SHOW…` or `EDIT…` button, which can be used to view/edit the questionnaire responses for a given project.

4.5 Projects

Figure 15 provides a screenshot of *Projects* detail view.

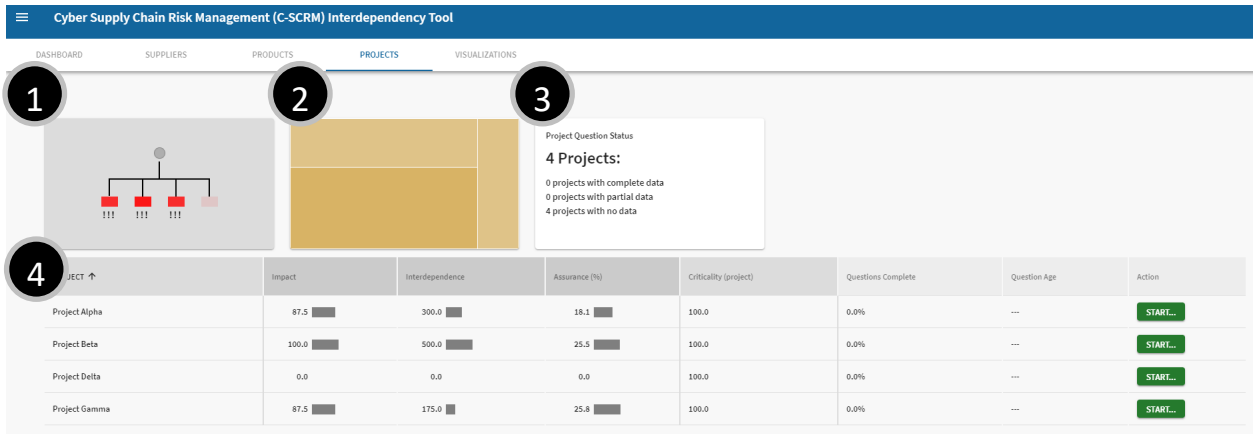

Figure 15: Projects detail view

The *Projects* view provides additional details about the projects that have been imported into the Tool and related metrics that have been calculated.

1. **Projects Visualization** – Shows projects with darker colors indicating higher *Impact* scores of individual projects.
2. **Heat Map** – Each box is colored based on project `Impact` with red, purple, pink, and brown denoting higher *Impact* and green, orange, and blue denoting lower *Impact* (depending on the color scheme selected). The size of the box denotes project *Interdependence* with larger boxes indicating larger *Interdependence*. View *Interdependence* and *Impact* values for each box in the heat map by hovering over a rectangle.
3. **Status Box** – Shows the total number of projects imported into the Tool and their statuses based on the number of questions answered in the project's questionnaire (see #3f below).
4. **Projects Table** – Lists projects and key metrics. Click on the column header to sort the table by that column's value in ascending or descending order. The dark grey columns (`Impact`, `Interdependence`, and `Assurance`) are calculated columns, which means they are calculated based on information provided in the node questionnaires. The light grey column (`Criticality (project)`) is derived directly from the associated supplier questionnaire and is not calculated from data in the *Product* or *Supplier* views.
    a. `Project` – Project name from imported data file
    b. `Impact` – Indicates potential impact to acquirer if suppliers and products that are part of the project experience disruption. An *Impact* score ranges from 0 to 100, with a score of 100 translating to devastating impact and 0 translating to no impact. It is calculated by taking the maximum *Access* and *Dependency* scores for all supply lines the node is a part of (see Appendix A for calculation details).
    c. `Interdependence` – Indicates influence of the suppliers and products in the supply chain. Scores are unbounded and calculated by adding the *Dependency* and

Access scores for each supply line that node is a part of (see Appendix A for calculation details). Higher scores indicate greater *Interdependence*.

d. `Assurance (%)` – Indicates degree of supply chain risk management security mitigating actions/controls implemented by suppliers related to the project (specifically, its products). *Assurance* scores range from 0 to 100 with 0 translating to the absence of any mitigating controls implemented. *Assurance* scores are calculated by averaging the *Assurance* scores of each supplier that a node is related to (e.g., any supplier contained in a supply line that the node is a part of) (see Appendix A for calculation details).
e. `Criticality (project)` – Indicates how important a project is to the organization's operations.
f. `Questions Complete` – Percentage of questions answered in project questionnaire.
g. `Question Age` – Length of time elapsed since project questionnaire has been edited.
h. `Action` – Contains the `SHOW...` or `EDIT...` button, which can be used to view/edit the questionnaire responses for a given project.

4.6 Suppliers, Products, and Projects Questionnaires

Figure 16 provides a screenshot of the questionnaire user interface. The default list of questions is included in Appendix B.

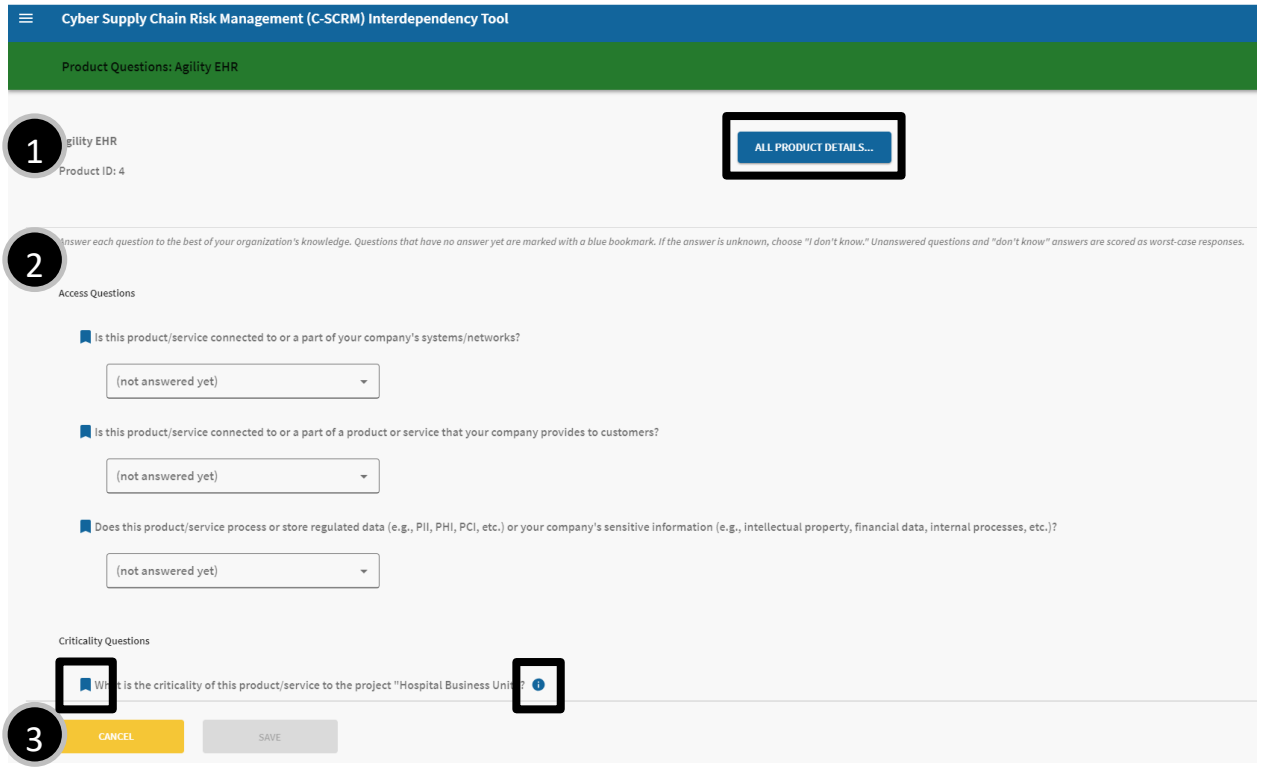

Figure 16: Questionnaire user interface

The questionnaire is visible after clicking the `EDIT...` button under the `Action` column in the *Suppliers*, *Products*, or *Projects* view.

1. **Information** – Any node information imported from CSV files is shown here. Click on the `ALL PRODUCT DETAILS...` button to view the information from the columns in the data file that were optional.
2. **Questionnaire Contents** – The body of the questionnaire appears here. Select an answer for each question by using the dropdown box below the question. If additional information is needed to answer the question, hover over the blue "*i*" icon for more information. Any questions that have a bookmark icon next to them denote unanswered questions.
3. **Cancel/Save** – Click `CANCEL` to exit the questionnaire without saving. Click `SAVE` to save any answers made in the questionnaire.

4.7 Visualizations

The *Visualizations* view provides the user with a visual representation of the supply chain, including the relationships between nodes, *Impact* level, and the relative *Interdependence* level. There are three sub-views in the *Visualizations* view: Hierarchy, Candlestick, and Scatterplots.

4.7.1 Hierarchy

Figure 17 provides a screenshot of the view of the Hierarchy visualization.

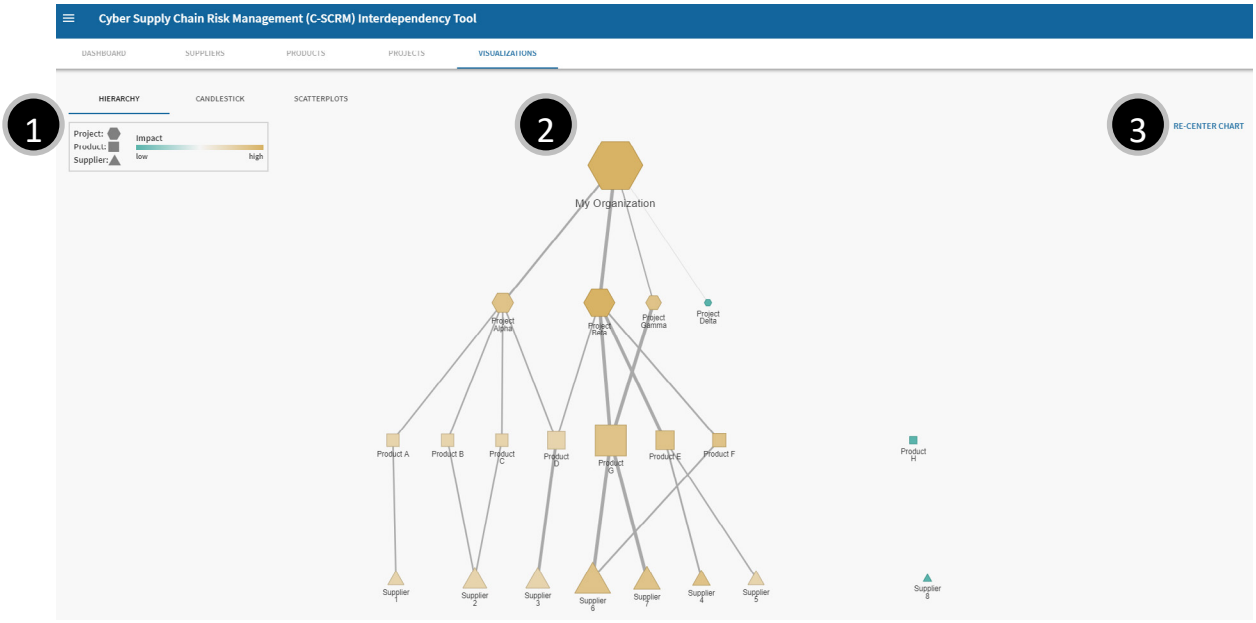

Figure 17: Hierarchy visualization

The Hierarchy provides a representation of the supply chain in a four-tiered hierarchy format with the organization at the top, followed by projects nodes, product nodes, and supplier nodes, respectively.

1. **Legend –** As indicated by the legend, the hexagons in the diagram denote the organization or projects; the squares denote products; and the triangles denote suppliers. The nodes on the chart are colored based on *Impact* with highest impact nodes in red, purple, pink, and brown and lowest impact nodes in green, orange, and blue (depending on color scheme selected). *Interdependence* is indicated based on the size of each node, where larger-sized nodes have higher *Interdependence* scores than smaller-sized nodes.
2. **Hierarchy chart –** The chart is interactive and can be manipulated in the following ways:
    a. Show additional metrics about a node by hovering over the node. A dialog box will appear and show `Impact`, `Interdependence`, and `Assurance` metrics. The nodes and their direct connections will also become highlighted.
    b. Zoom in and out of the diagram by hovering over the Hierarchy chart and scrolling up to zoom in and scrolling down to zoom out.

c. Click a node to highlight the node, its direct connections, and the supplier connections of any product the node is connected to. Hold the control key ("`Ctrl`") while clicking to select multiple nodes.
d. Customize the chart arrangement by clicking, holding, and dragging a node around the canvas to arrange the chart as desired. Hold control ("`Ctrl`") to select multiple nodes and move them as a group.
    - **Note**: Any changes to the layout of the chart are preserved and reappear when the Tool is reopened.
e. Navigate to the node's entry in a *Suppliers*, *Products*, or *Projects* view by double-clicking a node. The node will appear at the top of the table, and further analysis can be performed.

3. **Re-Center Chart –** This button allows the user to center the chart in the canvas area.

4.7.2 Candlestick

Figure 18 provides a screenshot of the Candlestick visualization.

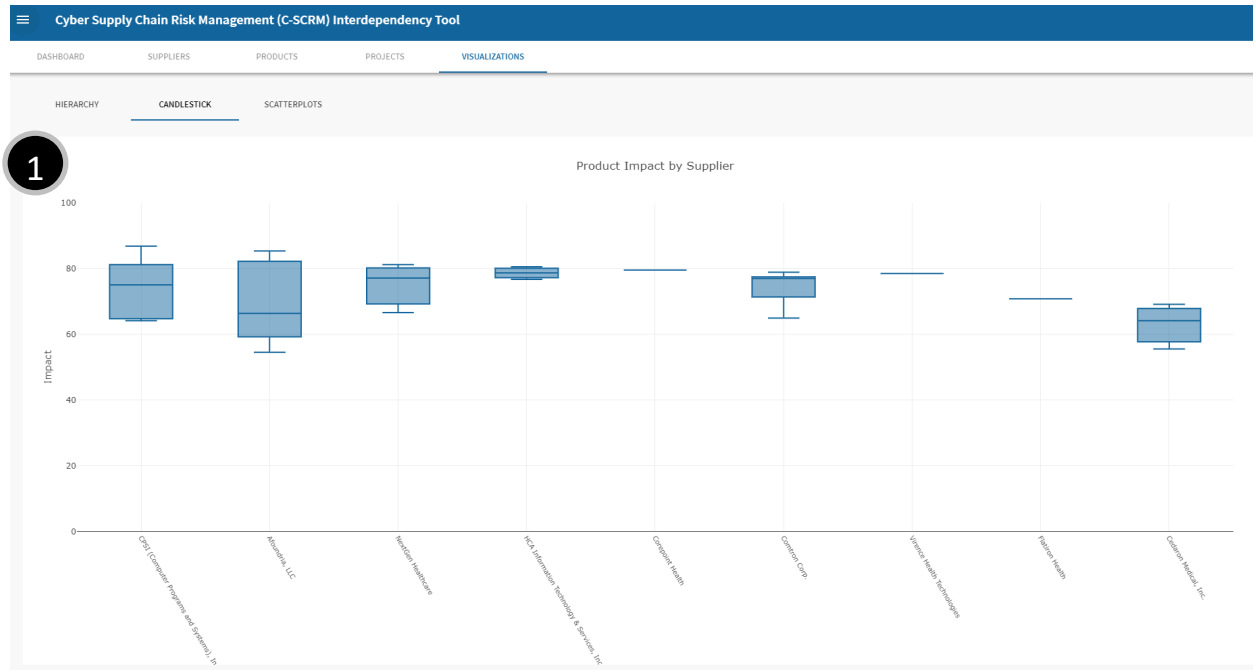

Figure 18: Candlestick visualization

The Candlestick chart provides a visual of the distributions of product impacts within a supplier. The *Impact* value metrics (see 1a below) are plotted on the *y-axis*, and each supplier is plotted on the *x-axis*.

1. **Candlestick Chart –** Hover over the area above each supplier for more metrics about the distribution of product impacts for a given supplier. This includes (if applicable):
    a. Min: Minimum value of *Impact* scores for a given supplier
    b. Max: Maximum value of *Impact* scores for a given supplier
    c. Median: Median value of *Impact* scores for a given supplier
    d. Q1: 1st Quartile, 25th percentile of *Impact* scores for a given supplier

e. Q3: 3rd Quartile, 75th percentile of *Impact* scores for a given supplier
f. Lower Fence: Lower fence of *Impact* scores is calculated as $Q1 - 1.5 \times IQR$, where $IQR = Interquartile\ range = (Q3 - Q1)$ and can be considered the "lower limit" of the *Impact* scores for a given supplier.
g. Upper Fence: Upper fence of *Impact* scores is calculated as $Q3 + 1.5 \times IQR$, where $IQR = Interquartile\ range = (Q3 - Q1)$ and can be considered the "upper limit" of the *Impact* scores for a given supplier.

4.7.3 Scatterplots

Figure 19 is a screenshot of the Scatterplot visualization.

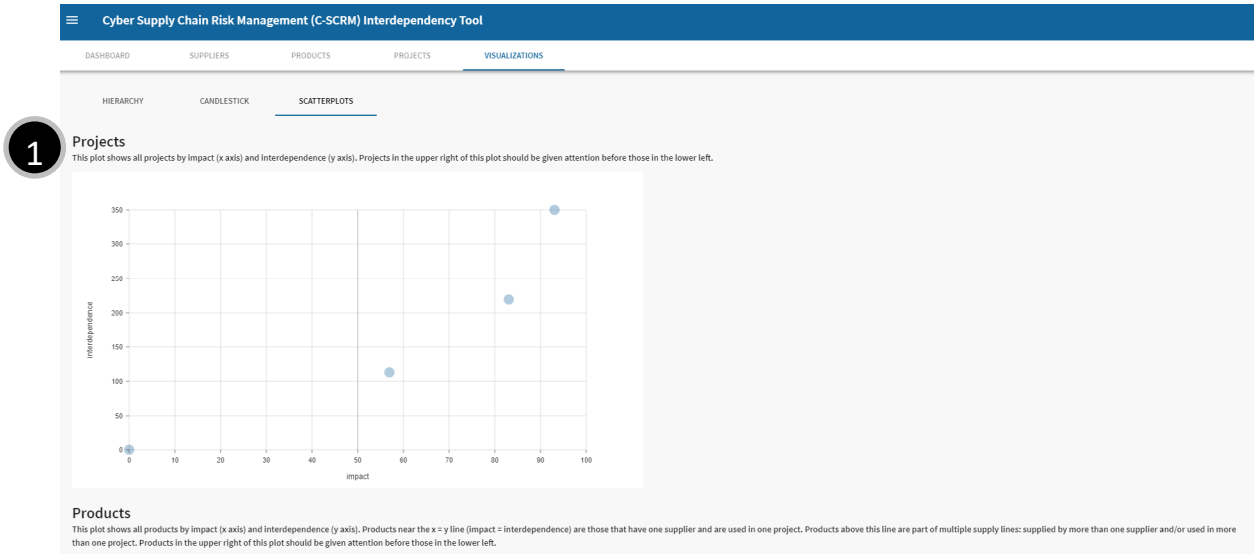

Figure 19: Scatterplots visualization

The Scatterplot provides a visual of the distributions of *Impact* and *Interdependence* values for each node type. The *Interdependence* value is plotted on the *y-axis*, and the *Impact* value is plotted on the *x-axis*.

1. **Scatterplot Chart**
   a. Hover over the area above each data point to display the actual *Impact* and *Interdependence* values.
   b. Navigate to the node's entry in a *Suppliers*, *Products*, or *Projects* navigation view by double-clicking a node. The node will appear at the top of the table, and further analysis can be performed.

4.8 Tool Menu

Tool settings can be accessed by clicking the three horizontal lines on the top left of the Tool window, as shown in Figure 20.

Figure 20: Tool menu button

Figure 21 shows the expanded view of the Tool menu. Figure 22 shows the user preferences window.

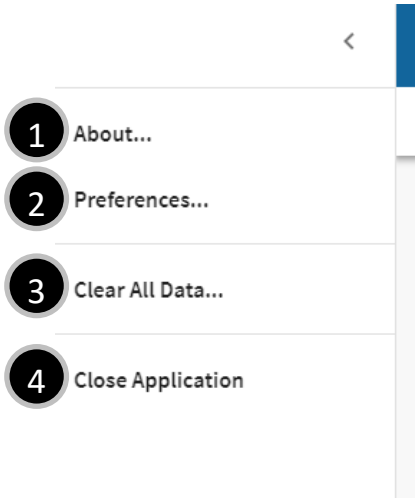

Figure 21: Tool menu

1. **About –** Provides information about the Tool owner and Tool version.

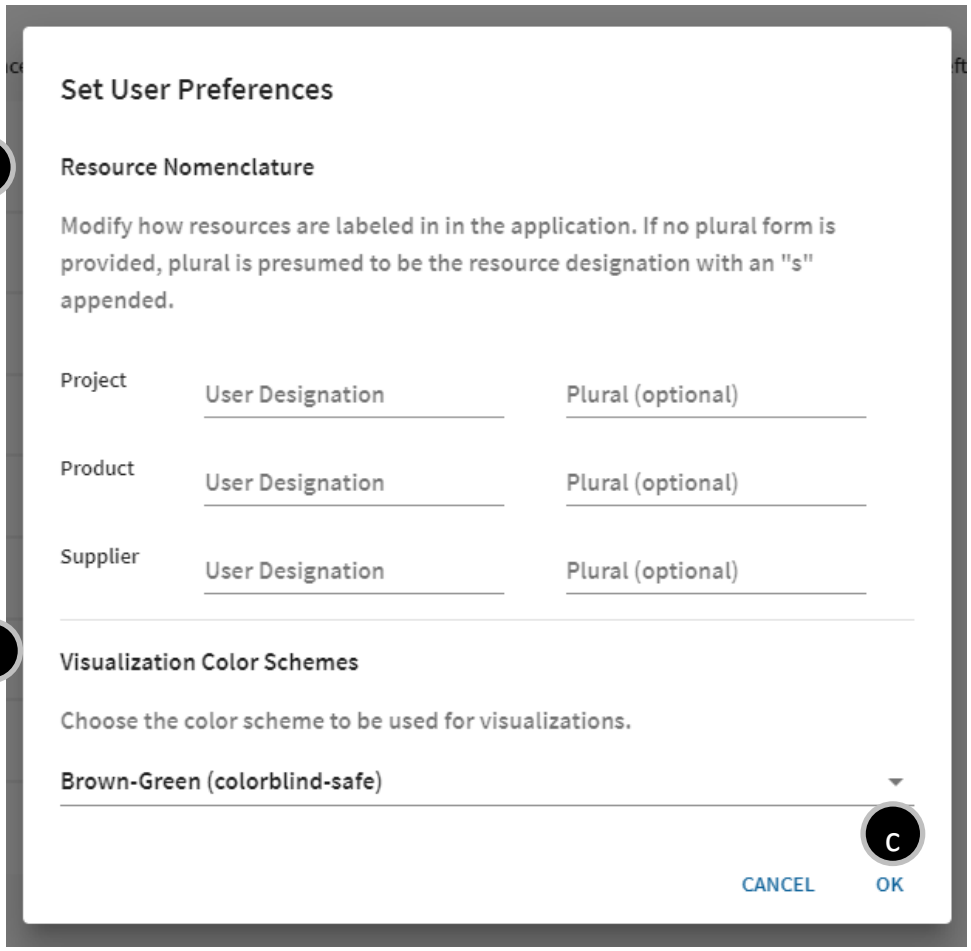

Figure 22: User preferences window

2. **Preferences –** Allows users to set preferences such as naming conventions and color schemes.
   a. **Resource Designations –** Type an alternate title in the ***User Designation*** field if the default *Project*/*Product*/*Supplier* naming convention does not fit an organization's use case nomenclature. For example, an organization may define the highest node type as *Business Units* instead of *Projects*. Fill in the ***Plural*** field if the plural of the word in the ***User Designation*** field is not derived by simply appending an "s" to the word (e.g., the plural of "focus" is "foci," not "focuss"; "foci" needs to be added to the ***Plural*** field).
   b. **Visualization Color Schemes –** Customize the color scheme used in the Tool by clicking the drop-down arrow and the desired color scheme.
   c. **Save** – Click ***OK*** to save the selected preferences.
3. **Clear All Data –** Clears all imported data and settings from Tool.
4. **Close Application –** Closes the Tool; all data and customizations (e.g., changes to the positions of the nodes) to the Hierarchy chart are saved.

5 Results

This section describes how to interpret the information provided by the Tool.

5.1 Overview

After the user imports supply chain CSV files and completes node questionnaires, the tool provides a series of scores and visualizations. The user may use these scores and visualizations to identify highly impactful and interdependent nodes. The relative scoring associated with these significant nodes may be used to inform C-SCRM program prioritization by highlighting where risk-mitigating controls may be most necessary.

This section explains how to identify these significant nodes and how to understand the *Impact*, *Interdependence*, and *Assurance* scores for each node. Each node type (*Supplier*, *Product*, and *Projects*) impacts the calculation of each of these scores. Therefore, updates to one node's questionnaire for a given node type may impact scores for nodes in a different node type. Please see Appendix A for more details about how these scores are calculated.

Note: The Tool scores unanswered questionnaire questions equal to the "worst-case" answer. This is a "fail-safe" feature designed to avoid inaccurate assumptions. For this reason, questionnaires with no answered questions result in the highest-possible *Impact* score (100.0), the highest possible *Interdependence* score (determined by the organization's supply chain topology), and the lowest possible *Assurance* score (0.0). Therefore, the Tool is more accurate if the user completes more questions.

5.2 Significant Nodes

The *Visualizations* view can help the user quickly identify highly impactful and interdependent nodes in the organization's supply network. In the Hierarchy visualization, the most significant nodes are the largest and are indicated by color (these colors may be red, purple, pink, or brown depending on the color scheme selected by the user). Double-click a node to review the node's complete score information and access its associated questionnaire in the *Suppliers, Products*, and *Projects* views. If the user wishes to increase the scores, risk mitigation actions can be developed and implemented. See Secs. 5.3 to 5.5 for more information on suggested methods of score improvement.

For an alternative visualization comparing nodes within a node type, click the *Suppliers*, *Products,* and *Projects* views to examine their respective heat maps. As in the Hierarchy visualization, the boxes that are the largest and colored red, purple, pink, or brown are the most critical nodes to perform further analysis on.

5.3 *Impact Scores*

The *Impact* score represents the highest potential negative impact a node can have on the organization if it fails. This score is bounded to a value between 0 and 100, where higher values indicate higher potential impact.

To reduce a node's *Impact* score, the organization needs to investigate reducing the criticality of products and/or projects that it is connected to. It can also look at ways to reduce the dependence on a given product, as well as reducing supplier and product access (data, physical, and IT network).

5.4 *Interdependence Scores*

The *Interdependence* score represents the relative influence of a node across the organization's supply chain. For suppliers, this translates to how many products the supplier provides the organization and the extent to which these products are used across the organization. For products, this translates to how many suppliers provide the product and in how many projects the product is used. This score is unbounded and best understood in relation to the node's *Impact* score and the *Interdependence* scores of similar nodes.

As noted previously, the user needs to reduce an *Interdependence* score if the *Interdependence* score of a node is high relative to similar nodes. To reduce the *Interdependence* score of a supplier, the organization needs to investigate expanding the number of suppliers that supply a given product to reduce the organization's dependence on any one supplier. To reduce the *Interdependence* score of a product, the organization needs to look at ways to reduce the *Impact* score as well as the number of suppliers that supply the product.

5.5 *Assurance Score*s

The *Assurance* score represents how completely the organization has implemented C-SCRM mitigations for a particular node. This score is a percentage of implemented mitigations over possible mitigations, and lower values indicate that the organization needs to work with the supplier to implement mitigating controls.

To improve a node's *Assurance* score, the organization needs to work with suppliers to implement risk mitigations. This includes gaining more visibility into the supplier's third parties and conducting supplier reviews (e.g., through completion of a questionnaire). Review the questions in the `Supplier Assurance` question category in Appendix B for more information.

6 Advanced Configuration

This section provides configuration instructions for advanced users to further customize the Tool, including modifying node questionnaires and the relative weight of specific questions. These instructions are intended for users capable of building/rebuilding web applications, including digitally signing executables.

While the code for the Tool may be modified however an organization desires, any configurations beyond those described in this section need to be executed by those with a high degree of experience in application development.

6.1 Overview

Questions that appear in the *Supplier*, *Product*, and *Project* questionnaires are stored as CSV files in the source distribution and can be found on the project webpage or in the top-level "`assets`" folder of the Tool's GitHub repository. The names of these files are "`supplier-questions.csv`", "`product-questions.csv`", and "`project-questions.csv`". These files can be edited directly without needing to modify the Tool's application source code. After making any edits to the CSV files, the application needs to be rebuilt and a distribution created for each target platform (Windows, Mac, and Linux).

Note: If any changes are made and the application needs to be rebuilt, the user may wish to digitally sign the resulting executable. This needs to be done in accordance with the organization's software signing policy.

The required columns that the Tool uses as input data are: `ID`, `Question`, `Answers`, `Type of Question`, `Question Info Text`, and `Weight`. For product and project CSV files, there is a `Relation` column that is also created.

For the current version of the Tool, the addition and deletion of questions and answer choices are *not* supported. The only columns considered editable in each CSV file are: `Question`, `Question Info Text`, `Weight`, and `Answers`. Acceptable inputs for each of these columns are described below.

6.2 Question

The `Question` column contains the text of the question and is freely editable. There are special variables that are used for certain questions.

For product questions where the `Type of question` column has value "`Criticality`" or "`Dependency`," the variable `[Project ID]` is substituted with the name of the project, and the variable `[Supplier ID]` is substituted with the name of the supplier.

If alternate nomenclature was configured in the Tool menu for the words "project," "product," or "supplier" (see Sec. 4.8), the user can also enclose "project," "product," or "supplier" in brackets ("`{}`") to substitute the alternate text values provided. For example, if the word "`project`" has been remapped to be "`business unit`" in the user preferences window, any appearance of

{project} in this column shows as business unit. If capitalization of the word is desired, the user needs to use {Supplier}. If the plural version of the word is desired, the user needs to use {suppliers} and {Suppliers}.

For instances where the phrase {product/service} appears, this phrase remains product/service in the final output if the user did not configure an alternate nomenclature for product. If an alternate nomenclature for product was configured, the alternate nomenclature is substituted where the word "product" appears in the phrase "product/service."

6.3 Question Info Text

The same variables for Question described above can also be used for the Question Info Text column. The one exception is that the variables [Project ID] and [Supplier ID] should not be used in this column.

6.4 Weight

The weight given to each question is provided in the Weight column. All questions are given a default weight of "1," but this weight can be changed to modify the relative weightings of questions *within the same category* (e.g., *Criticality*, *Access*, *Dependency*, and *Assurance*) and node type (e.g., *Supplier, Product*, and *Project*). The values in this column can be decimals. The values for each category are totaled, and the weight of a question is the value contained in the Weight column divided by the category total. If there is only one question in a given category, the Weight column is not relevant.

6.5 Answers

Answers are contained in the Answer column and listed in the following format: value=10;label="Yes" | value=0;label="No" | value=10;label="I don't know".

Each response option is separated by the pipe ("|") character. Each option contains the value of that response and the answer value showed in the response drop-down, respectively, with the semicolon (";") as the separator character. The label variable should contain the answer choice text that needs to be displayed. The value variable is the number of "points" associated with that answer choice. This value has no bounds, and decimals are allowed. However, it is recommended that a 0 to 10 scale is used where a 10 translates to the full number of points going to the score related to that question (e.g., worst-case scenario, such as confirmed physical access), and 0 translates to no points going to the score related to that question (e.g., best-case scenario, such as confirmed no physical access).

For the current version of the tool (version 1), Answer options cannot be added or removed. This may be modified in future versions of the tool.

References

[NIST CSF] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NISTIR 8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) *Criticality Analysis Process Model: Prioritizing Systems and Components*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8179. https://doi.org/10.6028/NIST.IR.8179

[SP 800-161] Boyens J, Paulsen C, Moorthy R, Bartol N (2015) *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[UMD1] University of Maryland, Robert H. Smith School of Business (2012) *Proof of Concept for an ICT SCRM Enterprise Assessment Package.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST White Paper. Available at https://csrc.nist.gov/CSRC/media/Publications/white-paper/2012/12/01/proof-of-concept-for-an-ict-scrm-enterprise-assessment-package/final/documents/umd_ict_scrm_portal_report3.pdf

[UMD2] University of Maryland, Robert H. Smith School of Business (2011) *The ICT SCRM Community Framework Development Project: Final Report* (National Institute of Standards and Technology, Gaithersburg, MD), NIST White Paper. Available at https://csrc.nist.gov/CSRC/media/Publications/white-paper/2011/12/01/ict-scrm-community-framework-development-project-final-report/final/documents/umd_ict_scrm_initiatives-report2-1.pdf

Appendix A – Calculation

This appendix provides a detailed description of the algorithm used to calculate each node's scores in the Tool.

a. Calculation Overview

Each node is measured with the three scores described in Sec. 5 (the *Impact* score, *Interdependence* score, and *Assurance* score) and referred to in this appendix as "terminal scores." Terminal scores are ultimately derived from a user's questionnaire answers and the node's relative placement in the organization's supply chain topology.

To calculate terminal scores from the user's questionnaire answers, the answers are first divided into question categories. Question categories are detailed below in Appendix A.b (**Question Categories**). Scores within each question category are used to determine variables known as "supporting figures." Supporting figures are detailed below in Appendix A.c (**Supporting Figures**). Simple arithmetic between these supporting figures directly determines the terminal scores for a given node. These final calculations are detailed below in Appendix A.d (**Terminal Scores**). The calculation flow is shown in Figure 23.

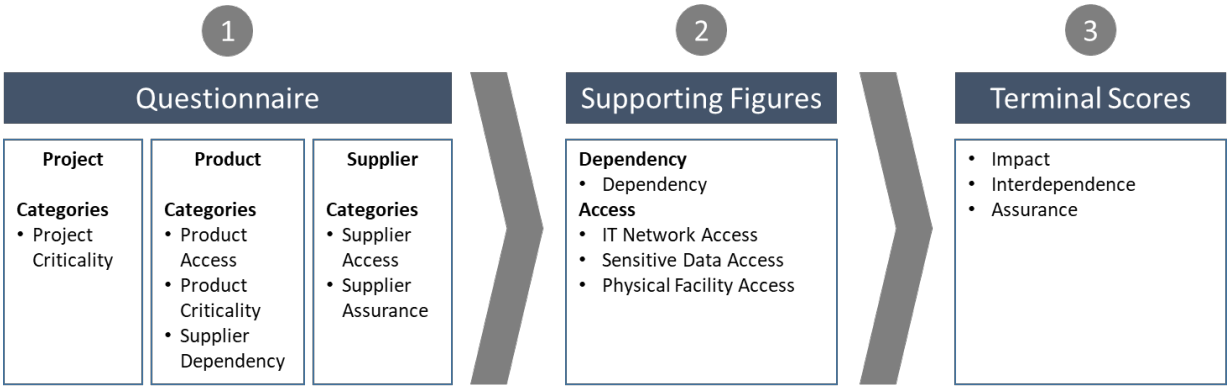

Figure 23: Calculation flow

Note: "Supporting figures" are exclusively for the calculation of the terminal scores and are not displayed to the user.

b. Question Categories

Each question is assigned to one of the categories below. The scores in each of the above categories and subcategories are calculated based on the *Logic* column in the tables of Appendix B and normalized to a percentage score (0 to 100). See Appendix B for a mapping of each question to its respective category.

Project Questionnaire Categories

- ***Project Criticality***: Questions that detail the importance of a particular project to the organization

Product Questionnaire Categories

- ***Product Access***: Questions that detail the degree of access a particular product has to the organization's sensitive assets. There are three access subcategories:
  - *Product IT Network Access*
  - *Product Sensitive Data Access*
  - *Product Physical Facility Access*
- ***Product Criticality***: Questions that detail the degree of importance that a particular product has to a given project
- ***Supplier Dependency***: Questions that detail the degree to which the organization depends on current suppliers for a particular product

Supplier Questionnaire Categories

- ***Supplier Access***: Questions that detail the degree of access that a particular supplier has to the organization's sensitive assets. There are three access subcategories:
  - *Supplier IT Network Access*
  - *Supplier Sensitive Data Access*
  - *Supplier Physical Facility Access*
- ***Supplier Assurance***: Questions that detail the degree to which a particular supplier follows cybersecurity and supply chain risk management best practices

c. Supporting Figures

Supporting figures are derived from the category and subcategory scores calculated in Appendix A.a above and are normalized so that each are equally weighted (worth 25 points each). Because each of these are derived from node questionnaires, changing questionnaire answers impacts these scores. The supporting figure categories are described below.

1. ***Dependency***: Measure of the degree of dependence that an organization has on a given product's supplier. This is a product of the *Supplier Dependency* score from the Product questionnaire and the *Criticality* of the Product and affected Project. This figure is normalized to 25 with a divisor (40 000).

   Calculation:

   ```
   Dependency = (Supplier Dependency × Product Criticality ×
   Project Criticality) / 40000
   ```

2. ***IT Network Access***: Measure of potential negative impact in the event of an information and communication technology (ICT) disruption. This is the sum of the *Product IT Network Access* and *Supplier IT Network Access* scores, scaled by the *IT Network Access Criticality*.[1] This figure is normalized to 25 with a divisor (800).

[1] Asset criticalities (e.g., `IT Network Access Criticality`, *Data Access Criticality*, and *Physical Access*

Calculation:

```
IT Network Access = (( Supplier IT Network Access + Product
IT Network Access) × IT Network Access Criticality ) / 800
```

3. ***Sensitive Data Access***: Measure of potential negative impact in the event of sensitive data compromise. This is the sum of the *Product Data Access* and *Supplier Data Access* scores, scaled by the *IT Network Access Criticality* (see footnote 1 for item #2, *IT Network Access Criticality*). This figure is normalized to 25 with a divisor (800).

   Calculation:

```
Sensitive Data Access = (( Supplier Sensitive Data Access +
Product Sensitive Data Access) × Data Access Criticality )
/ 800
```

4. ***Physical Facility Access***: Measure of potential negative impact in the event of physical facility compromise. This is the sum of the *Product Physical Access* and *Supplier Physical Access* scores, scaled by the *IT Network Access Criticality* (see footnote for item #2, *IT* Network *Access Criticality*). This figure is normalized to 25 with a divisor (800).

   Calculation:

```
Physical Facility Access = (( Supplier Physical Facility
Access + Product Physical Facility Access) × Physical
Access Criticality ) / 800
```

d. Terminal Scores

Scores are calculated by aggregating the supporting figures from Appendix A.c for all supply lines in which a given node participates.

1. ***Impact Score*:** The sum of the highest supporting figures in each supporting figure category affecting the node. This is the sum of the highest *Dependency* figure, the highest *IT Network Access* figure, the highest *Sensitive Data Access* figure, and the highest *Physical Facility Access* figure in which the node participates. This score is bounded between 0 and 100 as each component figure is normalized to 25.

Criticality) are hard-coded to 100. Future versions of this Tool may feature asset criticality tuning.

Calculation:

```
Impact Score =  max(Dependency) + max(IT Network Access) +
max(Sensitive Data Access) + max(Physical Facility Access)
```

2. ***Interdependence Score*:** The sum of all supporting figures affecting the node. This is the sum of all *Dependency* figures, all *IT Network Access* figures, all *Sensitive Data Access* figures, and all *Physical Facility Access* figures in which the node participates.

   Calculation:

```
Interdependence Score =  sum(Dependency) + sum(IT Network
Access) + sum(Sensitive Data Access) + sum(Physical
Facility Access)
```

3. ***Assurance Score*:** Percent of implemented mitigations over possible mitigations. Note that unlike the other scores described above, this score is not weighted based on the number of supply lines associated with a given supplier. The score is determined by averaging the *Supplier Assurance* scores of each supplier associated with a given node; the *Assurance Score* of each supplier is equally weighted.

   Calculation:

```
Assurance Score =  average(Supplier Assurance) / 100
```

See Appendix C for an example of how these calculations are determined for a sample supply chain.

Appendix B – Question Categories

The table below provides a listing of the questions in the questionnaire and the associated category and scoring logic for each question.

The logic column shows the percentage of points assigned to the question that are added or subtracted to the category score based on the response choice. For example, if the question category is *Supplier Assurance*, and the logic of the answer choice selected is "add 100 % of points allotted," the *Assurance Score* increases by 100 % of the points assigned to that question. By default, the questions are equally weighted so that each of the 12 questions in the *Supplier Assurance* category is worth 1/12 or ≈8.3 % of the entire score.

As mentioned in Appendix A, the assumption for the metrics is the worst-case scenario (e.g., highest criticality, highest access, lowest assurance, and highest dependency). This serves as the basis of the increase/decrease logic for each question. For example, the score will only change if the response to the *Supplier Access* question, "does the supplier have access to the acquirer's IT networks, OT systems, or sensitive platforms (e.g., payment portals)?" is "No." Since the assumption is the highest level of access, only responses which indicate lower access decrease the score.

a. Supplier Questions:

These supplier questions were developed based on a sample of existing supplier risk questionnaires as well as the opinions and advice of subject matter experts. They have been selected as the minimum information an organization needs to know about their suppliers in order to gain an understanding of the potential impact that a supplier may have. Many organizations have existing supplier questionnaires that differ from the questionnaire in this Tool. Those organizations are encouraged to compare their questionnaires with the one in this Tool and, where appropriate, update their questionnaire or modify this Tool to support their questionnaire. Instructions on how to modify the questionnaire contents and question weightings are included in Sec. 6.

Table 2: Supplier Questions, Category, and Logic

Question	Category	Logic
Does the supplier have access to the acquirer's IT networks, OT systems, or sensitive platforms (e.g., payment portals)?	*Supplier IT Network Access*	IF no, subtract 100 % of points allotted IF yes, no change
Does the supplier have access to the acquirer's physical facilities?	*Supplier Physical Facility Access*	IF no, subtract 100 % of points allotted IF yes, no change

Question	Category	Logic
Does the supplier have access to acquirer-sensitive information (e.g., intellectual property, financial data, internal processes, etc.) or regulated data (e.g., PII, PHI, PCI, etc.*) for which the acquirer is responsible?	*Supplier Sensitive Data Access*	IF no, subtract 100 % of points allotted IF yes, no change
Does the supplier have fewer than 10 employees?	*Supplier Assurance*	IF no, add 100 % of points allotted IF yes, no change
How long has this supplier been in business?	*Supplier Assurance*	IF < 3 years, no change IF 3 to 5 years, add 50 % of points allotted IF 5 to 10 years, add 80 % of points allotted IF > 10 years, add 100 % of points allotted
How much of the supplier's total business is provided by the acquirer?	*Supplier Assurance*	IF < 25 %, no change IF 25 to 50 %, add 50 % of points allotted IF 50 to 100 %, add 100 % of points allotted
Does this supplier follow relevant industry standards?	*Supplier Assurance*	IF no, no change IF self-attestation, add 30 % of points allotted IF self-attestation with proof, add 50 % of points allotted IF self-attestation with third-party assessment, add 70 % of points allotted IF conformity assessment, no change
Does this supplier operate in highly regulated industries or provide products/services to highly regulated industries (e.g., financial services, energy)?	*Supplier Assurance*	IF no, no change IF yes, add 100 % of points allotted
Is the supplier owned, controlled, or influenced in full or in part by an entity of concern (e.g. foreign nation state, competitors)?	*Supplier Assurance*	IF 1 (great concern), no change IF 2, add 30 % of points allotted IF 3, add 50 % of points allotted IF 4, add 70 % of points allotted IF 5 (no concern), add 100 % of points allotted

Question	Category	Logic
How sensitive is the supplier's ability to provide quality products/services to supply chain disruptions, both man-made and natural?	*Supplier Assurance*	IF 1 (very sensitive), no change IF 2, add 30 % of points allotted IF 3, add 50 % of points allotted IF 4, add 70 % of points allotted IF 5 (very robust), add 100 % of points allotted
Has this supplier filled out a questionnaire to qualify for providing products or services to the acquirer?	*Supplier Assurance*	IF no, no change IF yes, add 100 % of points allotted
Has the acquirer verified the information provided by the supplier on their supplier questionnaire?	*Supplier Assurance*	IF not provided, no change IF not verified, add 10 % of points allotted IF doc review, add 50 % of points allotted IF third-party audit, add 70 % of points allotted IF acquirer audit, no change
Is the acquirer able to influence this supplier's security practices through supplier agreements?	*Supplier Assurance*	IF 1 (not at all), no change IF 2, add 30 % of points allotted IF 3, add 50 % of points allotted IF 4, add 70 % of points allotted IF 5 (yes, for all product), add 100 % of points allotted
Does the acquirer know this supplier's sub-suppliers?	*Supplier Assurance*	If no existing relationships, add 50 % of points allotted IF no, no change IF some, add 50 % of points allotted IF all, add 100 % of points allotted
Has the supplier provided the acquirer with mitigation assurances (e.g. insurance, fallback partnerships with other vendors, etc.)?	*Supplier Assurance*	IF no, no change IF yes, add 100 % of points allotted

* "PII", "PHI" and "PCI" as used in the questionnaire may be defined as:

b. Product Questions:

The information to complete this questionnaire may come from a security plan, security architecture documentation, industry information, and/or supplier questionnaires and interviews. The criticality level can be determined using the methodology detailed in NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components* [NISTIR 8179], or an equivalent method. Criticality should be calculated in the context of the objectives of the project and the organization's goals.

Table 3: Product Questions, Category, and Logic

Question	Category	Logic
Is this product or service connected to or part of acquirer systems/networks?	*Product IT Network Access*	IF no, subtract 100 % of points allotted IF yes, no change
Is this product or service connected to or part of a product or service that the acquirer provides to customers?	*Product Physical Facility Access*	IF no, subtract 100 % of points allotted IF yes, no change
Does this product or service process or store regulated data (e.g., PII, PHI, PCI, etc.*) or acquirer-sensitive information (e.g., intellectual property, financial data, internal processes, etc.)?	*Product Sensitive Data Access*	IF no, subtract 100 % of points allotted IF yes, no change
What is the criticality of this product/service to this project? *Note:* If the product is connected to multiple projects, more than one question will display, each with the name of the project substituted where the word "project" is in the question text above.	*Product Criticality*	IF 1, no change IF 2, subtract 10 % of points allotted IF 3, subtract 20 % of points allotted IF 4, subtract 30 % of points allotted IF 5, subtract 40 % of points allotted IF 6, subtract 50 % of points allotted IF 7, subtract 60 % of points allotted IF 8, subtract 70 % of points allotted IF 9, subtract 80 % of points allotted IF 10, subtract 90 % of points allotted
What is the supplier's market share for this particular product/service? *Note:* If the product is connected to multiple suppliers, more than one question will display, each with the name of the project substituted where the word "supplier" is in the question text above.	*Supplier Dependency*	IF < 25, no change IF 25 to 50, subtract 50 % of points allotted IF 50 to 75, subtract 80 % of points allotted IF 75 to 100, subtract 100 % of points allotted
What percent of the supplier's sales of this product/service does the acquirer consume?	*Supplier Dependency*	IF < 25, no change IF 25 to 50, subtract 50 % of points allotted IF 50 to 75, subtract 80 % of

Note: If the product is connected to multiple suppliers, more than one question will display, each with the name of the project substituted where the word "supplier" is in the question text above.		points allotted IF 75 to 100, subtract 100 % of points allotted
Would switching to an alternative supplier constitute a significant cost or effort for the acquirer?	*Supplier Dependency*	IF no, subtract 100 % of points allotted IF yes, no change
Does the acquirer have an existing relationship with another supplier for this product/service?	*Supplier Dependency*	IF no, no change IF yes, subtract 100 % of points allotted
How confident is the acquirer that they will be able to obtain quality products/services regardless of major supply chain disruptions, both man-made and natural?	*Supplier Dependency*	IF 1 (low confidence), no change IF 2, subtract 30 % of points allotted IF 3, subtract 50 % of points allotted IF 4, subtract 80 % of points allotted IF 5 (high confidence), subtract 100 % of points allotted
Does the acquirer maintain a reserve of this product/service?	*Supplier Dependency*	IF no, no change IF yes, subtract 100 % of points allotted

* "PII", "PHI" and "PCI" as used in the questionnaire may be defined as:

- *Personally Identifiable Information (PII)* – The term "PII," as defined in OMB Memorandum M-07-1616, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
- *Protected Health Information (PHI)* – PHI is individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records.
- *Payment Card Industry (PCI)* – PCI data can be defined as any information related to the Payment Card Industry Data Security Standard (PCI DSS), such as credit card numbers and card verification values (CVV).

c. Project Questions

The criticality level can be determined using the methodology detailed in NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components* [NISTIR 8179], or an equivalent method. Criticality should be calculated in the context of the objectives of the project and the organization's goals.

Table 4: Project Questions, Category, and Logic

Question	Category	Logic
How critical is this project to the acquirer's mission/business?	*Project Criticality*	IF 1, no change IF 2, subtract 10 % of points allotted IF 3, subtract 20 % of points allotted IF 4, subtract 30 % of points allotted IF 5, subtract 40 % of points allotted IF 6, subtract 50 % of points allotted IF 7, subtract 60 % of points allotted IF 8, subtract 70 % of points allotted IF 9, subtract 80 % of points allotted IF 10, subtract 90 % of points allotted

Appendix C – Calculation Example

This appendix walks through the calculations performed as outlined in Appendix A and Appendix B using an example supply chain.

Part 1: Creating the Supply Chain Structure

This supply chain can be made by modifying the "`Sample Data Set – Interconnected`" file or be made from scratch. The suppliers, products, and projects CSV files should contain the following structure and information:

Table 5: Suppliers CSV File Structure and Contents

ID	Name
1	Supplier 1
2	Supplier 2

Table 6: Products CSV File Structure and Contents

ID	Name	Supplier ID	Project ID
1	Product 1	1	2
2	Product 2	1;2	2
3	Product 3	2	2
4	Product 4	2	2

Table 7: Projects CSV File Structure and Contents

ID	Level	Name
1	1	My Organization
2	1.1	Project Alpha

Part 2: Scenario Overview

Figure 24 depicts an example supply chain diagram.

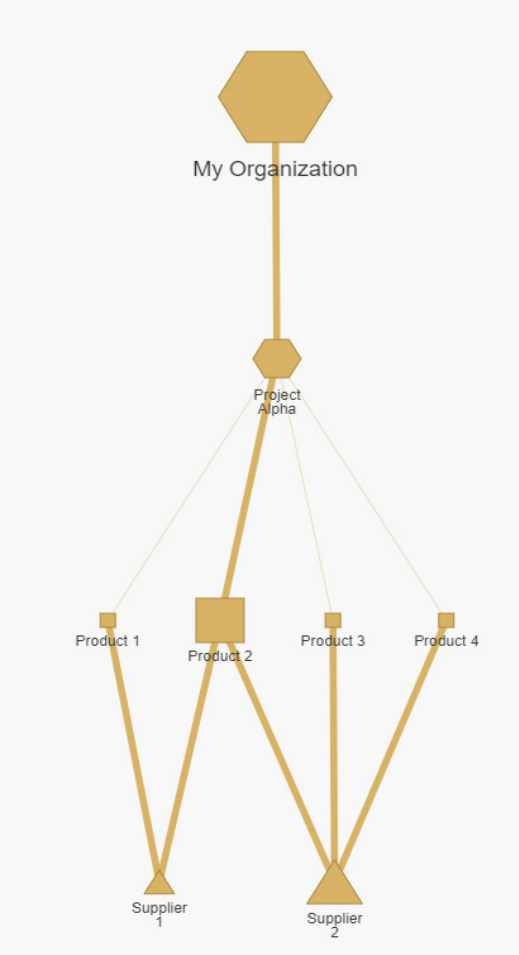

Figure 24: Supply chain diagram for example scenario

The example supply chain has one project associated with one organization. It has four products and two suppliers with one product (*Product 2*) supplied by two suppliers (*Supplier 1* and *Supplier 2*). All other products are supplied by one supplier.

This example begins with no questionnaire questions answered. With all questionnaire category variables being equal, the size of the nodes show that *Product 2* and *Supplier 2* have higher *Interdependence Scores*. This is expected given that *Product 2* is connected to two suppliers and *Supplier 2* supplies three products.

Part 3: Understanding Initial Conditions

"*Supply lines*" are an important concept for the Tool's algorithm. Every unique combination of a project, product, and supplier is a "supply line." Every supply line for a given node is highlighted when the user hovers their mouse pointer over the node in the Hierarchy visualization in the *Visualizations* view. Table 8, Table 9, and Table 10 provide a detailed breakdown of the supply lines for each node from Figure 24.

Supply Line Breakdown

Table 8: Supplier Supply Line Breakdown

Supplier Name	Supply Line Count	Supply Lines
Supplier 1	2	1. Project Alpha – Product 1 – Supplier 1 2. Project Alpha – Product 2 – Supplier 1
Supplier 2	3	1. Project Alpha – Product 2 – Supplier 2 2. Project Alpha – Product 3 – Supplier 2 3. Project Alpha – Product 4 – Supplier 2

Table 9: Products Supply Line Breakdown

Product Name	Supply Line Count	Supply Lines
Product 1	1	1. Project Alpha – Product 1 – Supplier 1
Product 2	2	1. Project Alpha – Product 2 – Supplier 1 2. Project Alpha – Product 2 – Supplier 2
Product 3	1	1. Project Alpha – Product 3 – Supplier 2
Product 4	1	1. Project Alpha – Product 4 – Supplier 2

Table 10: Project Supply Line Breakdown

Project Name	Supply Line Count	Supply Lines
Project Alpha	5	1. Project Alpha – Product 1 – Supplier 1 2. Project Alpha – Product 2 – Supplier 1 3. Project Alpha – Product 2 – Supplier 2 4. Project Alpha – Product 3 – Supplier 2 5. Project Alpha – Product 4 – Supplier 2

Figures and Scores Breakdown

a. Suppliers:

- **Question Categories**
  - ***Access*** – *Supplier 1* and *Supplier 2* each have the highest possible score (100.0) for each of the three access-related question categories because no questions have been answered.
- **Terminal Scores**
  - ***Impact Score***
    - *Supplier 1* and *Supplier 2* each have the highest possible score (`100`) because every component supporting figure of *Impact Scores* (i.e., *Dependency, IT Network Access, Sensitive Data Access, Physical Facility Access*) has the highest possible score (`25`).

- ***Interdependence Score***
  - *Supplier 1* has an *Interdependence Score* of `200` because each supply line has the highest possible score (`100`). There are two supply lines associated with *Supplier 1*, and `100 × 2 = 200`.
  - *Supplier 2* has an *Interdependence Score* of `300` because each supply line has the highest possible score (`100`). There are three supply lines associated with *Supplier 2*, and `100 × 3 = 300`.
- ***Assurance Score***
  - *Supplier 1* and *Supplier 2* have the lowest possible score (`0`) because no questions have been answered.

b. Products:

- **Question Categories**
  - *Criticality*, *Access*, and *Dependency* – All four products have the highest possible score (`100`) in every category because no questions have been answered.
- **Terminal Scores**
  - ***Impact Score***
    - All four products have the highest possible score (`100`) because every component supporting figure of *Impact Scores* (i.e., *Dependency, IT Network Access, Sensitive Data Access, Physical Facility Access*) has the highest possible score (`25`).
  - ***Interdependence Score***
    - *Product 1, Product 3,* and *Product 4* have an *Interdependence Score* of `100` because each supply line has the highest possible score (`100`). There are only supply lines associated with these products, and `100 × 1 = 100`.
    - *Product 2* has *an Interdependence Score* of `200` because each supply line has the highest possible score (`100`). There are two supply lines associated with this product, and `100 × 2 = 200`.
  - ***Assurance Score***
    - All products have the lowest possible score (`0`) because no questions have been answered.

c. Projects:

- **Question Categories**
  - ***Criticality*** – Project `Alpha` has the highest possible score (`100`) because no questions have been answered.
- **Terminal Scores**
  - ***Impact Score***
    - Project `Alpha` has the highest possible score (`100`) because every component supporting figure of *Impact Scores (*e.g., *Dependency, IT Network Access, Sensitive Data Access, Physical Facility Access*) has the highest possible score (`25`).

- ***Interdependence Score***
  - Project `Alpha` has an *Interdependence Score* of `500` because each supply line has the highest possible score (`100`). There are five supply lines associated with Project `Alpha`, and `100 × 5 = 500`.
- ***Assurance Score***
  - Project `Alpha` has the lowest score (`0`) due to worst case (no controls implemented) assumption.

Part 4: Questionnaire modifications and resulting impacts on figures and scores

To reduce complexity, the scenarios below change only one variable at a time. The reader can use this information to infer the influence of changing multiple variables together. This method of decomposing the influence of each part of the questionnaire is for the user's understanding only. The user needs to answer all questions in the questionnaire and interpret the results based on those responses alone.

Suppliers

Scenario 1: Answer to question, "Does the supplier have access to your company's IT networks, OT systems, or sensitive platforms (e.g., payment portals)?" is "No" for *Supplier 1*

Because the response to this question indicates a lower degree of access compared to the worst case (full access), the user would expect a lower access score for *Supplier 1* and any related supply lines. The logic for this question in Appendix B ("subtract 100 % of points allotted") supports this statement. Since this question is the only question in the *Supplier IT Network Access* subcategory, the 100 points allocated to this question become 0. This only impacts the *IT Network Access* supporting figure, which is now reduced to 12.5 from 25: *`((0 + 100) × 100)/ 800 = 12.5`*

The new *IT Network Access* score results in a supply line score of 87.5 (`25 + 12.5 + 25 + 25 = 87.5`). Since there are two supply lines that are associated with *Supplier 1* that each have this supply line score, the result is an `Interdependence Score` of 175 (`87.5 × 2 = 175`). The *Impact Score* takes the maximum of each supporting figure for all supply lines that the node is a member of. This means that the *Impact Score* is the same as the supply line score since the supply line score for the two supply lines are the same (`max(25,25) + max(12.5,12.5) + max(25,25) + max(25,25) = 87.5`).

As a result of these changes, the *Impact* and `I`*`nterdependence Score`* on the *Products* page for *Product 1* and *Product 2* have changed. This is because each product has a supply line with *Supplier 1* in it. *Product 1* only has one supply line and therefore takes the same supply line score of 87.5. With one supply line, the *Impact* and *Interdependence Score* are the same and equal to the supply line score. Thus, the impact and `I`*`nterdependence Scor`*`e` for *Product 1* is now 87.5. *Product 2* has two supply lines. The supply line associated with *Supplier 1* has a score of 87.5. However, the supply line associated with *Supplier 2* was not impacted, and the supply line score remains unchanged at 100. The *Impact Score* takes the maximum of each supporting figure for all supply lines that the node is a member of, which means the *Impact Score* remains

unchanged at 100 (`max(25,25) + max(25,12.5) + max(25,25) + max(25,25) = 100`). *Interdependence Score* takes the sum of the supply line scores and decreases to 187.5 (`100 + 87.5 = 187.5`).

In the *Projects* view, as with *Product 2*, the *Impact Score* remains unchanged at 100 since the *Impact Score* takes the maximum of each supporting figure for all supply lines that the project is a member of (`max(25,25,25,25,25) + max(12.5,12.5,25,25,25) + max(25,25,25,25,25) + max(25,25,25,25,25) = 100`). The *Interdependence Score* is reduced to 475 (`87.5 + 87.5 + 100 + 100 + 100 = 475`).

Scenario 2: Answer to question, "How long has this supplier been in business?" is "5-10 years" for Supplier 2

Because the response to this question indicates a higher degree of assurance compared to the worst case (no assurance), the user would expect a higher *Assurance Score* for *Supplier 2* and any related supply lines. The logic for this question in Appendix B ("IF 5-10 years, add 80% of points allotted") supports this statement. There are 12 questions in the `Supplier Assurance` category, and since each question is equally weighted in the default configuration, each question has a total of ≈8.3 points (1/12) allotted. This category only impacts the *Assurance Score*. Thus, the *Assurance Score* increases from 0 to 6.7 (`80% of 8.3 = 6.7`).

In the *Products* view, the *Assurance Score* is calculated by averaging the *Assurance Scores* of all suppliers that supply a given product. The *Assurance Score* of *Product 1* is unchanged because *Product 1* is not supplied by *Supplier 2*. *Product 3* and *Product 4* are both supplied only by *Supplier 2*, so each also gets an *Assurance Score* of 6.7. *Product 2* is supplied by both *Supplier 1* and *Supplier 2*. The supply line associated with *Supplier 1* remains unchanged with an *Assurance Score* of 0. The supply line associated with *Supplier 2* has increased to 6.7. The resulting *Assurance Score* for *Product 2* is 3.3 (`Average(6.7,0)/100 = 3.3 %`).

In the *Projects* view, the resulting *Assurance Score* for Project `Alpha` is 3.3 because both *Supplier 1* and *Supplier 2* supply products within the project (`Average(6.7,0)/100 = 3.3 %`).

Scenario 3: Answer to question, "Is this product/service connected to or part of a product or service that your company provides to customers?" is "No" for Product 2

Because the response to this question indicates a lower degree of access compared to the worst case (full access), the user would expect a lower access score for *Product 2* and any related supply lines. The logic for this question in Appendix B ("subtract 100 % of points allotted") supports this statement. Since this question is the only question in the *Product Physical Facility Access* subcategory, the 100 points allocated to this question becomes 0. This category only impacts the *Physical Facility Access* supporting figure, which is now reduced to 12.5 from 25: *((100 + 0) × 100)/ 800 = 12.5*

The new *Physical Facility* `Access` score results in a supply line score of 87.5 (`25 + 25 + 25 + 12.5 = 87.5`). Since there are two supply lines that are associated with *Product 2* that each have this supply line score, the resulting *Interdependence Score* is 175 (`87.5 × 2 =`

175). The *Impact Score* takes the maximum of each supporting figure for all supply lines that the node is a member of. This means that the *Impact Score* is the same as the supply line score (87.5) since the supply line score for the two supply lines are the same (max(25,25) + max(25,25) + max(25,25) + max(12.5,12.5) = 87.5).

In the *Suppliers view*, the Impact Score for *Supplier 1* remains unchanged at 100 because *Supplier 1* has two supply lines. The supply line associated with *Product 1* was not impacted. The supply line associated with *Product 2* is 87.5. The Impact Score takes the maximum of each supporting figure for all supply lines that the node is a member of, which means the Impact Score remains unchanged at 100 (max(25,25) + max(25,25) + max(25,25) + max(25,12.5) = 100). The *Interdependence Score* takes the sum of the supply line scores and decreases to 187.5 (100 + 87.5 = 187.5). Supplier 2's Impact Score also remains unchanged at 100 because *Supplier 2* has three supply lines. The supply line associated with *Product 3* and *Product 4* were not impacted. The supply line associated with *Product 2* is 87.5. The Impact Score takes the maximum of each supporting figure for all supply lines that the node is a member of, which means the Impact Score remains unchanged at 100 (max(25,25,25) + max(25,25,25) + max(25,25,25) + max(12.5,25,25) = 100). The *Interdependence Score* takes the sum of the supply line scores and decreases to 287.5 (87.5 + 100 + 100 = 287.5).

In the *Projects* view, as with *Supplier 1* and *Supplier 2*, the Impact Score remains unchanged at 100 since the Impact Score takes the maximum of each supporting figure for all supply lines that the project is a member of (max(25,25,25,25,25) + max(25,25,25,25,25) + max(25,25,25,25,25) + max(25,12.5,12.5,25,25) = 100). The *Interdependence Score* is reduced to 475 (100 + 87.5 + 87.5 + 100 + 100 = 475).

Scenario 4: Answer to question, "What is the criticality of this product/service to the project 'Project Alpha'?" is "5" for Product 2

Because the response to this question indicates a lower degree of criticality compared to the worst case (highest criticality), the user would expect a lower criticality score for *Product 2* and any related supply lines. The logic for this question in Appendix B ("IF 5, subtract 40 % of points allotted") supports this statement. Since this question is the only question in the *Product Criticality* category, the 100 points allocated to this question becomes 60 (100 – (.4(100) = 60). This category only impacts the Dependency supporting figure, which is now reduced to 15 from 25: *((100 × 60 × 100)/ 40000 = 15*

The new Dependency score results in a supply line score of 90 (25 + 25 + 25 + 15 = 90). Since there are two supply lines that are associated with *Product 2* that each have this supply line score, the resulting *Interdependence Score* is 175 (90 × 2 = 180). The Impact Score takes the maximum of each supporting figure for all supply lines that the node is a member of. This means that the Impact Score is the same as the supply line score (90) since the supply line scores for the two supply lines are the same (max(15,15) + max(25,25) + max(25,25) + max(25,25) = 90).

In the *Suppliers* view, the `Impact Score` for *Supplier 1* remains unchanged at 100. This is because Supplier 1 has two supply lines. The supply line associated with *Product 1* was not impacted. The supply line associated with *Product 2* is 90. The `Impact Score` takes the maximum of each supporting figure for all supply lines that the node is a member of, which means that the `Impact Score` remains unchanged at 100 (`max(25,15) + max(25,25) + max(25,25) + max(25,25) = 100`). The *Interdependence Score* takes the sum of the supply line scores and decreases to 190 (`100 + 90 = 190`). *Supplier 2*'s `Impact Score` also remains unchanged at 100 because *Supplier 2* has three supply lines. The supply line associated with *Products 3* and *4* were not impacted. The supply line associated with *Product 2* is 90. The `Impact Score` takes the maximum of each supporting figure for all supply lines that the node is a member of, which means that the `Impact Score` remains unchanged at 100 (`max(15,25,25) + max(25,25,25) + max(25,25,25) + max(25,25,25) = 100`). The *Interdependence Score* takes the sum of the supply line scores, and decreases to 287.5 (`90 + 100 + 100 = 290`).

In the *Projects* view, as with *Supplier 1* and *Supplier 2*, the `Impact Score` remains unchanged at 100 since the *Impact Score* takes the maximum of each supporting figure for all supply lines that the project is a member of (`max(25,15,15,25,25) + max(25,25,25,25,25) + max(25,25,25,25,25) + max(25,25,25,25,25) = 100`). The *Interdependence Score* is reduced to 480 (`100 + 90 + 90 + 100 + 100 = 480`).

Scenario 5: Answer to question, "What is the supplier's ("Supplier 2") market share for this particular product/service?" is "25-50 %" for Product 3

Because the response to this question indicates a lower degree of dependence compared to the worst case (highest dependence), the user would expect a lower `Dependency` score for *Product 3* and any related supply lines. The logic for this question in Appendix B ("IF 25-50, subtract 50 % of points allotted") supports this statement. There are six questions in the `Supplier Dependency` category. Thus, since each question is equally weighted in the default configuration, each question has a total of ~16.7 points (1/6) allotted. The *Supplier Dependency* score decreases from 100 to 91.7 (`100 – (50% of 16.7) = 91.7`). This category only impacts the `Dependency` supporting figure, which is reduced to 22.9 from 25: `((91.7 × 100 × 100))/ 40000 = 22.9`

The new *Dependency* score results in a supply line score of 97.9 (`22.9 + 25 + 25 + 25 = 97.9`). Since there is one supply line that is associated with *Product 2*, the resulting *Interdependence Score* is 97.9. The `Impact Score` takes the maximum of each supporting figure for all supply lines that the node is a member of. This means that the *Impact Score* is the same as the *Interdependence Score* (97.9) since there is only one supply line.

In the *Suppliers* view, the *Impact Score* for *Supplier 2* remains unchanged at 100 because *Supplier 2* has three supply lines. The supply line associated with *Product 2 and Product 4* were not impacted. The supply line associated with *Product 3* is 97.9. The *Impact Score* takes the maximum of each supporting figure for all supply lines that the node is a member of, which means that the *Impact Score* remains unchanged at 100 (`max(25,22.9,25) +`

max(25,25,25) + max(25,25,25) + max(25,25,25) = 100). The *Interdependence Score* takes the sum of the supply line scores and decreases to 297.9 (100 + 97.9 + 100 = 297.9).

In the *Projects* view, as with *Supplier 2*, the Impact Score remains unchanged at 100 since the Impact Score takes the maximum of each supporting figure for all supply lines that the project is a member of (max(25,25,25,22.9,25) + max(25,25,25,25,25) + max(25,25,25,25,25) + max(25,25,25,25,25) = 100). The *Interdependence Score* is reduced to 497.9 (100 + 100 + 100 + 97.9 + 100 = 497.9).

Scenario 6: Answer to question, "How critical is this project to your company's mission/business?" is "5" for Project Alpha

Because the response to this question indicates a lower degree of *criticality* compared to the worst case (highest criticality), the user would expect a lower *criticality* score for Project Alpha and any related supply lines. The logic for this question in Appendix B ("IF 5, subtract 40 % of points allotted") supports this statement. Since this question is the only question in the *Project Criticality* category, the 100 points allocated to this question becomes 60 (100 – (.4(100) = 60). This category only impacts the *Dependency* supporting figure, which is reduced to 15 from 25: *((100 × 60 × 100))/ 40000 = 15*

The new *Dependency* score results in a supply line score of 90 (25 + 25 + 25 + 15 = 90). Since there are five supply lines associated with Project Alpha that each have this supply line score, resulting *Interdependence Score* is 450 (90 × 5 = 450). The *Impact Score* takes the maximum of each supporting figure for all the supply lines that the node is a member of. This means that the *Impact Score* is the same as the supply line score (90) since the supply line score for the two supply lines are the same (max(15,15,15,15,15) + max(25,25,25,25,25) + max(25,25,25,25,25) + max(25,25,25,25,25) = 90).

In the *Suppliers* view, the *Impact Score* for *Supplier 1* decreases to 90. The *Impact Score* takes the maximum of each supporting figure for the two supply lines that the node is a member of, which means the *Impact Score* decreases to 90 (max(15,15) + max(25,25) + max(25,25) + max(25,25) = 90). The *Interdependence Score* takes the sum of the supply line scores and decreases to 180 (90 + 90 = 180). *Supplier 2*'s *Impact Score* also decreases to 90. The *Impact Score* takes the maximum of each supporting figure for all supply lines that the node is a member of, which means the *Impact Score* decreases to 90 (max(15,15,15) + max(25,25,25) + max(25,25,25) + max(25,25,25) = 90). The *Interdependence Score* takes the sum of the supply line scores and decreases to 270 (90 + 90 + 90 = 270).

In the *Products* view, as with *Supplier 1* and *Supplier 2*, the *Impact Score* for *Product 1, Product 3, and Product 4*—which all have only one supply line—decreases to 90. With one supply line, the *Impact Score* and *Interdependence Score*s are the same and equal to the supply line score. Thus, the *Impact Scores* and *Interdependence Scores* for *Product 1, Product 3, and Product 4* are now 90. For *Product 2*, which has two supply lines, the *Impact Score* decreases to 90. The

Impact Score takes the maximum of each supporting figure for the two supply lines that the node is a member of, which means the *Impact Score* decreases to 90 (`max(15,15) + max(25,25) + max(25,25) + max(25,25) = 90`). The *Interdependence Score* takes the sum of the supply line scores and decreases to 180 (`90 + 90 = 180`).