Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal DateAugust 25, 2020Original Release DateMarch 13, 2020

Superseding Document

Status Final

Series/Number NIST Interagency or Internal Report 8272

Title Impact Analysis Tool for Interdependent Cyber Supply Chain Risks

Publication Date August 2020

DOI <u>https://doi.org/10.6028/NIST.IR.8272</u>

CSRC URL https://csrc.nist.gov/publications/detail/nistir/8272/final

Additional Information <u>https://csrc.nist.gov/projects/cyber-supply-chain-risk-management</u>



1 Draft NISTIR	8272
 Impact Analysis Tool for Interdepend Cyber Supply Chain Ri 	lent isks
5	
6 Celia F 7 Jon F 8 Jeff 9 Kris V 10 James 11	Paulsen Boyens rey Ng Vinkler Gimbi
12	
13	
14This publication is available free of charge15https://doi.org/10.6028/NIST.IR.82716	e from: 2-draft
17	
18	



19	Draft NISTIR 8272
20	
21	Impact Analysis Tool for Interdependent
22	Cyber Supply Chain Risks
23	
24	Celia Paulsen
25	Jon Boyens
26	Computer Security Division
27	Information Technology Laboratory
20	Leffrey Na
29 30	Kris Winkler
31	Iames Gimbi
32	Boston Consulting Group
33	New York, NY
34	
35	
36	
37	This publication is available free of charge from:
38	https://doi.org/10.6028/NIST.IR.8272-draft
39	
40	
41	
42	March 2020
43	<nt co<="" qf="" td=""></nt>
44	Sometime. Sometime.
45 46	U.S. Department of Commerce
47	Wilbur L. Ross, Jr., Secretary
48 49	National Institute of Standards and Technology
50	Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

51	National Institute of Standards and Technology Interagency or Internal Report 8272
52	62 pages (March 2020)
53	This publication is available free of charge from:
54	https://doi.org/10.6028/NIST.IR.8272-draft
55 56 57 58	Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.
59 60 61 62	There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each multipation is completed, gurrent requirements, guidelings, and precedures, where they exist, remain concepting. For

61 may be used by federal agencies even before the completion of such companion publications. Thus, until each 62 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For 63 planning and transition purposes, federal agencies may wish to closely follow the development of these new 64 publications by NIST.

65 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to 66 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at 67 <u>https://csrc.nist.gov/publications</u>.

68	Public comment period: <i>March 13, 2020</i> through April 17, 2020
69 70 71 72	National Institute of Standards and Technology Attn: Computer Security Division, Information Technology Laboratory 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930 Email: <u>scrm-nist@nist.gov</u>
73	All comments are subject to release under the Freedom of Information Act (FOIA).
74	

Reports on Computer Systems Technology

76 The Information Technology Laboratory (ITL) at the National Institute of Standards and 77 Technology (NIST) promotes the U.S. economy and public welfare by providing technical 78 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test 79 methods, reference data, proof of concept implementations, and technical analyses to advance the 80 development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for 81 82 the cost-effective security and privacy of other than national security-related information in federal 83 information systems.

84

Abstract

85 As awareness of cybersecurity supply chain risks grows among federal agencies, there is a

86 greater need for solutions that evaluate the impacts of a supply chain-related cyber event. This

87 can be a difficult activity, especially for those organizations with complex operational

88 environments and supply chains. A publicly available solution to support supply chain risk

analysis that specifically takes into account the potential impact of an event does not currently

90 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

92 assess the potential impact of cybersecurity events in their interconnected supply chains.

93

94 C-SCRM; cyber supply chain risk management; risk management; secure supply chain; supply

Keywords

94 C-SCRW, cyber supply chain fisk management, fisk management, secure supply chain, supply
 95 chain; supply chain assurance; supply chain dependencies; supply chain risk; supply chain risk

96 management; supply chain security.

Acknowledgments

98 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

101 helped to improve this publication. We would especially like to thank Nadya Bartol (Boston

102 Consulting Group) for her contribution to the content during the document development and

103 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
- 105 C-SCRM Interdependency Tool described in this document.

106

Document Conventions

107 Several of the terms used in this document are not intended to be definitive. Organizations may

108 use different terms for the concepts described herein. For example, the term "projects" as used in

109 this document may be better described as "missions" for some organizations or "business units"

110 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

- 112 on the preferred nomenclature (see Section 4.8).
- 113

116

114 When referencing any specific button, field, or text in the Tool, the text is displayed in

115 Courier New font.

Supplemental Content

117 The source code for the tool described in this document, along with sample data and multiple

118 installer packages are available on the project webpage at: <u>https://csrc.nist.gov/Projects/cyber-</u>

119 <u>supply-chain-risk-management/interdependency_tool.</u>

120 The source code, sample data, and a windows installer are also available in the NIST GitHub

121 library at <u>https://github.com/usnistgov/supply-chain-interdependency-tool</u>.

122

Call for Patent Claims

124 This public review includes a call for information on essential patent claims (claims whose use 125 would be required for compliance with the guidance or requirements in this Information 126 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be 127 directly stated in this ITL Publication or by reference to another publication. This call also 128 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications 129 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents. 130 131 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, 132 in written or electronic form, either: 133 134 a) assurance in the form of a general disclaimer to the effect that such party does not hold 135 and does not currently intend holding any essential patent claim(s); or 136 137 b) assurance that a license to such essential patent claim(s) will be made available to 138 applicants desiring to utilize the license for the purpose of complying with the guidance 139 or requirements in this ITL draft publication either: 140 141 i. under reasonable terms and conditions that are demonstrably free of any unfair 142 discrimination: or 143 ii. without compensation and under reasonable terms and conditions that are 144 demonstrably free of any unfair discrimination. 145 146 Such assurance shall indicate that the patent holder (or third party authorized to make assurances 147 on its behalf) will include in any documents transferring ownership of patents subject to the 148 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on 149 the transferee, and that the transferee will similarly include appropriate provisions in the event of 150 future transfers with the goal of binding each successor-in-interest. 151 152 The assurance shall also indicate that it is intended to be binding on successors-in-interest 153 regardless of whether such provisions are included in the relevant transfer documents. 154 155 Such statements should be addressed to: scrm-nist@nist.gov 156 157

158			Table of Contents	
159	1	Intro	duction	1
160		1.1	Purpose	1
161		1.2	Relationship to Other Publications	1
162		1.3	Audience	2
163		1.4	Location of files	2
164	2	Tool	Overview	3
165		2.1	Licensing	4
166		2.2	Use Case	4
167		2.3	Data Requirements	4
168			2.3.1 Sample Data	5
169		2.4	Security Advisory	5
170	3	Gett	ing Started	6
171		3.1	System Requirements	6
172		3.2	Installing the Tool	6
173		3.3	Running the Tool	7
174		3.4	Uninstalling the Tool	7
175		3.5	Creating CSV Files	8
176			3.5.1 CSV File Requirements	8
177			3.5.2 CSV File Optional Fields	9
178		3.6	Importing CSV Files	9
179			3.6.1 Importing Updated CSV Files	10
180			3.6.2 Handling Import Errors	11
181		3.7	Completing Questionnaires	12
182			3.7.1 Using the Artificial Answer Generator	13
183	4	User	[.] Interface	15
184		4.1	Interface Overview	15
185		4.2	Dashboard	16
186		4.3	Suppliers	17
187		4.4	Products	19
188		4.5	Projects	21
189		4.6	Suppliers, Products, and Projects Questionnaires	23
190		4.7	Visualizations	24

171		4.7.1 Hierarchy	24
192		4.7.2 Candlestick	25
193		4.7.3 Scatterplots	
194	4.8	Tool Menu	27
195	5 Res	ılts	29
196	5.1	Overview	
197	5.2	Significant Nodes	
198	5.3	Impact Scores	
199	5.4	Interdependence Scores	30
200	5.5	Assurance Scores	30
201	6 Adv	anced Configuration	31
202	6.1	Overview	31
203	6.2	Question	31
204	6.3	Question Info Text	32
205	6.4	Weight	32
206	6.5	Answers	32
207	Reference	ces	33
208			
208 209		List of Appendices	
208 209 210	Appendi	List of Appendices x A – Calculation	
208 209 210 211	Appendi Appendi	List of Appendices x A – Calculation x B – Question Categories	
208 209 210 211 212	Appendi Appendi Appendi	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example	34 38 44
208 209 210 211 212 213	Appendi Appendi Appendi	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example	34 38 44
208 209 210 211 212 213 214	Appendi Appendi Appendi	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example List of Figures	34 38 44
208 209 210 211 212 213 214 215	Appendi Appendi Appendi Figure 1:	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example List of Figures Node relationship diagram	
208 209 210 211 212 213 214 215 216	Appendi Appendi Appendi Figure 1: Figure 2:	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example List of Figures Node relationship diagram macOS Installation Window	
208 209 210 211 212 213 214 215 216 217	Appendi Appendi Appendi Figure 1: Figure 2: Figure 3:	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example List of Figures Node relationship diagram macOS Installation Window Ubuntu Linux Install Message	
208 209 210 211 212 213 214 215 216 217 218	Appendi Appendi Appendi Figure 1: Figure 2: Figure 3: Figure 4:	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example List of Figures Node relationship diagram macOS Installation Window Ubuntu Linux Install Message Importing CSV files	
208 209 210 211 212 213 214 215 216 217 218 219	Appendi Appendi Appendi Figure 1: Figure 2: Figure 3: Figure 4: Figure 5:	List of Appendices x A – Calculation x B – Question Categories	
208 209 210 211 212 213 214 215 216 217 218 219 220	Appendi Appendi Appendi Figure 1: Figure 2: Figure 3: Figure 4: Figure 5: Figure 6:	List of Appendices x A – Calculation	
208 209 210 211 212 213 214 215 216 217 218 219 220 221	Appendi Appendi Appendi Figure 1: Figure 2: Figure 3: Figure 3: Figure 5: Figure 5: Figure 5:	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example List of Figures Node relationship diagram macOS Installation Window Ubuntu Linux Install Message Importing CSV files Choosing file to import Example of inactive supplier entry. Sample import error message	
208 209 210 211 212 213 214 215 216 217 218 219 220 221 222	Appendi Appendi Appendi Appendi Figure 1: Figure 2: Figure 2: Figure 3: Figure 5: Figure 5: Figure 5: Figure 5: Figure 5:	List of Appendices x A – Calculation x B – Question Categories x C – Calculation Example List of Figures Node relationship diagram macOS Installation Window Ubuntu Linux Install Message Importing CSV files Choosing file to import Example of inactive supplier entry Sample import error message Accessing questionnaires	

Figure 10: Generate random answers dialog box
Figure 11: Top navigation bar
Figure 12: Dashboard view
Figure 13: Suppliers detail view
Figure 14: Products detail view
Figure 15: Projects detail view
Figure 16: Questionnaire user interface
Figure 17: Hierarchy visualization
Figure 18: Candlestick visualization
Figure 19: Scatterplots visualization
Figure 20: Tool menu button
Figure 21: Tool menu
Figure 22: User preferences window
Figure 23: Calculation flow
Figure 24: Supply chain diagram for example scenario45

List of Tables

241	Table 1: Import error codes	. 11
242	Table 2: Supplier Questions, Category and Logic	. 38
243	Table 3: Product Questions, Category and Logic	. 41
244	Table 4: Project Questions, Category and Logic	. 43
245	Table 5: Suppliers CSV File Structure and Contents	. 44
246	Table 6: Products CSV File Structure and Contents	. 44
247	Table 7: Projects CSV File Structure and Contents	. 44
248	Table 8: Supplier Supply Line Breakdown	. 46
249	Table 9: Products Supply Line Breakdown	. 46
250	Table 10: Project Supply Line Breakdown	. 46
251		

252 **1** Introduction

253 **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 changes; most focus on contract management or compliance. There is a need to provide organizations with a visual and systematic 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.

- 260 This publication describes one potential way to visualize and measure these impacts: a Cyber
- 261 Supply Chain Risk Management (C-SCRM) Interdependency Tool (hereafter "Tool"), which is a
- prototype tool 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
- 267 overlooked. Thus, this Tool is intended to bridge that gap and enable users and tool developers to 268 create a more complete understanding of an organization's risk by measuring impact in their
- 269 specific environments.
- 270 The Tool also provides the user greater visibility over the supply chain and the relative
- 271 importance of particular projects, products, and suppliers (hereafter referred to as "nodes")
- compared to others. This can be determined by examining the metrics which contribute to a
- 273 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
- 278 organization's supply chain and overall business.

279 **1.2** Relationship to Other Publications

- 280 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 [CSF1] [CSF2].

292 **1.3 Audience**

293 The Tool is intended for organizations that are exploring ways to improve their supply chain risk

- 294 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
- 296 where to invest in more comprehensive risk management activities. It is not intended to be a
- stand-alone solution for the holistic management of supply chain risk.
- 298 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
- 300 wish to analyze and assess cybersecurity risks in their organization's supply chain. The Tool may
- 301 also be used by developers and researchers looking at ways supply chain cybersecurity impacts
- 302 can be measured.

303 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-

306 <u>management/interdependency_tool</u> as well as in the NIST GitHub library, which can be found at: 307 https://github.com/usnistgov/supply-chain-interdependency-tool.

3082Tool 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

313 be applied.

314 For the purposes of this publication, the terms suppliers, products, and projects were chosen to

315 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

317 operational technology (IT/OT) products. Products are provided by one or more suppliers. This

318 relationship is depicted in Figure 1.



- 319
- 320

321 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.

326 Each node is given an Impact Score, an Interdependence Score, and an Assurance Score (see

327 Section 5 for more information) with illustrative visualizations to assist in the identification of

328 high-impact nodes. The Tool runs locally on the user's machine, granting the user complete

329 control over the data and algorithms used by the Tool.

330 2.1 Licensing

- 331 The software associated with this publication was developed at the National Institute of
- 332 Standards and Technology in whole or in part by employees of the Federal Government in the
- 333 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
- 336 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
- 340 warranty appears in all copies.

341 THE SOFTWARE ASSOCIATED WITH THIS PUBLICATION IS PROVIDED 'AS IS' 342 WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR 343 STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THE 344 SOFTWARE WILL CONFORM TO SPECIFICATIONS, ANY IMPLIED WARRANTIES OF 345 MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND FREEDOM FROM 346 INFRINGEMENT, AND ANY WARRANTY THAT THE DOCUMENTATION WILL 347 CONFORM TO THE SOFTWARE, OR ANY WARRANTY THAT THE SOFTWARE WILL 348 BE ERROR FREE. IN NO EVENT SHALL NIST BE LIABLE FOR ANY DAMAGES, 349 INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR 350 CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY 351 CONNECTED WITH THIS SOFTWARE. WHETHER OR NOT BASED UPON WARRANTY. 352 CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS 353 354 SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE 355 SOFTWARE OR SERVICES PROVIDED HEREUNDER.

356 **2.2 Use Case**

357 The Tool can be used in conjunction with existing risk tools used by the organization. For

- 358 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
- 360 supply chain risk. This Tool can be used with other tools that map the supply chain to create a

361 more accurate picture of the risk of sub-suppliers. It can also be used to complement governance,

- 362 risk, and compliance (GRC) tools used by the organization.
- 363 Users (e.g., organizations and developers) are encouraged to modify this Tool as they see fit to
- 364 integrate information from existing sources such as an accounting system or supplier
- 365 management portal. Users may also integrate the concepts and ideas presented herein or portions
- 366 of the source code of this Tool into their existing systems.

367 2.3 Data Requirements

368 The Tool requires two types of user input:

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

2.3.1 Sample Data

- 376 Users may test the Tool with sample data sets available here: <u>https://csrc.nist.gov/Projects/cyber-</u>
- 377 <u>supply-chain-risk-management/interdependency_tool</u> or here:
- 378 <u>https://github.com/usnistgov/supply-chain-interdependency-tool</u>. The sample data sets include:
- 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.
- Sample Data Set Interconnected: Three CSV files that provide more complicated
 supply lines. This data set contains four projects and more complex node relationships.

384 2.4 Security Advisory

385 The Tool does not contain any security mechanisms to protect the data contained within (e.g.,

- 386 password protection). All data imported and created during the use of this Tool is stored locally
- 387 on the user's file system and is not encrypted or otherwise protected by the Tool. The Tool and
- 388 related data need to be treated with care as supply chain data may be sensitive for an
- 389 organization.

390 3 Getting Started

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

392 3.1 System Requirements

- 393 The Tool was developed for use on Microsoft Windows 10, Apple macOS Mojave, or Ubuntu.
- 394 The Tool may function on different versions of Windows, Mac, and Linux operating systems,
- 395 but other versions have not been tested. Updates to the tool to ensure continued compatibility
- 396 with various operating systems is not guaranteed.
- 397 The user is required to create CSV files as input to the Tool and may require a spreadsheet
- 398 editor, such as Microsoft Excel, or a text editor, such as Notepad, nano, or vi. The user is
- 399 required to have at least 200MB of available space on the file system.

400 **3.2** Installing the Tool

- 401 The latest stable version of the Tool is v1.0.0. Binary releases for each platform and other
- 402 information related to the Tool can be found at the following sites:
- 403 <u>https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/interdependency_tool</u> or
- 404 <u>https://github.com/usnistgov/supply-chain-interdependency-tool</u>. Select the appropriate
- 405 download for the computer's operating system.
- 406 On Microsoft Windows systems, double click the file "C-SCRM-Installer.exe"
- 407 downloaded either from the project webpage or GitHub.
- 408 On Apple Macintosh systems, double click the .dmg file, and drag the C-SCRM application icon409 to the "Applications" folder as shown in Figure 2.



410

411

Figure 2: macOS Installation Window

- 412 On Linux systems, exact installation steps vary based on distribution and configuration. The
- 413 binary distributions located on the project webpage include both a Debian package file for

- 414 Ubuntu (c-scrm 1.0.0 amd64.deb) and a tar (.tar.gz) file for use with other
- 415 distributions. When downloading and running the Debian package on Ubuntu, a window similar
- 416 to that in Figure 3 may appear. Click the "Install" button to install the Tool.

<	c-scrm
~	c-scrm Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool
Install	
Cyber Suppl	y Chain Risk Management (C-SCRM) Interdependency Tool
Web	site
Details	
Version	1.0.0
Updated	Never
License	Proprietary
Source	c-scrm_1.0.0_amd64.deb
Download S	ize 295.7 MB

418

Figure 3: Ubuntu Linux Install Message

419 **3.3 Running the Tool**

420 On Microsoft Windows systems, the user can access the Tool by searching for "C-SCRM" in All

421 Applications. All Applications can be accessed by clicking the Windows icon in the toolbar,

422 which is located on the far left of the toolbar. The Tool can then be run by double-clicking the

423 "C-SCRM" result. The Tool can also be run directly by double-clicking the "C-SCRM" shortcut

424 added by the installer to the desktop. Files used to run the Tool are stored at C:\Users\[Your

425 User Name]\AppData\Local\C-SCRM.

426 On Apple Macintosh systems, the Tool can be accessed by searching for "C-SCRM" in Spotlight

427 (located in the upper right corner), or locating "C-SCRM" in the Applications folder. The Tool

428 can then be run by double-clicking the "C-SCRM" search result in Spotlight or the "C-SCRM"

- 429 row or icon in the Applications folder.
- 430 On Ubuntu Linux systems, the Tool can be accessed in the /usr/share/applications
- 431 folder. The Tool can then be run by double-clicking the "C-SCRM" application in the folder or

432 directly from the desktop when "Show Applications" is selected.

433 **3.4 Uninstalling the Tool**

434 On Microsoft Windows systems, uninstall the Tool by navigating to Settings > Apps &

- 435 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
- 437 manually. Navigate to C:\Users\[Your User Name]\AppData\Local\C-SCRM or
- 438 C:\Users\[Your User Name]\AppData\Roaming\C-SCRM, move this directory to
- 439 the Recycle Bin, and empty the Recycle Bin.

- 440 On Apple Macintosh systems, drag the installed Tool into the Trash. The folder containing the
- 441 Tool's data can be found at /Users/[Your User Name]/Library/Application
- 442 Support/C-SCRM and also needs to be deleted by right-clicking on the folder and selecting
- 443 Move to Trash or dragging the directory into the Trash.
- 444 On Ubuntu Linux systems, if the Debian package is installed, uninstall the Tool from the
- 445 terminal by running "sudo dpkg -r c-scrm." If installed from the tar file, remove the
- 446 unarchived directory. The directory location when using Ubuntu is
- 447 /home/USERNAME/.config/C-SCRM, but the exact location of the application data files
- 448 may vary based on configuration and Linux version used.

449 **3.5 Creating CSV Files**

- 450 The tool is initially populated using comma-separated (CSV) files created by the user. Data in
- 451 these files may come from a variety of sources, including accounting systems and vendor
- 452 management tools, or be manually created by leveraging institutional knowledge. This section
- 453 provides details on the three CSV files that are required to be imported. Sample template files are
- 454 available (see Section 2.2.1) to provide an example of an acceptable file format based on the
- 455 requirements described in Section 3.5.1.

456 **3.5.1 CSV File Requirements**

- 457 Three separate CSV files are required: one containing supplier information, one containing
- 458 product information, and one containing project information. While any file name may be used,
- 459 including the appropriate designation (e.g., "supplier," "product," or "project") in the file name
- 460 may simplify the import process.
- 461 The CSV files are required to contain the required fields (also known as "column headings")
- 462 outlined below. These fields are required to be included in the first row of each CSV file and463 spelled exactly as shown within the quotations:

464	1. Required fields for Supplier CSV file
465	a. "ID" – Supplier ID, user's choice of alphanumeric value
466	b. "Name" – Supplier Name
467	2. Required fields for Product CSV file
468	a. "ID" – Product ID, user's choice of alphanumeric value
469	b. "Name" – Product name
470	c. "Supplier ID" – ID of suppliers that supply this product. If there are
471	multiple suppliers, each entry is required to be separated by a semicolon (;).
472	d. "Project ID" – ID of projects that utilize this product. If there are multiple
473	projects, each entry is required to be separated by a semicolon (;).
474	3. Required fields for Project CSV file
475	a. "ID" – Project ID, user's choice of alphanumeric value

- b. "Level" Organization is recommended assigned level = '1', and projects is recommended assigned level = '1.x' where x is the project number (1.1, 1.2, etc.)
- 479 c. "Name" Project Name

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

483 **3.5.2 CSV File Optional Fields**

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

487 **3.6 Importing CSV Files**

- 488 This section details how to import the CSV files into the Tool.
- 489 1. Run the Tool (see Section 3.3). Note the IMPORT... buttons, as shown in Figure 4

 Import supplier data (CSV) Import project data (CSV) Impo	DASHBOARD	SUPPLIERS P	RODUCTS PROJECTS VISUALI	ZATIONS	
No Suppliers Provided No Products Provided No Projects Provided DETAILS IMPORT DETAILS IMPORT Figure 4: Importing CSV files 2. Click the IMPORT buttons to import the CSV files for each node type (Supplier Products, and Projects). CSV files may be imported in any order. a. Note: Future versions of this Tool may support importing a single file in	sa jogo de la companya de la company	0 0 0 Ngh	output for a line of the line		TO DO TO DO Items • Import supplier data (CSV) • Import product data (CSV) • Import project data (CSV)
 DETAILS IMPORT DETAILS IMPORT DETAILS IMPORT DETAILS IMPORT Figure 4: Importing CSV files 2. Click the IMPORT buttons to import the CSV files for each node type (Supplier Products, and Projects). CSV files may be imported in any order. a. Note: Future versions of this Tool may support importing a single file in 	No Suppliers	s Provided	No Products Provided	No Projects Provided	
 Figure 4: Importing CSV files 2. Click the IMPORT buttons to import the CSV files for each node type (<i>Supple Products</i>, and <i>Projects</i>). CSV files may be imported in any order. a. Note: Future versions of this Tool may support importing a single file in 	DETAILS IMPOR	RT	DETAILS IMPORT	DETAILS IMPORT	
 Click the IMPORT buttons to import the CSV files for each node type (Supple Products, and Projects). CSV files may be imported in any order. a. Note: Future versions of this Tool may support importing a single file in 			Figure 4: In	nporting CSV files	
<i>Products</i>, and <i>Projects</i>). CSV files may be imported in any order.a. Note: Future versions of this Tool may support importing a single file in	2. Clic	k the IMPOF	RT buttons to impor	t the CSV files for each	n node type (Suppliers
a. Note: Future versions of this I ool may support importing a single file in	Proc	<i>ducts</i> , and <i>Pi</i>	<i>cojects</i>). CSV files ma	y be imported in any or	rder.
	,	a Note Fu	ture versions of this 'l	ool may support impor	ting a single file inclu

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



Figure 5: Choosing file to import

500

501 **3.6.1** Importing Updated CSV Files

502 CSV files can be re-imported if updates are made to a data file (e.g., adding new nodes or 503 changing column values in an existing node). To re-import an updated CSV file, click the 504 IMPORT button and select the new data file

504 IMPORT... button and select the new data file.

505

506 If updates are made to the name of an existing node and/or product connections, the

- 507 visualizations and metrics are be updated to reflect this updated data. If a node is deleted, the
- 508 entry is moved to "inactive" as shown in Figure 6. If, at a later point, a new CSV file is
- 509 imported with the same ID as that of the previously deleted node, the table entry and the
- 510 questionnaire data associated with that entry will be activated.

Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool									
DASHBOARD	SUPPLIERS	PRODUCTS	PROJECTS VISUAL	IZATIONS					
# Suppleors	8 0 0 0	-0		_	Supplier Ques 5 Suppl 0 suppliers w 0 suppliers w 5 suppliers w	tion Status ier (+ 3 inactive): thit complete data th partial data th no data			
SUPPLIER	^	Impact	Interdependence	Assurance (16)	Access (supplier)	Questions Complete	Question Age	Action
Supplier 1	u -	100.0	100.0	0.0		100.0	0.0%		START
Supplier 2	2	100.0	200.0	0.0		100.0	0.0%		START
Supplier 3	3	100.0	200.0	0.0		100.0	0.0%		START
Supplier 4	1	100.0	100.0	0.0		100.0	0.0%		START
Supplier 5	5	100.0	100.0	0.0		100.0	0.0%		START
Supplier 6	î (inactive)								
Supplier 7	(inactive)								
Supplier 8	t (inactive)								

511512

Figure 6: Example of inactive supplier entry

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

515 **3.6.2 Handling Import Errors**

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



- 518
- 519

Figure 7: Sample import error message

- 520 Table 1 lists potential error messages and provides a description of how to interpret each error.
- 521

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 Section 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 Section 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.

523 **3.7 Completing Questionnaires**

524 After importing the CSV files, the user must complete questionnaires for each individual node as 525 shown in Figure 8. Currently, the questionnaire must be completed manually.

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

					2		
SUPPLIER 1	Impact	Interdependence	Assurance (%)	Access (supplier)	Questions Complete	Question Age	Action
Supplier 1	100.0	100.0	0.0	100.0	6.7%	less than 1 minute ago	EDIT
Supplier 2	100.0	200.0	0.0	100.0	0.0%		START
Supplier 3	100.0	200.0	0.0	100.0	6.7%	less than 1 minute ago	EDIT
Supplier 4	100.0	100.0	0.0	100.0	6.7%	less than 1 minute ago	EDIT
Supplier 5	100.0	100.0	0.0	100.0	0.0%		START

528

527

Figure 8: Accessing questionnaires

529 To access the questionnaires, click the *SUPPLIERS*, *PRODUCTS*, or *PROJECTS* view (see

530 Section 4) towards the top of the Tool, and then click the START... button (see #1 in Figure 8).

531 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

533 questionnaire is, the more accurate the calculated metrics are.

534 Once saved, the button in the Action column will now display EDIT... instead of START... (see

535 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

537 column indicate the questionnaire is incomplete (see #2 in Figure 8). After all questionnaires are

538 completed to the extent possible, the results are ready to be analyzed.

539 This questionnaire was developed based on subject matter experts' opinions and advice as well

540 as existing supplier risk questionnaires. The questions in the questionnaire have been selected as

541 the minimum information an organization needs to know about their suppliers, products, and

542 processes in order to gain an understanding of the potential impact that a node may have. Many

543 organizations have existing supplier questionnaires that differ from the questionnaire in this

544 Tool. Those organizations are encouraged to compare their questionnaires with the one in this

- 545 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
- 547 are included in Section 6.

548 **3.7.1** Using the Artificial Answer Generator

- 549 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
- 551 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.
- 553 To generate random sample data for the questionnaires, click on the bottom right of the question
- status box (see #1 in Figure 9).



555 556

Figure 9: Accessing random answer generator

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

Generate Random Answers

This will replace all existing answers with randomly generated answers.

	ACCESS QUESTIONS				
U	% chance question is answered				
2	response strength		70.0	D	
		50.0			
	ASSURANCE QUESTIONS				
	% chance question is answered				
	response strength		70.0	D	
		50.0			
				CANCEL	CONTINUE

559

560

Figure 10: Generate random answers dialog box

561 The box is organized by question categories: *ACCESS*, *ASSURANCE*, *CRITICALITY*, and 562 *DEPENDENCY* (see Appendix B for a listing of questions in each category). The following 563 options are provided to generate random answers:

- 564
 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 Section
 5 for more information about how scores are calculated and this default assumption.
- 572 2. Response strength: Drag the slider to set the "strength" of the answer choices. A 573 higher response strength translates to a better score. For example, a higher response 574 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 575 category translates to a lower access score (indicating that the supplier/product has less 576 access to acquirer's environment); a higher response strength in the dependency category 577 578 translates to a lower dependency score (indicating that the acquirer has low dependency 579 on the product); and a higher response strength in the assurance category translates to a 580 higher assurance score (indicating that the acquirer has a high number of implemented 581 mitigations for the supplier).

582 See Section 4 for more information about the questionnaire interface. See Section 5 for more 583 information about how to analyze the results generated.

4 User Interface

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

4.1 Interface Overview

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

Syber Supply Chain Risk Management (C-SCRM) Interdependency Tool

_	DASHBOARD	SUPPLIERS	PRODUCTS	PROJECTS	VISUALIZATI
		Figu	ure 11: Top navigation	bar	
The	Tool has five m	nain views:			
1	DASHBOAR	\boldsymbol{D} – The dashboard	provides a visual su	ummary of the avail	able Supplier
	Product, and	Project data. It als	o summarizes activ	ities that need to be	completed to
	• 1	e accurate informat	1 - 1	1	
	provide mor	c accurate mitorinat	tion for the I ool to	anaiyze.	
2	provide mor 2. SUPPLIER	s – The Suppliers v	view shows information	analyze. tion about the supp	liers that prov
2	provide mor 2. SUPPLIER products to t	s – The <i>Suppliers</i> v the organization.	view shows information	analyze. tion about the supp	liers that prov
	2. <i>SUPPLIER</i> products to t 3. <i>PRODUCTS</i>	<i>s</i> – The <i>Suppliers</i> v the organization. – The <i>Products</i> vie	view shows information	analyze. ition about the supp on about the produc	liers that prov
	 SUPPLIER, products to t PRODUCTS provide to th 	s – The Suppliers with the organization. – The Products view organization.	view shows information with the fool to a view shows information and the shows information and t	analyze. ition about the supp on about the produc	liers that prov
2	 SUPPLIER. SUPPLIER. products to t PRODUCTS provide to th PROJECTS 	<i>s</i> – The <i>Suppliers</i> v the organization. – The <i>Products</i> vie ne organization. – The <i>Projects</i> view	view shows information with the fool to a view shows information with the shows information with the shows informatic shows i	analyze. ition about the supp on about the produc on about the projects	liers that prov ets that the sup s or business u
2	 SUPPLIER, products to t PRODUCTS provide to th PROJECTS that utilize o 	 <i>s</i> – The Suppliers with organization. – The Products viewer organization. – The Projects viewer or more product 	w shows information w shows information	analyze. tion about the supp on about the produc on about the projects	liers that prov ets that the sup s or business u
2	 SUPPLIER. SUPPLIER. products to t PRODUCTS provide to th PROJECTS that utilize o VISUALIZ. 	 <i>s</i> – The Suppliers with organization. – The Products viewer organization. – The Projects viewer one or more product <i>ATIONS</i> – The Vis 	w shows information w shows information w shows information ts. <i>ualizations</i> view sh	analyze. tion about the supp on about the produc on about the projects ows the interconnect	liers that prov ts that the sup s or business u ctions betweer

603 views.

604 **4.2 Dashboard**

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

DASHBOARD	SUPPLIERS	PRODUCTS	PROJECTS	VISUALIZATIONS			
saladono s low	Assurance	-0	494 low low high	3		• Answer question • Answer question • Answer question • Answer question • Review visualiza	ns
8 Suppliers 0 suppliers with con 8 suppliers with par 0 suppliers with no DETAILS IMP(: Iplete data tial data data DRT	8 Pro 0 produ 0 produ 8 produ DETAIL:	oducts: cts with complete data cts with partial data cts with no data S IMPORT	4 0 pr 0 pr 4 pr	Projects: ojects with complete data ojects with partial data ojects with no data		

606 607

Figure 12: Dashboard view

608 There are four tiles on the Dashboard:

- 609
 1. SUPPLIERS The bar chart shows the distribution of the supplier Assurance Scores
 610 (see Section 5.5 for a description of Assurance Scores). Click the DETAILS... button to
 611 navigate to the Suppliers view. Click the IMPORT... button to import a Supplier CSV file.
- 612 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
 614 diagram. The darker colors indicate the number of products in a given category. In the
 615 example above, the bottom left-most box has a dark blue color, which means there are a
 616 large number of products that have low *Interdependence* and low *Impact* compared to
 617 other impact-interdependence combinations. Click the DETAILS... button to navigate to
 618 the *Products* view. Click the IMPORT... to import a Products CSV file.
- 619 3. *Projects* The tree diagram represents each project as a rectangular box, and each
 620 box is colored by degree of *Impact* with the darker red colors indicating higher *Impact*.
 621 Click the DETAILS... button to navigate to the *Projects* view. Click the IMPORT... button
 622 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.

626 4.3 Suppliers

DAS	Cyber Supply Chain Risk Managemen SHBOARD SUPPLIERS PRO	t (C-SCRM) Interdepend	visualizations					
1	Assumed	2		3 with the status B Suppliers: B suppliers with complete data suppliers with partial data suppliers with no data				
4	SUPPLIER 1	Impact	Interdependence	Assurance (%)	Access (supplier)	Questions Complete	Question Age	Action
	Supplier 1	75.0	75.0	12.5	33.3	86.7%	13 hours ago	EDIT
	Supplier 2	75.0	150.0	33.3	33.3	86.7%	4 days ago	EDIT
	Supplier 3	75.0	150.0	8.3	33.3	93.3%	19 hours ago	EDIT
	Supplier 4	87.5	87.5	19.2	66.7	80.0%	24 hours ago	EDIT
	Supplier 5	75.0	75.0	48.3	33.3	80.0%	23 hours ago	EDIT
	Supplier 6	87.5	262.5	35.0	66.7	86.7%	2 days ago	EDIT

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

629

Figure 13: Suppliers detail view

630 The *Suppliers* view provides additional details about the suppliers that have been imported into

631 the Tool and related metrics that have been calculated:

632 1. Supplier Visualization – Bar chart shows the distribution of supplier Assurance Scores. 633 2. Heat Map – Each box in the heat map is colored based on supplier *Impact* with 634 red/purple/pink/brown denoting higher Impact and green/orange/blue denoting lower 635 Impact (depending on the color scheme selected). See Section 4.8 for more information 636 on how to update the color scheme. The size of the box denotes supplier *Interdependence* 637 with larger boxes indicating larger Interdependence. 638 a. Get *Interdependence* and *Impact* values for each box in the heat map by hovering 639 over a rectangle. 640 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 641 642 below). 4. **Supplier Table** – Lists suppliers and key metrics. Click on the column header to sort the 643 644 table by that column's value in ascending or descending order. The dark grey columns 645 (Impact, Interdependence and Assurance) are calculated columns, which 646 means they are calculated based on information provided in the questionnaires across 647 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 648 Project views. 649 650 a. Supplier – Supplier name from imported data file. b. Impact – Indicates potential impact if supplier faces disruption. An Impact score 651 652 ranges from 0 to 100, with a score of 100 translating to devastating impact and 0 653 translating to no impact. An *Impact* score is calculated by taking the maximum

654		Access and Dependency scores for all supply lines the node is a part of (see
655		Appendix A for calculation details).
656	c.	Interdependence – Indicates influence of the supplier in the supply chain.
657		Interdependence Scores are unbounded and are calculated by adding the
658		Dependency and access scores for each supply line that node is a part of (see
659		Appendix A for calculation details). Higher scores indicate greater
660		Interdependence.
661	d.	Assurance (%) – Indicates degree of supply chain risk management security
662		mitigating actions/controls implemented by supplier. Assurance Scores range
663		from 0 to 100 with 0 translating to the absence of any mitigating controls
664		implemented. An Assurance score is calculated by averaging the Assurance
665		Scores of each supplier that a node is related to (e.g., any supplier contained in a
666		supply line that the node is a part of) (see Appendix A for calculation details).
667	e.	Access (supplier) – Supplier Access scores indicates degree of access
668		supplier has to the acquirer's sensitive assets (specifically systems, information
669		and physical location). This score is calculated by taking the average score of the
670		questions in the access section of the questionnaire. Access scores range from 0 to
671		100 with 100 translating to complete access.
672	f.	Questions Complete – Percentage of questions answered in supplier
673		questionnaire.
674	g.	Question Age – Length of time elapsed since product questionnaire has been
675		edited.
676	h.	Action - Contains the SHOW or EDIT button, which can be used to view/edit
677		the questionnaire responses for a given project.

678 **4.4 Products**

- Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool 2 3 8 Products:) products with complete data) products with partial data 3 products with no data duct A 75.0 75.0 12.5 100.0 100.0 100.0 0.0% START... 75.0 75.0 33.3 100.0 100.0 100.0 0.0% START... Product B 100.0 100.0 0.0% START ... 75.0 100.0 100.0 START... 8.3 100.0 100.0 100.0 0.0% START... Product P 162.5 33.8 0.0% START ... 100.0 100.0 100.0 0.0% START... START... 0.0%
- 679 Figure 14 provides a screenshot of *Products* detail view.

- 680
- 681

Figure 14: Products detail view

682 The *Products* view provides additional details about the products that have been imported into 683 the Tool and related metrics that have been calculated:

- 684 1. Products Visualization - Matrix shows distribution of products' Impact Score and 685 Interdependence Score with darker colors indicating more products in a given category. 686 In the example above, the bottom right-most box has a dark blue color which means there 687 are a large number of products that have low *Interdependence* and high *impact* compared 688 to other impact-interdependence combinations 2. Heat Map - Each box is colored based on product *impact* with red/purple/pink/brown 689 690 denoting higher Impact and green/orange/blue denoting lower Impact (depending on the 691 color scheme selected). The size of the box denotes product *Interdependence* with larger 692 boxes indicating larger Interdependence. a. Get Interdependence and Impact values for each box in the heat map by hovering 693 694 over a rectangle.
- 695 3. Status Box Shows the total number of products imported into the Tool and their
 696 statuses based on the number of questions answered in the products questionnaire (see
 697 #4h below).
- 698
 698
 699
 699
 699
 699 table by that column's value in ascending or descending order. The dark grey columns
 700 (Impact, Interdependence, and Assurance) are calculated based on
- 701 information provided in the node questionnaires. The light grey columns
- 702 (Criticality (product), Access (product), and Dependency
- 703 (product)) are derived directly from the associated supplier questionnaire and is not
- calculated from data in the *Suppliers* or *Project* views.

705	a.	Product – Product name from imported data file.
706	b.	Impact – Indicates potential impact to acquirer if supplier faces disruption. An
707		<i>Impact Score</i> ranges from 0 to 100, with a score of 100 translating to devastating
708		impact and 0 translating to no impact. An Impact score is calculated by taking the
709		maximum Access and Dependency scores for all supply lines the node is a part of
710		(see Appendix A for calculation details).
711	c.	Interdependence – Indicates influence of the product in the supply chain.
712		Interdependence scores are unbounded and are calculated by adding the
713		Dependency and Access scores for each supply line that node is a part of (see
714		Appendix A for calculation details). Higher scores indicate greater
715		Interdependence.
716	d.	Assurance (%) – Indicates degree of supply chain risk management security
717		mitigating actions/controls implemented by suppliers providing a product.
718		Assurance scores range from 0 to 100 with 0 translating to the absence of any
719		mitigating controls implemented. Assurance scores are calculated by averaging
720		the Assurance scores of each supplier that a node is related to (e.g., any supplier
721		contained in a supply line that the node is a part of) (see Appendix A for
722		calculation details).
723	e.	Criticality (product) – Product Criticality indicates how important
724		product is to its associated projects. If the product is connected to more than one
725		project, the project with the highest criticality value is displayed.
726	f.	Access (product) – <i>Product Access</i> indicates degree of access product has
727		to the acquirer's sensitive assets (specifically, information and physical location).
728		This score is calculated by taking the average score of the questions in the access
729		category of the questionnaire. Scores range from 0 to 100 with 100 translating to
730		complete access.
731	g.	Dependency (product) – This column is equivalent to Supplier
732		Dependency and indicates degree of dependence acquirer has on a supplier to
733		supply the project with a given product. If the product is connected to more than
734		one supplier, the supplier with the highest dependency value is displayed.
735	h.	Questions Complete – Percentage of questions answered in product
736		questionnaire.
737	i.	Question Age – Length of time elapsed since product questionnaire has been
738		edited.
739	j.	Action - Contains the SHOW or EDIT button, which can be used to view/edit
740		the questionnaire responses for a given project.
741		
/ - 1		

742 **4.5 Projects**

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

=	Cyber Supply Chain Risk Managemer	nt (C-SCRM) Interdepend	lency Tool					
DA	SHBOARD SUPPLIERS PR	ODUCTS PROJECTS	S VISUALIZATIONS					
1		2	3	3				
				Project Question Status				
				4 Projects:				
				0 projects with complete data 0 projects with partial data 4 projects with no data				
4	JECT 🛧	Impact	Interdependence	Assurance (%)	Criticality (project)	Questions Complete	Question Age	Action
	Project Alpha	87.5	300.0	18.1	100.0	0.096		START
	Project Beta	100.0	500.0	25.5	100.0	0.096		START
	Project Delta	0.0	0.0	0.0	100.0	0.0%	-	START
	Project Gamma	87.5	175.0	25.8	100.0	0.0%		START

744



754

755

766

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.

- Projects Visualization Shows projects with darker colors indicating higher *Impact* scores of individual projects.
- 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*.

- a. Get *Interdependence* and *Impact* values for each box in the heat map by hovering over a rectangle.
- 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
- 765 *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).

772	c. Interdependence – Indicates influence of the suppliers and products in the
773	supply chain. Scores are unbounded and calculated by adding the Dependency and
774	Access scores for each supply line that node is a part of (see Appendix A for
775	calculation details). Higher scores indicate greater Interdependence.
776	d. Assurance (%) – Indicates degree of supply chain risk management security
777	mitigating actions/controls implemented by suppliers related to the project
778	(specifically, its products). Assurance scores range from 0 to 100 with 0
779	translating to the absence of any mitigating controls implemented. Assurance
780	scores are calculated by averaging the Assurance scores of each supplier that a
781	node is related to (e.g., any supplier contained in a supply line that the node is a
782	part of) (see Appendix A for calculation details).
783	e. Criticality (project) – Indicates how important a project is to the
784	organization's operations
785	f. Questions Complete – Percentage of questions answered in project
786	questionnaire
787	g. Question Age – Length of time elapsed since project questionnaire has been
788	edited
789	h. Action – Contains the SHOW or EDIT button, which can be used to view/edit
790	the questionnaire responses for a given project.
791	

792 **4.6** Suppliers, Products, and Projects Questionnaires

Figure 16 provides a screenshot of the questionnaire user interface.

	Supply Chain Risk Management (C-SCRM) Interdependency Tool
Produc	t Questions: Agility EHR
gility E	HR ALL PRODUCT DETAILS
Answer ea	ch question to the best of your organization's knowledge. Questions that have no answer yet are marked with a blue bookmark. If the answer is unknown, choose "I don't know." Unanswered questions and "don't know" answers are scored as worst-case re
Access Qu	restions
📕 Is	; this product/service connected to or a part of your company's systems/networks?
	(not answered yet)
s ls	s this product/service connected to or a part of a product or service that your company provides to customers?
	(not answered vet)
D	oes this product/service process or store regulated data (e.g., PII, PFI, etc.) or your company's sensitive information (e.g., intellectual property, financial data, internal processes, etc.)?

794 795

Figure 16: Questionnaire user interface

796 The questionnaire is visible after clicking the EDIT... button under the Action column in the 797 Suppliers, Products, or Projects view.

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

NISTIR 8272 (DRAFT)

808 **4.7 Visualizations**

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

812 **4.7.1** Hierarchy

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



814815

Figure 17: Hierarchy visualization

- 816 The Hierarchy provides a representation of the supply chain in a four-tiered hierarchy format
- 817 with the organization at the top, followed by projects nodes, product nodes, and supplier nodes, 818 respectively.

819	1.	Legend – As indicated by the legend, the hexagons in the diagram denote the
820		organization or projects; the squares denote products; and the triangles denote suppliers.
821		The nodes on the chart are colored based on <i>Impact</i> with highest impact nodes in red,
822		purple, pink, and brown and lowest impact nodes in green, orange, and blue (depending
823		on color scheme selected). Interdependence is indicated based on the size of each node,
824		where larger-sized nodes have higher <i>Interdependence</i> scores than smaller-sized nodes.
825	2.	Hierarchy chart – The chart is interactive and can be manipulated in the following
826		ways:
827		a. Show additional metrics about a node by hovering over a node (denoted by a
828		hexagon, square, or triangle shape). A dialog box will appear and show Impact,
829		Interdependence, and Assurance metrics. The nodes and their direct
830		connections will also become highlighted.

- 831 b. Zoom in and out of the diagram by hovering over the Hierarchy chart and 832 scrolling up to zoom in and scrolling down to zoom out. Click a node to highlight the node, its direct connections, and the supplier 833 c. 834 connections of any product the node is connected to. Hold the control key 835 ("Ctrl") while clicking to select multiple nodes. d. Customize the chart arrangement by clicking, holding, and dragging a node 836 837 around the canvas to arrange the chart as desired. Hold control ("Ctrl") to select 838 multiple nodes and move them as a group. 839 **Note**: Any changes to the layout of the chart are preserved and reappear 840 when the Tool is reopened. 841 e. Navigate to the node's entry in a Suppliers, Products, or Projects view by doubleclicking a node. The node will appear at the top of the table, and further analysis 842 843 can be performed. 3. **Re-Center Chart** – This button allows the user to center the chart in the canvas area. 844
- 845 **4.7.2 Candlestick**
- Figure 18 provides a screenshot of the Candlestick visualization.



847

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
- 851 the *x*-axis.
- 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):

854 a. Min: Minimum value of *Impact* scores for a given supplier 855 b. Max: Maximum value of *Impact* scores for a given supplier c. Median: Median value of *Impact* scores for a given supplier 856 d. Q1: 1st Quartile, 25th percentile of *Impact* scores for a given supplier 857 e. Q3: 3rd Quartile, 75th percentile of *Impact* scores for a given supplier 858 f. Lower Fence: Lower fence of *Impact* scores is calculated as $Q1 - 1.5 \times IQR$, 859 where IQR = Interquartile range = (Q3 - Q1) and can be considered the "lower 860 limit" of the Impact scores for a given supplier. 861 g. Upper Fence: Upper fence of *Impact* scores is calculated as $Q3 + 1.5 \times IQR$, 862 863 where IQR = Interquartile range = (Q3 - Q1) and can be considered the "upper limit" of the Impact scores for a given supplier. 864

865 **4.7.3 Scatterplots**



866 Figure 19 provides a screenshot of the Scatterplot visualization.

868

874

875 876

877

867

Figure 19: Scatterplots visualization

- 869 The Scatterplot provides a visual of the distributions of *Impact* and *Interdependence* values for
- 870 each node type. The *Interdependence* value is plotted on the *y-axis*, and the *Impact* value is 871 plotted on the *x-axis*.
- F

872 1. Scatterplot Chart873 a. Hover over

- 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.

NISTIR 8272 (DRAFT)

878 **4.8 Tool Menu**

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

\equiv Cyber Supply Chain Risk Management (C-SCRM) Interdependency Tool							
DASHBOARD	SUPPLIERS	PRODUCTS	PROJECTS	VISUALIZATIONS			

- 882Figure 20: Tool menu button
- Figure 21 shows the expanded view of the Tool menu. Figure 22 shows the user preferenceswindow.

	<	
About		
2 Preferences		
3 Clear All Data		
4 Close Application		
Figure 21: Tool menu		

885 886

881

- 887
- 1. About Provides information about the Tool owner and Tool version.
- 889

	Set User	Preferences		ft			
	-	Set 0ser l'relefences					
a	Resource	Nomenclature					
Modify how resources are labeled in in the application. If no plural form is							
	provided, appended	plural is presumed to be the 1	resource designation with an "s"	1			
	Project	User Designation	Plural (optional)				
	Product	User Designation	Plural (optional)				
	Supplier	User Designation	Plural (optional)				
Ь	Visualizati	on Color Schemes					
	Choose th	Choose the color scheme to be used for visualizations					
	Brown-Gre	een (colorblind-safe)					
			CANCEL OK				
		Figure 22: User pre	ferences window				
l		Figure 22: User pre	ferences window				
efer	ences – All	Figure 22: User pre	ferences window	and co			
refer	ences – Alle es	Figure 22: User pre	ferences window	and co			
refer hemo Re	ences – Alle es source Desi fault <i>Proiec</i> i	Figure 22: User pre ows users to set preferer ignations – Type an alter	ferences window nces such as naming conventions a ernate title in the <i>User Designatio</i> ng convention does not fit an organic	and co <i>n</i> field			
efer nemo Re def	rences – Alle es source Des fault <i>Project</i> e case nome	Figure 22: User pre ows users to set preferer ignations – Type an alte // <i>Product/Supplier</i> nami nclature. For example, a	ferences window nces such as naming conventions a ernate title in the <i>User Designatio</i> ng convention does not fit an organ n organization may define the high	and co <i>n</i> field anizat			
efer hemo Re def use typ	rences – Alle es fault <i>Project</i> e case nome be as <i>Busine</i> .	Figure 22: User pre ows users to set preferer ignations – Type an alter t/Product/Supplier nami nclature. For example, a ss Units instead of Proje	ferences window nees such as naming conventions a ernate title in the <i>User Designatio</i> ng convention does not fit an organization may define the hig ects. Fill in the <i>Plural</i> field if the province of the second	and co <i>n</i> field anizat ghest r			
efer nema def use typ wo	rences – Alle es fault <i>Project</i> e case nome be as <i>Busine</i> . ord in the Us	Figure 22: User pre ows users to set preferer ignations – Type an alte <i>Product/Supplier</i> nami nclature. For example, a ss Units instead of Proje er Designation field is p	ferences window nees such as naming conventions a ernate title in the <i>User Designatio</i> ng convention does not fit an organ n organization may define the hig ects. Fill in the <i>Plural</i> field if the p not derived by simply appending a	and co <i>n</i> field anizat ghest r plural an "s"			
efer nema def use typ wo	rences – Alle es fault <i>Project</i> e case nome be as <i>Busine</i> . ord in the Us ord (e.g., the	Figure 22: User pre ows users to set preferer ignations – Type an alter t/Product/Supplier nami nclature. For example, a ss Units instead of Project er Designation field is a plural of "focus" is "focus"	ferences window nees such as naming conventions a ernate title in the <i>User Designatio</i> ng convention does not fit an organization may define the hig ects. Fill in the <i>Plural</i> field if the p not derived by simply appending a ei," not "focuss"; "foci" needs to b	and co <i>n</i> field anizat ghest r plural an "s" be add			
efer nema def use typ wo wo the	rences – Alle es fault <i>Project</i> e case nomen be as <i>Busine</i> . ord in the <i>Us</i> ord (e.g., the e <i>Plural</i> field	Figure 22: User pre ows users to set preferer ignations – Type an alte <i>Product/Supplier</i> nami nclature. For example, a ss Units instead of Proje er Designation field is n plural of "focus" is "foc 1).	ferences window nees such as naming conventions a ernate title in the <i>User Designatio</i> ng convention does not fit an organ n organization may define the hig ects. Fill in the <i>Plural</i> field if the p not derived by simply appending a ci," not "focuss"; "foci" needs to b	and co <i>n</i> field anizat ghest r plural an "s" be add			

- c. Save Click OK to save the selected preferences.
- 3. Clear All Data Clears all imported data and settings from Tool 905
- 4. Close Application Closes the Tool; all data and customizations (e.g., changes to the 906 positions of the nodes) to the Hierarchy chart are saved. 907

908

890

891

892 893

894 895

896

897

898

899

900

901 902

903

904

909 5 Results

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

911 5.1 **Overview**

- 912 After the user imports supply chain CSV files and completes node questionnaires, the tool
- 913 provides a series of scores and visualizations. The user may use these scores and visualizations to
- 914 identify highly impactful and interdependent nodes. The relative scoring associated with these
- 915 significant nodes may be used to inform C-SCRM program prioritization by highlighting where
- 916 risk-mitigating controls may be most necessary.
- 917 This section explains how to identify these significant nodes and how to understand the *Impact*,
- 918 Interdependence, and Assurance scores for each node. Each node type (Supplier, Product, and
- 919 Projects) impacts the calculation of each of these scores. Therefore, updates to one node's
- 920 questionnaire for a given node type may impact scores for nodes in a different node type. Please
- 921 see Appendix A for more details about how these scores are calculated.
- 922 **Note**: The Tool scores unanswered questionnaire questions equal to the "worst-case" answer.
- 923 This is a "fail-safe" feature designed to avoid inaccurate assumptions. For this reason,
- 924 questionnaires with no answered questions result in the highest-possible *Impact* score (100.0),
- 925 the highest possible Interdependence score (determined by the organization's supply chain
- 926 topology), and the lowest possible Assurance score (0.0). Therefore, the Tool is more accurate
- 927 if the user completes more questions.

928 **Significant Nodes** 5.2

- 929 The Visualizations view can help the user quickly identify highly impactful and interdependent
- 930 nodes in the organization's supply network. In the Hierarchy visualization, the most significant
- 931 nodes are the largest and are indicated by color (these colors may be red, purple, pink, or brown
- 932 depending on the color scheme selected by the user). Double-click a node to review the node's
- 933 complete score information and access its associated questionnaire in the Suppliers, Products, 934
- and *Projects* views. If the user wishes to improve the scores, risk mitigation actions can be
- 935 developed and implemented. See Sections 5.3 to 5.5 for more information on suggested methods 936 of score improvement.
- 937 For an alternative visualization comparing nodes within a node type, click the *Suppliers*,
- 938 *Products*, and *Projects* views to examine their respective heat maps. As in the Hierarchy
- 939 visualization, the boxes that are the largest and colored red, purple, pink, or brown are the most
- 940 critical nodes to perform further analysis on.

941 5.3 Impact Scores

- 942 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 943 944 indicate higher potential impact.

945 To reduce a node's *Impact* score, the organization needs to investigate reducing the criticality of

- 946 products and/or projects that it is connected to. It can also look at ways to reduce the dependence 947 on a given product, as well as reducing supplier and product access (data, physical, and IT
- 948 network).

949 **5.4** Interdependence Scores

950 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

952 organization and the extent to which these products are used across the organization. For

953 products, this translates to how many suppliers provide the product and in how many projects the 954 product is used. This score is unbounded and best understood in relation to the node's *Impact*

- 955 score and the *Interdependence* scores of similar nodes.
- As noted previously, the user needs to reduce an *Interdependence* score if the *Interdependence*
- 957 score of a node is high <u>relative to</u> 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
- 960 Interdependence score of a product, the organization needs to look at ways to reduce the
- 961 *Impact* score as well as the number of suppliers that supply the product.

962 **5.5** Assurance Scores

963 The Assurance score represents how completely the organization has implemented C-SCRM 964 mitigations for a particular node. This score is a percentage of implemented mitigations over 965 possible mitigations, and lower values indicate that the organization needs to work with the

966 supplier to implement mitigating controls.

967 To improve a node's *Assurance* score, the organization needs to work with suppliers to

968 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

970 questions in the Supplier Assurance question category in Appendix B for more

971 information.

972 6 Advanced Configuration

- 973 This section provides configuration instructions for advanced users to further customize the
- 974 Tool, including modifying node questionnaires and the relative weight of specific questions.
- 975 These instructions are intended for users capable of building/rebuilding web applications,
- 976 including digitally signing executables.
- 977 While the code for the Tool may be modified however an organization desires, any
- 978 configurations beyond those described in this section need to be executed by those with a high 979 degree of experience in application development.

980 **6.1 Overview**

- 981 Questions that appear in the Supplier, Product, and Project questionnaires are stored as CSV
- 982 files in the source distribution and can be found on the project webpage or in the top-level
- 983 "assets" folder of the Tool's GitHub repository. The names of these files are "supplier-
- 984 questions.csv", "product-questions.csv", and "project-questions.csv".
- 985 These files can be edited directly without needing to modify the Tool's application source code.
- 986 After making any edits to the CSV files, the application needs to be rebuilt and a distribution
- 987 created for each target platform (Windows, Mac, and Linux).
- 988 **Note**: If any changes are made and the application needs to be rebuilt, the user may wish to
- 989 digitally sign the resulting executable. This needs to be done in accordance with the 990 organization's software signing policy.
- 991 The required columns that the Tool uses as input data are: ID, Question, Answers, Type
- 992 of Question, Question Info Text, and Weight. For product and project CSV files,
- 993 there is a Relation column that is also created.
- 994 For the current version of the Tool, the addition and deletion of questions and answer choices are
- 995 *not* supported. The only columns considered editable in each CSV file are: Question,
- 996 Question Info Text, Weight, and Answers. Acceptable inputs for each of these
- 997 columns are described below.

998 **6.2 Question**

- 999 The Question column contains the text of the question and is freely editable. There are special 1000 variables that are used for certain questions.
- 1001 For product questions where the Type of question column has value "Criticality" or
- 1002 "Dependency," the variable [Project ID] is substituted with the name of the project, and
- 1003 the variable [Supplier ID] is substituted with the name of the supplier.
- 1004 If alternate nomenclature was configured in the Tool menu for the words "project," "product," or
- 1005 "supplier" (see Section 4.8), the user can also enclose "project," "product," or "supplier" in
- 1006 brackets ("{ }") to substitute the alternate text values provided. For example, if the word

- 1007 "project" has been remapped to be "business unit" in the user preferences window, any
- 1008 appearance of {project} in this column shows as business unit. If capitalization of the
- 1009 word is desired, the user needs to use {Supplier}. If the plural version of the word is
- 1010 desired, the user needs to use {suppliers} and {Suppliers}.
- 1011 For instances where the phrase {product/service} appears, this phrase remains
- 1012 product/service in the final output if the user did not configure an alternate nomenclature
- 1013 for product. If an alternate nomenclature for product was configured, the alternate
- 1014 nomenclature is substituted where the word "product" appears in the phrase
- 1015 "product/service."

1016 6.3 Question Info Text

- 1017 The same variables for Question described above can also be used for the Question Info
- 1018 Text column. The one exception is that the variables [Project ID] and [Supplier ID]
- 1019 should not be used in this column.

1020 6.4 Weight

- 1021 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
- 1023 questions within the same category (e.g., Criticality, Access, Dependency, and Assurance) and
- 1024 node type (e.g., *Supplier, Product*, and *Project*). The values in this column can be decimals. The 1025 values for each category are totaled, and the weight of a question is the value contained in the
- 1026 Weight column divided by the category total. If there is only one question in a given category,
- 1020 weight column arviad by the category total. If there is only 1027 the Weight column is not relevant.

1028 6.5 Answers

- 1029 Answers are contained in the Answer column and listed in the following format:
- 1030 value=10;label="Yes" | value=0;label="No" | value=10;label="I
- 1031 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

- 1034 semicolon ("; ") as the separator character. The label variable should contain the answer choice
- 1035 text that needs to be displayed. The value variable is the number of "points" associated with that
- 1036 answer choice. This value has no bounds, and decimals are allowed. However, it is
- 1037 recommended that a 0-10 scale is used where a 10 translates to the full number of points going to
- 1038 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,
- 1040 such as confirmed no physical access).
- 1041 For version 1, Answer options cannot be added or removed.

1042

1043	References	
	[UMD1]	University of Maryland, Robert H. Smith School of Business (2012) <i>Proof of Concept for an ICT SCRM Enterprise Assessment Package.</i> (National Institute of Standards and Technology, Gaithersburg, MD), NIST White Paper. <u>https://csrc.nist.gov/CSRC/media/Publications/white-</u> paper/2012/12/01/proof-of-concept-for-an-ict-scrm-enterprise- <u>assessment-package/final/documents/umd_ict_scrm_portal_report3.pdf</u>
	[UMD2]	University of Maryland, Robert H. Smith School of Business (2011) <i>The</i> <i>ICT SCRM Community Framework Development Project: Final Report</i> (National Institute of Standards and Technology, Gaithersburg, MD), NIST White Paper. <u>https://csrc.nist.gov/CSRC/media/Publications/white-</u> paper/2011/12/01/ict-scrm-community-framework-development-project- final-report/final/documents/umd_ict_scrm_initiatives-report2-1.pdf
	[SP 800-161]	Boyens J, Paulsen C, Moorthy R, Bartol N (2015) <i>Supply Chain Risk Management Practices for Federal Information Systems and Organizations</i> . (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. http://dx.doi.org/10.6028/NIST.SP.800-161
	[NISTIR 8179]	Paulsen C, Boyens JM, Bartol N, Winkler K (2018) <i>Criticality Analysis</i> <i>Process Model: Prioritizing Systems and Components</i> . (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8179. <u>https://doi.org/10.6028/NIST.IR.8179</u>
1044	[NIST CSF]	National Institute of Standards and Technology (2018) <i>Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.</i> (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018
1044		
1045		

1046 Appendix A – Calculation

1047 This appendix provides a detailed description of the algorithm used to calculate each node's 1048 scores in the Tool.

1049 a. Calculation Overview

- 1050 Each node is measured with the three scores described in Section 5 (the *Impact* score,
- 1051 *Interdependence* score, and *Assurance* score) and referred to in this appendix as "terminal
- 1052 scores." Terminal scores are ultimately derived from a user's questionnaire answers and the
- 1053 node's relative placement in the organization's supply chain topology.
- 1054 To calculate terminal scores from the user's questionnaire answers, the answers are first divided
- 1055 into question categories. Question categories are detailed below in Appendix A.b (Question
- 1056 **Categories**). Scores within each question category are used to determine variables known as
- 1057 "supporting figures." Supporting figures are detailed below in Appendix A.c (Supporting
- 1058 **Figures**). Simple arithmetic between these supporting figures directly determines the terminal
- 1059 scores for a given node. These final calculations are detailed below in Appendix A.d (Terminal
- 1060 **Scores**). The calculation flow is shown in Figure 23.



1062

1061

Figure 23: Calculation flow

1063 Note: "Supporting figures" are exclusively for the calculation of the terminal scores and are not1064 displayed to the user.

1065 **b. Question Categories**

- 1066 Each question is assigned to one of the categories below. The scores in each of the above 1067 categories and subcategories are calculated based on the *Logic* column in the tables of Appendix
- 1068 B and normalized to a percentage score (0 100). See Appendix B for a mapping of each
- B and normalized to a percentage score (0 100). See Appendix B for a mapping of each
- 1069 question to its respective category.

1070 **Project Questionnaire Categories**

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

1072 organization

1073 Product Questionnaire Categories

- 1074
 Product Access: Questions that detail the degree of access a particular product has to the organization's sensitive assets. There are three access subcategories:

 1075
 Product IT Network Access

 1076
 Product IT Network Access

 1077
 Product Sensitive Data Access

 1078
 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
- 1083 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

1091 c. Supporting Figures

- 1092 Supporting figures are derived from the category and subcategory scores calculated in Appendix 1093 A.a above and are normalized so that each are equally weighted (worth 25 points each). Because 1094 each of these are derived from node questionnaires, changing questionnaire answers impacts 1095 these scores. The supporting figure categories are described below.
- 1095 these scores. The supporting figure categories are described below.
- 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 (40000).

1100	Calculation:

- 1101Dependency = (Supplier Dependency x Product Criticality x1102Project Criticality) / 40000
- 11032. IT Network Access: Measure of potential negative impact in the event of an information1104and communication technology (ICT) disruption. This is the sum of the Product IT

1105Network Access and Supplier IT Network Access scores, scaled by the IT Network Access1106Criticality.1 This figure is normalized to 25 with a divisor (800).

1107 Calculation:

1108IT Network Access = ((Supplier IT Network Access + Product1109IT Network Access) x IT Network Access Criticality) / 800

1110**3.** Sensitive Data Access: Measure of potential negative impact in the event of sensitive1111data compromise. This is the sum of the Product Data Access and Supplier Data Access1112scores, scaled by the IT Network Access Criticality (see footnote 1 for item #2, IT1113Network Access Criticality). This figure is normalized to 25 with a divisor (800).

1114 Calculation:

1115	Sensitive Data Access = ((Supplier Sensitive Data Access +
1116	Product Sensitive Data Access) x Data Access Criticality)
1117	/ 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).

1122 Calculation:

1123Physical Facility Access = ((Supplier Physical Facility1124Access + Product Physical Facility Access) x Physical1125Access Criticality) / 800

1126 d. Terminal Scores

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

- 1129 **1.** *Impact Score* : The sum of the highest supporting figures in each supporting figure
- 1130 category affecting the node. This is the sum of the highest *Dependency* figure, the highest
- 1131 *IT Network Access* figure, the highest *Sensitive Data Access* figure, and the highest
- 1132 *Physical Facility Access* figure in which the node participates. This score is bounded

¹ Asset criticalities (e.g., *IT Network Access Criticality, Data Access Criticality*, and *Physical Access Criticality*) are hard-coded to 100. Future versions of this Tool may feature asset criticality tuning.

NISTIR 8272 (DRAFT)

1133		between 0 and 100 as each component figure is normalized to 25.
1134		Calculation:
1135 1136		<pre>Impact Score = max(Dependency) + max(IT Network Access) + max(Sensitive Data Access) + max(Physical Facility Access)</pre>
1137 1138 1139	2.	<i>Interdependence Score</i> : The sum of all supporting figures affecting the node. This is the sum of all <i>Dependency</i> figures, all <i>IT Network Access</i> figures, all <i>Sensitive Data Access</i> figures, and all <i>Physical Facility Access</i> figures in which the node participates.
1140		Calculation:
1141 1142 1143		<pre>Interdependence Score = sum(Dependency) + sum(IT Network Access) + sum(Sensitive Data Access) + sum(Physical Facility Access)</pre>
1144 1145 1146 1147 1148	3.	<i>Assurance Score</i> : 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 <i>Supplier Assurance</i> scores of each supplier associated with a given node; the <i>Assurance Score</i> of each supplier is equally weighted.
1149		Calculation:
1150		Assurance Score = average(Supplier Assurance) / 100

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

Appendix B – Question Categories

1154 The table below provides a listing of the questions in the questionnaire and the associated 1155 category and scoring logic for each question.

1156 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

1158 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*

1161 *Assurance* category is worth 1/12 or ~ 8.3 % of the entire score.

1162 As mentioned in Appendix A, the assumption for the metrics is the worst-case scenario (e.g.,

1163 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

1166 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

1168 the score.

1169 **a. Supplier Questions:**

- 1170 These supplier questions were developed based on a sample of existing supplier risk
- 1171 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

1173 order to gain an understanding of the potential impact that a supplier may have. Many

1174 organizations have existing supplier questionnaires that differ from the questionnaire in this

1175 Tool. Those organizations are encouraged to compare their questionnaires with the one in this

1176 Tool and, where appropriate, update their questionnaire or modify this Tool to support their

1177 questionnaire. Instructions on how to modify the questionnaire contents and question weightings

are included in Section 6.

1179

Table 2: Supplier Questions, Category, and Logic

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

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

1181 **b. Product Questions:**

1182 The information to complete this questionnaire may come from a security plan, security

1183 architecture documentation, industry information, and/or supplier questionnaires and interviews.

1184 The criticality level can be determined using the methodology detailed in NISTIR 8179,

1185 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

1187 and the organization's goals.

Table 3: Product Questions, Category, and Logic

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

consume? <i>Note:</i> 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.		allotted IF 50-75, subtract 80 % of points allotted IF 75-100, 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

1189 *The following are potential definitions that can be leveraged to more concretely define the 1190 terms "PII", "PHI" and "PCI"

- 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).

1202 c. Project Questions

1203 The criticality level can be determined using the methodology detailed in NISTIR 8179,

- 1204 Criticality Analysis Process Model: Prioritizing Systems and Components [NISTIR 8179], or an
- 1205 equivalent method. Criticality should be calculated in the context of the objectives of the project1206 and the organization's goals.
- 1207

Table 4: Project Questions, Category, and Logic

Question	Category	Logic
How critical is this project to the	Project	IF 1, no change
acquirer's mission/business?	Criticality	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

1208

1209

1210 Appendix C – Calculation Example

- 1211 This appendix walks through the calculations performed as outlined in Appendix A and
- 1212 Appendix B using an example supply chain.

1213 Part 1: Creating the Supply Chain Structure

- 1214 This supply chain can be made by modifying the "Sample Data Set -
- 1215 Interconnected" file or be made from scratch. The suppliers, products, and projects CSV
- 1216 files should contain the following structure and information:
- 1217

Table 5: Suppliers CSV File Structure and Contents

ID	Name
1	Supplier 1
2	Supplier 2

1218

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

1219

Table 7: Projects CSV File Structure and Contents

ID	Level	Name
1	1	My Organization
2	1.1	Project Alpha

1220

1221 Part 2: Scenario Overview

1222 Figure 24 depicts an example supply chain diagram.



1224

Figure 24: Supply chain diagram for example scenario

- 1225 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
- 1227 *Supplier 2*). All other products are supplied by one supplier.
- 1228 In this example, assume no questionnaire questions have been answered. With all questionnaire
- 1229 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
- 1231 suppliers and *Supplier 2* supplies three products.

1232 Part 3: Understanding Initial Conditions

- 1233 "Supply lines" are an important concept for the Tool's algorithm. Every unique combination of a
- 1234 project, product, and supplier is a "supply line." Every supply line for a given node is highlighted
- 1235 when the user hovers their mouse pointer over the node in the Hierarchy visualization in the
- 1236 *Visualizations* view. Table 8, Table 9, and Table 10 provide a detailed breakdown of the supply

1237 lines for each node from Figure 24.

1238 Supply Line Breakdown

1239

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

1240

Table 9: Products Supply Line Breakdown

Product Name	Supply Line	Supply Lines	
	Count		
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	

1241

Table 10: Project Supply Line Breakdown

Project Name	Supply Line	Supply Lines	
	Count		
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	

1242 Figures and Scores Breakdown

1243 **a. Suppliers:**

1249

1250

1251

1244

• 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.,

1252 1253	Dependency, IT Network Access, Sensitive Data Access, Physical Facility Access) has the highest possible score (25)
1255	 Interdenendence Score
1255	 Supplier 1 has an Interdemendence Score of 200 because each supply
1255	line has the highest possible score (100). There are two supply
1250	associated with Supplier 1 and $100 \times 2 = 200$
1257	associated with <i>Supplier 1</i> , and $100 \times 2 = 200$.
1238	• Supplier 2 has an Interdependence Score of 300 because each supply
1259	line has the highest possible score (100) . There are three supply lines
1260	associated with Supplier 2, and $100 \times 3 = 300$.
1261	• Assurance Score
1262	 Supplier 1 and Supplier 2 have the lowest possible score (0) because
1263	no questions have been answered.
1264	b. Products:
1265	Question Categories
1266	 Criticality, Access, and Dependency – All four products have the
1267	highest possible score (100) in every category because no questions
1268	have been answered.
1269	Terminal Scores
1270	• Impact Score
1271	 All four products have the highest possible score (100) because every
1272	component supporting figure of <i>Impact Scores</i> (i.e., <i>Dependency</i> , IT
1273	Network Access Sensitive Data Access Physical Facility Access) has
1274	the highest possible score (2.5).
1275	• Interdependence Score
1276	 Product 1 Product 3 and Product 4 have an Interdependence Score of
1277	100 because each supply line has the highest possible score (100).
1278	There are only supply lines associated with these products and $100 \times$
1270	1 = 100
1279	 Product 2 has an Interdependence Score of 200 because each supply
1200	line has the highest possible score (100). There are two supply
1201	according to the inglest possible score (100). There are two supply lines
1202	associated with this product, and $100 \times 2 = 200$.
1283	• Assurance Score
1284	• All products have the lowest possible score (0) because no questions
1285	have been answered.
1286	c. Projects:
1287	Question Categories
1288	• <i>Criticality</i> – Project Alpha has the highest possible score (100) because no
1289	questions have been answered.
1290	Terminal Scores
1291	• Impact Score
	1

1292	 Project Alpha has the highest possible score (100) because every
1293	component supporting figure of Impact Scores (e.g., Dependency, IT
1294	Network Access, Sensitive Data Access, Physical Facility Access) has
1295	the highest possible score (25).
1296	Interdependence Score
1297	 Project Alpha has an Interdependence Score of 500 because each
1298	supply line has the highest possible score (100). There are five supply
1299	lines associated with Project Alpha, and $100 \times 5 = 500$.
1300	Assurance Score
1301	 Project Alpha has the lowest score (0) due to worst case (no controls
1302	implemented) assumption.

1303 Part 4: Questionnaire modifications and resulting impacts on figures and scores

1304 To reduce complexity, the scenarios below change only one variable at a time. The reader can 1305 use this information to infer the influence of changing multiple variables together. This method 1306 of decomposing the influence of each part of the questionnaire is for the user's understanding 1307 only. The user needs to answer all questions in the questionnaire and interpret the results based

1308 on those responses alone.

1309 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*

1312 *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*

1317 Access subcategory, the 100 points allocated to this question become 0. This only impacts the IT 1318 Network Access supporting figure, which is now reduced to 12.5 from 25: $((0 + 100) \times$

- $1319 \quad 100) / \ 800 = 12.5$
- 1320 The new *IT Network Access* score results in a supply line score of 87.5 (25 + 12.5 + 25 +
- 1321 25 = 87.5). Since there are two supply lines that are associated with Supplier 1 that each have
- 1322 this supply line score, the result is an Interdependence Score of 175 (87.5 x 2 =
- 1323 175). The *Impact Score* takes the maximum of each supporting figure for all supply lines that
- 1324 the node is a member of. This means that the *Impact Score* is the same as the supply line score
- 1325 since the supply line score for the two supply lines are the same (max (25, 25) +
- 1326 $\max(12.5, 12.5) + \max(25, 25) + \max(25, 25) = 87.5$).

1327 As a result of these changes, the *Impact* and *Interdependence Score* on the *Products* page for

- 1328 *Product 1* and *Product 2* have changed. This is because each product has a supply line with
- 1329 Supplier 1 in it. Product 1 only has one supply line and therefore takes the same supply line

- 1330 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 Interdependence Score for Product 1 is
- 1332 now 87.5. *Product 2* has two supply lines. The supply line associated with *Supplier 1* has a score
- 1333 of 87.5. However, the supply line associated with *Supplier 2* was not impacted, and the supply
- 1334 line score remains unchanged at 100. The *Impact Score* takes the maximum of each supporting
- 1335 figure for all supply lines that the node is a member of, which means the *Impact Score* remains
- 1336 unchanged at 100 (max (25, 25) + max (25, 12.5) + max (25, 25) + max (25, 25)
- 1337 100). Interdependence score takes the sum of the suppry line scores and decreases to 187. 1338 (100 + 87.5 = 187.5).
- 1339 In the *Projects* view, as with *Product 2*, the *Impact Score* remains unchanged at 100 since the
- 1340 *Impact Score* takes the maximum of each supporting figure for all supply lines that the project is
- 1341 a member of $(\max(25, 25, 25, 25, 25) + \max(12.5, 12.5, 25, 25, 25) +$
- 1342 max(25,25,25,25,25) + max(25,25,25,25,25) = 100). The Interdependence
- 1343 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

- 1346 Because the response to this question indicates a higher degree of assurance compared to the
- 1347 worst case (no assurance), the user would expect a higher Assurance Score for Supplier 2 and
- 1348 any related supply lines. The logic for this question in Appendix B ("IF 5-10 years, add 80% of
- 1349 points allotted") supports this statement. There are 12 questions in the Supplier
- 1350 Assurance category, and since each question is equally weighted in the default configuration,
- 1351 each question has a total of ~8.3 points (1/12) allotted. This category only impacts the Assurance
- 1352 Score. Thus, the Assurance Score increases from 0 to 6.7 (80% of 8.3 = 6.7).
- 1353 In the *Products* view, the Assurance Score is calculated by averaging the Assurance Scores of all
- 1354 suppliers that supply a given product. The *Assurance Score* of *Product 1* is unchanged because
- 1355 *Product 1* is not supplied by *Supplier 2*. *Product 3* and *Product 4* are both supplied only by
- 1356 Supplier 2, so each also gets an Assurance Score of 6.7. Product 2 is supplied by both Supplier 1
- 1357 and *Supplier 2*. The supply line associated with *Supplier 1* remains unchanged with an *Assurance*
- 1358 *Score* of 0. The supply line associated with *Supplier 2* has increased to 6.7. The resulting
- 1359 Assurance Score for Product 2 is 3.3 (Average (6.7,0)/100 = 3.3 %).
- 1360 In the *Projects* view, the resulting *Assurance Score* for Project Alpha is 3.3 because both
- 1361Supplier I and Supplier 2 supply products within the project (Average (6.7,0)/100 =13623.3 %).
- 1362 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

- 1365 Because the response to this question indicates a lower degree of access compared to the worst
- 1366 case (full access), the user would expect a lower access score for *Product 2* and any related
- 1367 supply lines. The logic for this question in Appendix B ("subtract 100 % of points allotted")

- 1368 supports this statement. Since this question is the only question in the *Product Physical Facility* 1369 Access subcategory, the 100 points allocated to this question becomes 0. This category only 1370 impacts the *Physical Facility Access* supporting figure, which is now reduced to 12.5 from 25: 1371 $((100 + 0) \times 100) / 800 = 12.5$
- 1372 The new *Physical Facility* Access score results in a supply line score of 87.5 (25 + 25 + 1373 25 + 12.5 = 87.5). Since there are two supply lines that are associated with *Product 2* that 1374 each have this supply line score, the resulting *Interdependence Score* is 175 (87.5 \times 2 = 1375 175). The Impact Score takes the maximum of each supporting figure for all supply lines that 1376 the node is a member of. This means that the *Impact Score* is the same as the supply line score 1377 (87.5) since the supply line score for the two supply lines are the same (max(25, 25) +
- 1378 $\max(25, 25) + \max(25, 25) + \max(12.5, 12.5) = 87.5).$
- 1379 In the Suppliers view, the Impact Score for Supplier 1 remains unchanged at 100 because
- 1380 Supplier 1 has two supply lines. The supply line associated with *Product 1* was not impacted.
- 1381 The supply line associated with *Product 2* is 87.5. The Impact Score takes the maximum of 1382
- 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) + 1383
- 1384 $\max(25, 25) + \max(25, 12.5) = 100$). The Interdependence Score takes the sum of the 1385 supply line scores and decreases to 187.5(100 + 87.5 = 187.5). Supplier 2's Impact
- 1386 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 1387
- 1388 *Product 2* is 87.5. The Impact Score takes the maximum of each supporting figure for all
- 1389 supply lines that the node is a member of, which means the Impact Score remains
- 1390 unchanged at 100 (max (25, 25, 25) + max (25, 25, 25) + max (25, 25, 25) +
- 1391 max (12.5, 25, 25) = 100). The *Interdependence Score* takes the sum of the supply line
- 1392 scores and decreases to 287.5 (87.5 + 100 + 100 = 287.5).
- 1393 In the *Projects* view, as with *Supplier 1* and *Supplier 2*, the Impact Score remains 1394 unchanged at 100 since the Impact Score takes the maximum of each supporting figure for
- 1395 all supply lines that the project is a member of (max (25, 25, 25, 25, 25) +
- 1396 max(25,25,25,25,25) + max(25,25,25,25,25) +
- 1397 $\max(25, 12.5, 12.5, 25, 25) = 100$). The Interdependence Score is reduced to 475 (100) 1398 +87.5 + 87.5 + 100 + 100 = 475).

1399 Scenario 4: Answer to question, "What is the criticality of this product/service to the 1400 project 'Project Alpha'?" is "5" for Product 2

- 1401 Because the response to this question indicates a lower degree of criticality compared to the
- 1402 worst case (highest criticality), the user would expect a lower criticality score for *Product 2* and
- 1403 any related supply lines. The logic for this question in Appendix B ("IF 5, subtract 40 % of
- 1404 points allotted") supports this statement. Since this question is the only question in the Product
- 1405 *Criticality* category, the 100 points allocated to this question becomes 60(100 - (.4(100)))
- 1406 = 60). This category only impacts the Dependency supporting figure, which is now reduced

1407 to 15 from 25: $((100 \times 60 \times 100) / 40000 = 15)$

1408 The new Dependency score results in a supply line score of 90 (25 + 25 + 25 + 15 =1409 90). Since there are two supply lines that are associated with *Product 2* that each have this 1410 supply line score, the resulting *Interdependence Score* is 175 (90 x 2 = 180). The Impact 1411 Score takes the maximum of each supporting figure for all supply lines that the node is a 1412 member of. This means that the Impact Score is the same as the supply line score (90) since 1413 the supply line scores for the two supply lines are the same (max (15, 15) + max (25, 25) 1414 + max (25, 25) + max (25, 25) = 90).

1415 In the Suppliers view, the Impact Score for Supplier 1 remains unchanged at 100. This is 1416 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 1417 1418 maximum of each supporting figure for all supply lines that the node is a member of, which 1419 means that the Impact Score remains unchanged at 100 (max (25, 15) + max (25, 25) 1420 $+ \max(25, 25) + \max(25, 25) = 100$). The Interdependence Score takes the sum of the 1421 supply line scores and decreases to 190 (100 + 90 = 190). Supplier 2's Impact Score 1422 also remains unchanged at 100 because Supplier 2 has three supply lines. The supply line 1423 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 1424 1425 that the node is a member of, which means that the Impact Score remains unchanged at 100 1426 $(\max(15, 25, 25) + \max(25, 25, 25) + \max(25, 25, 25) + \max(25, 25, 25) =$ 1427 100). The *Interdependence Score* takes the sum of the supply line scores, and decreases to 287.5 1428 (90 + 100 + 100 = 290).

1429 In the *Projects* view, as with *Supplier 1* and *Supplier 2*, the Impact Score remains

1430 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) +

1432 $\max(25, 25, 25, 25, 25, 25) + \max(25, 25, 25, 25, 25, 25) + \max(25, 25, 25, 25, 25, 25)$ 1433= 100). The Interdependence Score is reduced to 480 (100 + 90 + 90 + 100 + 100 =1434480).

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

1437 Because the response to this question indicates a lower degree of dependence compared to the 1438 worst case (highest dependence), the user would expect a lower Dependency score for *Product*

1439 *3* and any related supply lines. The logic for this question in Appendix B ("IF 25-50, subtract 50

1440 % of points allotted") supports this statement. There are six questions in the Supplier

1441 Dependency category. Thus, since each question is equally weighted in the default

1442 configuration, each question has a total of ~16.7 points (1/6) allotted. The Supplier Dependency

1443 score decreases from 100 to 91.7 (100 - (50% of 16.7) = 91.7). This category only

1444 impacts the Dependency supporting figure, which is reduced to 22.9 from 25: ((91.7 \times

1445 100 x 100))/ 40000 = 22.9

- 1446 The new Dependency score results in a supply line score of 97.9(22.9 + 25 + 25 + 25 =
- 1447 97.9). Since there is one supply line that is associated with *Product 2*, the resulting
- 1448 Interdependence Score is 97.9. The Impact Score takes the maximum of each supporting
- 1449 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.
- 1451 In the *Suppliers* view, the *Impact Score* for *Supplier 2* remains unchanged at 100 because
- 1452 Supplier 2 has three supply lines. The supply line associated with Product 2 and Product 4 were
- 1453 not impacted. The supply line associated with *Product 3* is 97.9. The *Impact Score* takes the
- 1454 maximum of each supporting figure for all supply lines that the node is a member of, which
- 1455 means that the *Impact Score* remains unchanged at 100 (max (25, 22.9, 25) +
- 1456 max (25, 25, 25) + max (25, 25, 25) + max (25, 25, 25) = 100). The 1457 Interdependence Score takes the sum of the supply line scores and decreases to 297.9 (100 +
- 1458 97.9 + 100 = 297.9).
- 1459 In the Projects view, as with Supplier 2, the Impact Score remains unchanged at 100 since
- 1460 the Impact Score takes the maximum of each supporting figure for all supply lines that the
- 1461 project is a member of (max (25, 25, 25, 22.9, 25) + max (25, 25, 25, 25, 25) +
- 1462 $\max(25, 25, 25, 25, 25) + \max(25, 25, 25, 25, 25) = 100$). The Interdependence 1463 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

1466 Because the response to this question indicates a lower degree of *criticality* compared to the

- 1467 worst case (highest criticality), the user would expect a lower *criticality* score for Project
- 1468 Alpha and any related supply lines. The logic for this question in Appendix B ("IF 5, subtract
- 1469 40 % of points allotted") supports this statement. Since this question is the only question in the 1470 $P_{\rm ext}$ (0.(100)
- 1470 Project Criticality category, the 100 points allocated to this question becomes 60 (100 1471)
- 1471 (.4(100) = 60). This category only impacts the *Dependency* supporting figure, which is
- 1472 reduced to 15 from 25: $((100 \times 60 \times 100)) / 40000 = 15$
- 1473 The new Dependency score results in a supply line score of 90 (25 + 25 + 25 + 15 =
- 1474 90). Since there are five supply lines associated with Project Alpha that each have this supply
- 1475 line score, resulting *Interdependence Score* is $450 (90 \times 5 = 450)$. The *Impact Score* takes
- 1476 the maximum of each supporting figure for all the supply lines that the node is a member of. This
- 1477 means that the *Impact Score* is the same as the supply line score (90) since the supply line score
- 1478 for the two supply lines are the same (max (15, 15, 15, 15, 15) +
- 1479 $\max(25, 25, 25, 25, 25) + \max(25, 25, 25, 25, 25) + \max(25, 25, 25, 25, 25)$ 1480 = 90).
- 1481 In the Suppliers view, the Impact Score for Supplier 1 decreases to 90. The Impact Score takes
- 1482 the maximum of each supporting figure for the two supply lines that the node is a member of,
- 1483 which means the Impact Score decreases to $90 \pmod{15,15} + \max{25,25} +$

1484max(25,25) + max(25,25) = 90). The Interdependence Score takes the sum of the1485supply line scores and decreases to 180(90 + 90 = 180). Supplier 2's Impact Score also1486decreases to 90. The Impact Score takes the maximum of each supporting figure for all supply1487lines that the node is a member of, which means the Impact Score decreases to 901488(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 2701490(90 + 90 + 90 = 270).

- 1491 In the Products view, as with Supplier 1 and Supplier 2, the Impact Score for Product 1, Product
- 1492 *3, and Product 4*—which all have only one supply line—decreases to 90. With one supply line,
- 1493 the *Impact Score* and *Interdependence Scores* are the same and equal to the supply line score.
- 1494 Thus, the Impact Scores and Interdependence Scores for Product 1, Product 3, and Product 4 are
- 1495 now 90. For *Product 2*, which has two supply lines, the *Impact Score* decreases to 90. The
- 1496 *Impact Score* takes the maximum of each supporting figure for the two supply lines that the node 1497 is a member of, which means the *Impact Score* decreases to 90 (max(15, 15) +
- 1498 $\max(25, 25) + \max(25, 25) + \max(25, 25) = 90$). The Interdependence Score takes
- 1499 the sum of the supply line scores and decreases to 180(90 + 90 = 180).