

2 **Using Business Impact Analysis to**
3 **Inform Risk Prioritization and Response**

4
5 Initial Public Draft
6

7 Stephen Quinn
8 Nahla Ivy
9 Matthew Barrett
10 Larry Feldman
11 Daniel Topper
12 Greg Witte
13 R. K. Gardner
14

15
16
17
18 This publication is available free of charge from:
19 <https://doi.org/10.6028/NIST.IR.8286D.ipd>
20

Using Business Impact Analysis to Inform Risk Prioritization and Response

Initial Public Draft

Stephen Quinn
*Computer Security Division
Information Technology Laboratory*

Matthew Barrett
*CyberESI Consulting Group, Inc.
Baltimore, MD*

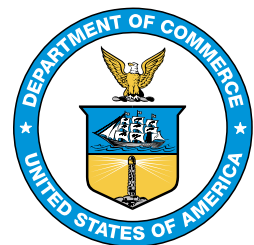
Nahla Ivy
*Enterprise Risk Management Office
Office of Financial Resource Management*

Larry Feldman
Daniel Topper
Greg Witte
*Huntington Ingalls Industries
Annapolis Junction, MD*

R. K. Gardner
*New World Technology Partners
Annapolis, MD*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8286D.ipd>

June 2022



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

57 National Institute of Standards and Technology Interagency or Internal Report 8286D
58 Initial Public Draft
59 24 pages (June 2022)

60 This publication is available free of charge from:
61 <https://doi.org/10.6028/NIST.IR.8286D.ipd>

62 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
63 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
64 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
65 available for the purpose.

66 There may be references in this publication to other publications currently under development by NIST in accordance
67 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,
68 may be used by federal agencies even before the completion of such companion publications. Thus, until each
69 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For
70 planning and transition purposes, federal agencies may wish to closely follow the development of these new
71 publications by NIST.

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

75 **Public comment period:** June 9, 2022 – July 18, 2022

76 **Submit comments on this publication to:** nistir8286@nist.gov

77 National Institute of Standards and Technology
78 Attn: Applied Cybersecurity Division, Information Technology Laboratory
79 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

80 All comments are subject to release under the Freedom of Information Act (FOIA).

81

Reports on Computer Systems Technology

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

90

Abstract

91 While business impact analysis (BIA) has historically been used to determine availability
92 requirements for business continuity, the process can be extended to provide broad
93 understanding of the potential impacts to the enterprise mission from any type of loss. The
94 management of enterprise risk requires a comprehensive understanding of the mission-essential
95 functions (i.e., what must go right) and the potential risk scenarios that jeopardize those
96 functions (i.e., what might go wrong).

97 The process described in this publication helps leaders determine which assets enable the
98 achievement of mission objectives and to evaluate the factors that render assets as critical and
99 sensitive. Based on those factors, enterprise leaders provide risk directives (i.e., risk appetite and
100 tolerance) as input to the BIA. System owners then apply the BIA to developing asset
101 categorization, impact values, and requirements for the protection of critical or sensitive assets.
102 The output of the BIA is the foundation for ERM/CSRM process, as described in the NISTIR
103 8286 series, and enables consistent prioritization, response, and communication regarding
104 information security risk.

105

Keywords

106 Business Impact Analysis; Cybersecurity Risk Management; Cybersecurity Risk Register;
107 Enterprise Risk Management; Information and Communications Technology.

108

Audience

109 The primary audience for this publication includes public- and private-sector cybersecurity
110 professionals at all levels who understand cybersecurity but may be unfamiliar with the details of
111 enterprise risk management (ERM). The secondary audience includes both federal and non-
112 Federal Government corporate officers, high-level executives, ERM officers and staff members,
113 and others who understand ERM but may be unfamiliar with the details of cybersecurity. All
114 readers are expected to gain an improved understanding of how cybersecurity risk management
115 (CSRM) and ERM complement and relate to each other as well as the benefits of integrating
116 their use.

117

118

Call for Patent Claims

119 This public review includes a call for information on essential patent claims (claims whose use
120 would be required for compliance with the guidance or requirements in this Information
121 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
122 directly stated in this ITL Publication or by reference to another publication. This call also
123 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
124 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

125

126 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
127 in written or electronic form, either:

128

129 a) assurance in the form of a general disclaimer to the effect that such party does not hold
130 and does not currently intend holding any essential patent claim(s); or

131

132 b) assurance that a license to such essential patent claim(s) will be made available to
133 applicants desiring to utilize the license for the purpose of complying with the guidance
134 or requirements in this ITL draft publication either:

135

136 i. under reasonable terms and conditions that are demonstrably free of any unfair
137 discrimination; or

138 ii. without compensation and under reasonable terms and conditions that are
139 demonstrably free of any unfair discrimination.

140

141 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
142 on its behalf) will include in any documents transferring ownership of patents subject to the
143 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
144 the transferee, and that the transferee will similarly include appropriate provisions in the event of
145 future transfers with the goal of binding each successor-in-interest.

146

147 The assurance shall also indicate that it is intended to be binding on successors-in-interest
148 regardless of whether such provisions are included in the relevant transfer documents.

149

150 Such statements should be addressed to: nistir8286@nist.gov

151 **Executive Summary**

152 Risk is measured in terms of impact on enterprise mission, so it is vital to understand the various
153 information and technology (IT) assets whose functions enable that mission. Each asset has a
154 value to the enterprise. For government enterprises, many of those IT assets are key components
155 for supporting critical services provided to citizens. For corporations, IT assets have a direct
156 influence on enterprise capital and valuation, and IT risks can have a direct impact on the
157 balance sheet or budget. For each type of enterprise, it is both vital and challenging to determine
158 the conditions that will truly impact a mission. Today’s government agencies continue to provide
159 critical services, yet they must also adhere to priority directives from senior leaders. In the
160 commercial world, mission priority is often driven by long-term goals as well as factors that
161 might impact the next quarter’s earnings call. Therefore, it is highly important to continually
162 analyze and understand the enterprise resources that enable enterprise objectives and that can be
163 jeopardized by cybersecurity risks.

164 The NIST Interagency or Internal Report (NISTIR) 8286 series has coalesced around the risk
165 register as a construct for storing and a process for communicating risk data [NISTIR8286].
166 Another critical artifact of risk management that serves as both a construct and a means of
167 communication with the risk register is the Business Impact Analysis (BIA) Register. The BIA
168 examines the potential impact associated with the loss or degradation of an enterprise’s
169 technology-related assets based on a qualitative or quantitative assessment of the criticality and
170 sensitivity of those assets and stores the results in the BIA Register. An asset criticality or
171 resource dependency assessment identifies and prioritizes the information assets that support the
172 enterprise’s critical missions. Similarly, assessments of asset sensitivity identify and prioritize
173 information assets that store, process, or transmit information that must not be modified or
174 disclosed to unauthorized parties. In the cybersecurity realm, the use of the BIA has historically
175 been limited to calculations of quality-based and time-based objectives for incident handling
176 (including continuity of operations and disaster recovery).

177 Because the BIA serves as a nexus for understanding risk (which is the measurement of
178 uncertainty on the mission), it provides a basis for risk appetite and tolerance values as part of
179 the enterprise risk strategy.¹ That guidance supports performance and risk metrics based on the
180 relative value of enterprise assets to communicate and monitor CSRM activities, including
181 measures determined to be key performance indicators (KPIs) and key risk indicators (KRIs).
182 BIA supports asset classification that drives requirements, risk communications, and monitoring.

183 Expanding use of the BIA to include confidentiality and integrity considerations supports
184 comprehensive risk analysis. The basis of asset valuation on enterprise impact helps to better
185 align risk decisions to enterprise risk strategy. CSRM/ERM integration helps to complete the risk
186 cycle by informing future iterations of impact analysis based on previous information gained
187 through cybersecurity risk register (CSRR) aggregation, as detailed in NISTIR 8286C. As

¹ OMB Circular A-123 defines risk appetite as “the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization’s most senior level leadership and serves as the guidepost to set strategy and select objectives.” The same document defines *risk tolerance* as “the acceptable level of variance in performance relative to the achievement of objectives.”

188 organizational and enterprise leaders gain an understanding of aggregate risk exposure and
189 composite impact, that information helps adjust risk expectations (including business impact
190 guidance to ensure ongoing balance among asset value, resource optimization, and risk
191 considerations).

192 The BIA process enables system owners to record the benefits provided by an asset by
193 considering the contribution to the enterprise, particularly in terms of mission, finance, and
194 reputational aspects. Informed about how each asset supports enterprise value, system owners
195 can then work with risk managers to determine the implications of uncertainty on those assets.

196 It is more critical than ever to have centralized and reliable asset information recorded in the BIA
197 Register since enterprises increasingly rely on various types of information and communications
198 technology (ICT) resources, which are increasingly targeted by adversaries. The BIA process
199 provides information that can be consistently recorded in a centralized registry of important asset
200 management information, such as system ownership, contact information for key stakeholders,
201 and characteristics of the physical devices (or services). Since asset management is an important
202 element of cybersecurity risk management, this information is quite valuable for protecting the
203 asset, detecting cyber events, responding quickly to potential issues, and recovering services
204 when necessary.

205 Public- and private-sector enterprises must maintain a continual understanding of potential
206 business impacts, the risk conditions that might lead to those impacts, and the steps being taken
207 (as recorded in various risk registers and, ultimately, in the Enterprise Risk Profile). In many
208 cases, when a company or agency is asked about risks, they are being asked to describe potential
209 impacts. Companies must describe the risk factors that could have a material adverse effect on
210 the enterprise's financial position, its ability to operate, or its corporate cash flow. Agencies must
211 report to legislative and regulatory stakeholders about adverse impacts that could impair agency
212 funding and mission. Use of the BIA methodology to categorize the criticality and *sensitivity* of
213 enterprise assets enables effective risk management and the subsequent integration of reporting
214 and monitoring at the enterprise level to ensure that risk and resource utilization are optimized in
215 light of the value of those assets.

216 **Table of Contents**

217 **Executive Summary iv**

218 **1 Introduction 1**

219 1.1 Benefits of Extending the BIA for All Risk Types 1

220 1.2 Foundational Practices for Business Impact Analysis..... 2

221 1.3 Document Structure 2

222 **2 Cataloging and Categorizing Assets Based on Enterprise Value..... 4**

223 2.1 Identification of Enterprise Business Asset Types 4

224 2.2 The Business Impact Analysis Process 4

225 2.3 Determining Asset Value to Support CSRM Activities 7

226 2.4 Determining Loss Scenarios and Their Consequences 8

227 2.5 Business Impact Analysis in Terms of Criticality and Sensitivity 10

228 2.6 Using a BIA to Record Interdependencies 11

229 2.7 Consistent Business Impact Analysis Through an Enterprise Approach..... 12

230 2.8 Using a BIA to Support an Enterprise Registry of System Assets 13

231 **3 Conclusion 14**

232 **References 15**

233

234 **List of Appendices**

235 **Appendix A— Acronyms 16**

236

237 **List of Figures**

238 Figure 1: Integration of BIA Process with Cybersecurity Risk Management..... 5

239 Figure 2: Level 3 BIA Activities..... 6

240 Figure 3: Impacts of Enterprise Assets for a Business or Agency 8

241 Figure 4: Elements of Information Risk Identification (from NISTIR 8286A)..... 9

242

243 **1 Introduction**

244 Risk is measured in terms of impact on the enterprise mission, so it is vital to understand the
245 various information and communications technology (ICT) assets whose functions enable that
246 mission, as well as any potential uncertainties that jeopardize those assets. Each IT asset has a
247 value to the enterprise. For government enterprises, many of those IT assets are key components
248 for supporting critical services provided to citizens. For corporations, IT assets have a direct
249 influence on enterprise capital and valuation, and IT risks can have a direct impact on the
250 balance sheet or budget. For each type of enterprise, it can be challenging to determine what
251 conditions will truly impact the mission. Today’s government agencies continue to provide
252 critical services, yet they must also adhere to priority directives from senior leaders. In the
253 commercial world, mission priority is often driven by long-term goals as well as impacts on the
254 next quarter’s earnings call. Therefore, it is highly important to continually analyze and
255 understand the enterprise resources that enable enterprise objectives and that can be jeopardized
256 by cybersecurity risks.

257 The NIST Interagency or Internal Report (NISTIR) 8286 series has coalesced around the risk
258 register as a construct for storing and a process for communicating risk data [[NISTIR8286](#)].
259 Another critical artifact of risk management that serves as both a construct and a means of
260 communication with the risk register is the Business Impact Analysis (BIA) Register. The BIA
261 examines the potential impact associated with the loss or degradation of an enterprise’s
262 information assets based on a qualitative or quantitative assessment of the criticality and
263 sensitivity of those assets. An asset criticality or resource dependency assessment identifies and
264 prioritizes the information assets that support the enterprise’s critical missions. Similarly,
265 assessments of asset sensitivity identify and prioritize information assets that store, process, or
266 transmit information that must not be modified or disclosed to unauthorized parties.

267 *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*, NISTIR 8286A,
268 points out that

269 ...the first prerequisite for risk identification is the determination of enterprise
270 assets that could be affected by risk. Assets are not limited to technology; they
271 include any resource that helps to achieve the mission (e.g., people, facilities,
272 critical data, intellectual property, services).

273 Section 2 of that NISTIR further describes BIA as a helpful process “to consistently evaluate,
274 record, and monitor the criticality and sensitivity of enterprise assets. The BIA categorization
275 can, in turn, inform the establishment of risk tolerance levels.”

276 **1.1 Benefits of Extending the BIA for All Risk Types**

277 The BIA is broadly recognized as a proven method for business continuity and disaster recovery
278 planning and prioritization. BIA processes and templates enable the discussion and
279 documentation of recovery objectives and service delivery criteria for important business
280 applications. Availability considerations, however, only comprise a portion of the types of
281 cybersecurity risks facing the enterprise. In fact, many recent attack patterns indicate that an
282 adversary is likely to combine attack types. For example, a criminal might encrypt important

283 company information (causing availability impact) while also threatening to disclose those same
284 sensitive corporate records (causing confidentiality impact) unless a ransom is paid. A
285 consideration of the potential harmful impacts of loss on important assets enables risk planning
286 and prepares for the completion of cybersecurity risk registers (CSRRs) as described in this
287 NISTIR 8286 series.

288 Enterprise stakeholders can also use the BIA process to identify enterprise resources that use
289 critical information types. In addition to internal reasons for protecting critical and sensitive
290 information, enterprises may also need to categorize assets for mandatory external compliance.
291 Many regulations and contractual requirements stipulate that certain critical and sensitive
292 information must be protected, so the BIA determination helps to understand where those
293 mandates apply.

294 The BIA provides a solid foundation to identify, monitor, and communicate about potential
295 impacts related to the loss of availability, confidentiality and integrity. This supports the process
296 that has been described throughout the NISTIR 8286 series, applying an understanding of
297 enterprise strategy and risk direction to guide cybersecurity risk management (CSRM) and to
298 record and communicate CSRM activities in support of ERM objectives.

299 **1.2 Foundational Practices for Business Impact Analysis**

300 To gain the enterprise benefits of BIAs for consistent prioritization and risk assessment, there
301 must be a consistent application of the processes and forms used. When impact analysis is
302 performed in a structured and repeatable manner, the impact assertions and resulting decisions
303 are more reliable.² To support a consistent analysis of business impact, senior leaders define
304 clear criteria for criticality and sensitivity. These criteria should be reviewed periodically and
305 adjusted as needed. Guidance should also direct those performing a BIA to consider the worst-
306 case scenario when determining potential impacts, such as a disruption to an e-commerce
307 website on the busiest day of the sales year.

308 As with many elements of risk management, it is usually more important to be consistent than to
309 be exactly precise in analytic results. Even if the actual calculation of the business impact of a
310 loss might not be exact, that figure can be adjusted through subsequent iterations, and an
311 understanding of the relative priority and severity of a loss still enables effective decision-
312 making.

313 **1.3 Document Structure**

314 The remainder of this document is organized into the following major sections:

- 315 • Section 2 describes specific considerations for the documentation and analysis of
316 business impacts resulting from a full or partial loss of confidentiality, integrity, or
317 availability of a mission-essential resource.

² Section 2.2 provides details regarding a BIA process that can be consistently applied in an enterprise.

- 318 • Section 3 provides a conclusion that summarizes this report and points out relevant
319 connections to other NIST publications, including companion documents from the
320 NISTIR 8286 series.

- 321 • Appendix A contains acronyms used in the document.

322 **2 Cataloging and Categorizing Assets Based on Enterprise Value**

323 All public- and private-sector enterprises use a significant array of assets to accomplish their
 324 missions. While the term “asset” may immediately call to mind technical equipment, assets cover
 325 a much broader set of resources. An asset may be tangible (e.g., a physical item such as
 326 hardware, firmware, computing platform, network device, or another technology component) or
 327 intangible (e.g., data, information, software, trademark, copyright, patent, intellectual property,
 328 image, or reputation). The value of an asset is driven by stakeholders based on the enterprise’s
 329 mission. Practitioners should keep in mind that intangible assets (e.g., privacy, reputation, public
 330 confidence, institutional knowledge, and intellectual property) are often impacted by attacks.

331 **2.1 Identification of Enterprise Business Asset Types**

332 To inform risk identification and analysis, the reviewer must begin with the types of information
 333 that might be impacted. For ICT assets, those are primarily risks to information-related systems
 334 but also include operational technology that supports transactions, sensors, and cyber-physical
 335 control signals.³ Some examples are provided in Table 1.

336 **Table 1: Examples of Enterprise Business Asset Types**

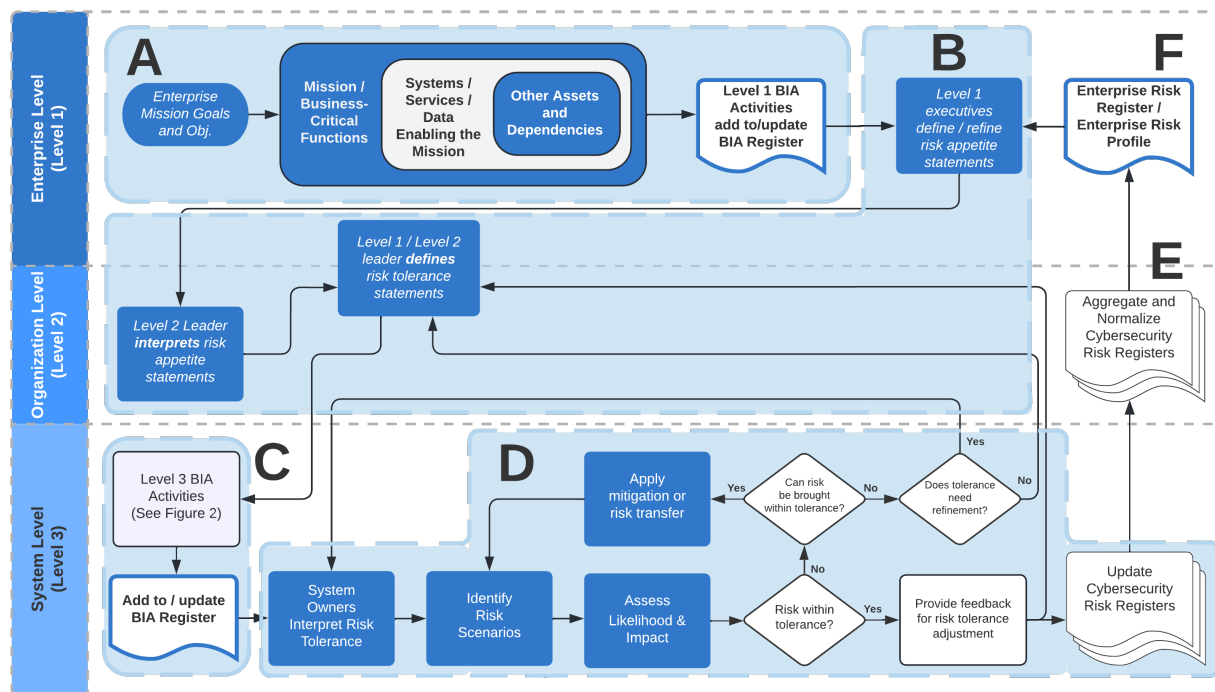
Asset Type	Description	Examples
Information-related Items (Tangible)	The physical assets needed to support operations, including financial records, customer data, or supporting systems	Hardware, firmware, computing platform, network device, or another technology component
Information-related Items (Intangible)	General information needed to support operations, including financial records, customer data, or supporting systems	Data, information, software, trademark, patent, intellectual property, image, or reputation
Transactions	Information related to or resulting from a specific business-related interaction	Product sale, agency service, non-profit grant provision
Control Signals	An electronic command intended to control the functions of an automated system or infrastructure	Command to close a cyber-physical valve, electronic message to close an electrical breaker
Sensor Readings	Information produced by dedicated device types to convert physical process variables into control signals to monitor or manage an automated system	Alarms and indicators (e.g., pipeline pressure, system temperature)

337 **2.2 The Business Impact Analysis Process**

338 To consider the possible impacts of loss on an asset, one must first determine the value of the
 339 asset to the enterprise. While the direct replacement cost of components of the asset are a factor
 340 in that valuation, an asset’s value is directly dependent on the extent to which it helps achieve the
 341 organization’s objectives (or to support other assets’ ability to do so). Understanding the
 342 enterprise value of an asset requires an understanding of “what needs to go right” to accomplish
 343 the mission.

³ Specifics about the security and reliability of operational technology and other cyber-physical systems are available throughout many NIST publications including the Framework for Cyber-Physical Systems, NIST Special Publication 1500-201, available from <https://doi.org/10.6028/NIST.SP.1500-201>.

344 Figure 1 illustrates the integration of the business impact analysis process with the cybersecurity
345 risk management (CSRM) processes described throughout the NISTIR 8286 series.



346
347

Figure 1: Integration of BIA Process with Cybersecurity Risk Management

348 BIA activities, described in more detail below, should be performed on the enterprise and system
349 levels (Level 1 and Level 3). The analysis is highly dependent upon the Level 2 as depicted in
350 Step E of figure 1.

351 The process in Figure 1 is described below:

- 352 • Step A – Based on the enterprise mission, executives identify the systems and services
353 that represent “mission/business-critical functions” that are essential to the successful
354 operation of the enterprise. Based on that list, the executives and senior leaders identify
355 the enterprise-level assets⁴ that enable those functions. Those assets inherit the
356 criticality/priority of the functions they support.
- 357 • Step B – Leaders establish and communicate the risk appetite associated with those
358 enterprise assets, and organizational managers determine the resulting risk tolerance.

⁴ The term ‘asset’ or ‘assets’ is used in multiple frameworks and documents. For the purposes of this publication, ‘assets’ are defined as technologies that may comprise an information system. Examples include laptop computers, desktop computers, servers, sensors, data, mobile phones, tablets, routers, and switches. In instances where the authors mean ‘assets’ as they appear on a balance sheet, the word ‘asset’ will be preceded by words such as ‘high-level’ or ‘balance sheet’ or ‘Level 1’ to differentiate context.

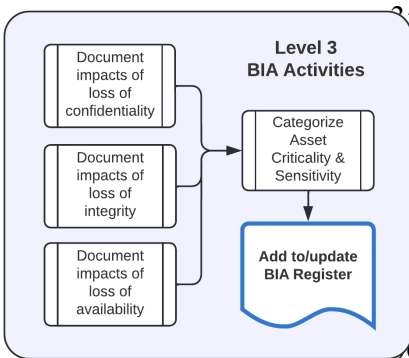


Figure 2: Level 3 BIA Activities

359
360
361
362
363
364
365
366
367
368

- Step C – As part of the CSRM process, the system owner will determine the extent to which every system or activity enables a mission/business-critical function (as illustrated in Figure 2). The criticality/priority direction from leaders, expressed through risk appetite/risk tolerance statements (Step B), is used to help determine what the impact of losses would be on confidentiality, integrity, or availability. That impact understanding and the basis for those determinations are recorded in the system BIA Register.

370
371

- Step D – The analysis and results provide the input into the CSRM process illustrated in the diagram and described in NISTIRs 8286A, 8286B, and 8286C.

372
373
374
375

- Step E – Residual risks, particularly those that impact critical and sensitive resources, are highlighted in the Level 2 risk registers as those CSRRs are normalized and aggregated. Of important note is that cybersecurity is one component of technology risk that feeds operational risks (OpRisk).

376
377
378
379
380
381
382
383
384

- Step F – Enterprise leaders consider the results of ongoing risk activities reported through Level 2 CSRRs as integrated into an Enterprise Cybersecurity Risk Register (E-CSRR) and assess the aggregate impact of the Level 3 and Level 2 risks. This understanding of the composite impact on “mission/business-critical functions” (including OpRisk) is used to prioritize risk response based on enterprise finance, mission, and reputation consequences.⁵ Composite understanding also helps to confirm that risks are within the stated risk appetite or to identify necessary adjustments. If adjustments are necessary, an action plan is created that will result in the appropriate increase or decrease of risk appetite to achieve the appropriate impact levels.

385
386
387
388
389
390
391
392
393
394
395
396

The BIA activities described in Figure 1 Steps A and C provide an opportunity to record information about enterprise assets, their value, and their relationship to enterprise risks. This asset management information supports recommendations from many risk management frameworks, including several from NIST, that encourage the use of an asset registry or repository to provide centralized knowledge management about the technology and data used to support the enterprise mission. For example, Cybersecurity Framework outcomes support an “asset inventory,” including hardware, software, external connections or services, and network segments. The Privacy Framework category “Inventory and Mapping” (ID.IM-P) includes inventory outcomes for systems, products, services, organizational roles, data actions and their purposes, data elements, and data processing components. Understanding the many types of assets in use by and for the enterprise helps to evaluate the potential consequences of a loss and supports effective risk response and monitoring.

⁵ Operational risk is discussed more fully in NISTIR 8286C Section 3.1.

397 Once practitioners have determined the relative importance of various assets to the enterprise
398 mission, they can evaluate the impact of a partial or full loss of confidentiality, integrity, or
399 availability of those assets. As with other CSRM elements, this analysis (Step C) will be iterative
400 in that impact analysis will support risk identification, and the understanding of potential risks
401 informs impact determination (Step D). As system-level and organization-level CSRRs are
402 aggregated and correlated (Step E), enterprise risk managers will use the composite set of
403 information to determine the accuracy of previous risk analyses and assumptions. Specifically,
404 risk management plans and results, as portrayed through the aggregated risk registers, provide
405 details regarding residual risk, including the anticipated enterprise exposure. The integrated
406 understanding of all potential exposure – financial, missional, and reputational – is recorded in
407 the Enterprise Risk Profile (ERP) and helps enterprise leadership make informed risk decisions.
408 That enterprise-level understanding also provides leaders with valuable information to support
409 the next iteration of the CSRM cycle through criteria for asset classification, past performances
410 to inform quantifiable impact analysis, and a refined determination (Step B) of security
411 requirements and risk appetite for various asset classes.

412 This cycle enables an equilibrium that helps to balance the value of enterprise assets with an
413 optimization of resources for operating and protecting those assets given what is known about
414 the risks to those assets. Knowledge of asset value is gained throughout the life cycle through
415 aggregated risk information, improving leaders' understanding of the potential impact of losses
416 to key assets. The value that is recorded in the BIA may extend well beyond replacement costs (a
417 traditional measure of cost). For example, while one can calculate the direct cost of research and
418 development underlying a new product offering, the long-term losses of the potential theft of that
419 intellectual property could have more far-reaching impacts, including future revenue, share
420 prices, enterprise reputation, and competitive advantage.

421 It is important to remember that although Figures 1 and 2 show a high-level and serial process
422 for managing risk, actual CSRM/ERM integration is very dynamic and is rarely this simple. Risk
423 conditions change frequently and drastically, so risk managers throughout the enterprise must
424 stay in close communication and must be prepared for out-of-cycle adjustments.

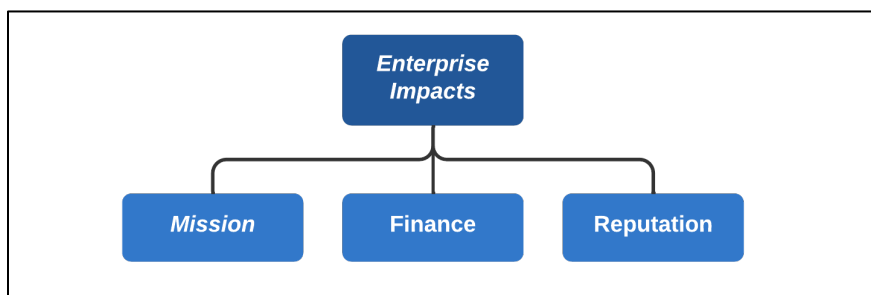
425 **2.3 Determining Asset Value to Support CSRM Activities**

426 Consistent asset valuation and impact analyses are important elements of enterprise risk strategy.
427 Enterprise leaders and their supporting managers review the enterprise mission objectives and
428 expected outcomes to develop the risk management strategy for the enterprise. These strategic
429 considerations then provide input to consider and calculate the harm that would occur if those
430 benefits were reduced or eliminated. The BIA process provides that consistent model for
431 determining and documenting the intended value of an asset and the potential harm of a loss to
432 that asset. BIA enables the consideration of any types of assets that enable the mission, many of
433 which are related to the correct functioning of operational technology and cyber-physical
434 systems. It is important to continually evaluate the role of various types of ICT in consideration
435 of the harmful effects of any incident that might degrade or disrupt enterprise capabilities or that
436 might have deleterious effects on the enterprise's reputation or finances. For example, traditional
437 information technology is almost always important, but it can be equally important to ensure that
438 a manufacturing system operates properly or that chemicals flow safely throughout an industrial

439 plant. Each of the elements that enable both data and control signals should be included in the
440 BIA.

441 By recording the benefits provided by an asset in light of its contribution to the enterprise, the
442 potential impacts of a loss to those assets can be determined (see Figure 3), particularly in terms
443 of:

- 444 • **Mission** – Including direct or indirect support to corporate or agency products and
445 services
- 446 • **Finance** – Benefits that will improve the enterprise’s earnings (net revenue or return on
447 investment for a government entity) or that will support fiscal capital and free cash flow
448 for a business
- 449 • **Reputation** – Attributes that enable stakeholders (e.g., citizens, shareholders, regulators,
450 partners) to view the enterprise in a favorable light and contribute to its well-being



451
452 **Figure 3: Impacts of Enterprise Assets for a Business or Agency**

453 By documenting the harmful impacts of losses to enterprise assets, the BIA provides important
454 input into the information security risk assessment process.

455 **2.4 Determining Loss Scenarios and Their Consequences**

456 Historically, the BIA provides a consistent method for considering the impacts of disruptions to
457 the delivery of products and services. While disruption (i.e., partial or full loss of availability) is
458 an important impact to consider, the factors described above highlight the need to also consider
459 high-level impacts from losses that occur to confidentiality and integrity. This high-level set of
460 loss scenarios is related to but separate from the detailed risk scenarios that occur as part of the
461 cybersecurity risk management (CSRM) process.

462 In preparation for the BIA, the system owner will determine sources of loss to the asset being
463 discussed.⁶ Threat modeling processes, such as the OCTAVE Allegro method, may help to
464 develop scenarios about the impacts of critical or sensitive data being disclosed, modified,
465 interrupted, or destroyed [[OCTAVE](#)]. These loss scenarios consider the enterprise risk strategy,

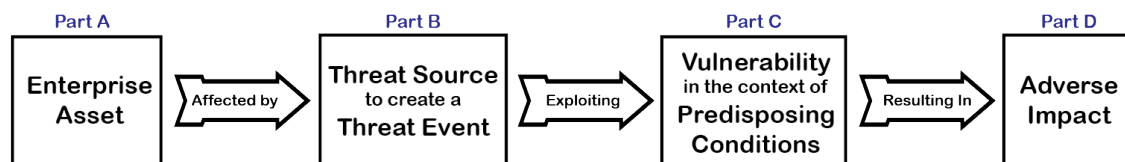
⁶ For federal systems, the system owner may be a program manager or business/asset owner and may represent the official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. Non-federal entities may consider this role to be a business manager with oversight of the development, production, and operation of the information resource.

466 leadership’s risk appetite and tolerance, and the mission, finance, and reputation factors
467 described in Section 2.3.

468 ISO 22317 points out that, to support consistency, many enterprises define a scale to aid in the
469 classification or categorization of assets, as determined through the BIA process [ISO22317]. For
470 example, FIPS Publication 199 defines three levels (low, moderate, and high) of potential impact
471 on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality,
472 integrity, or availability). These levels are determined based upon an assessment of whether a
473 loss could be expected to have a limited, serious, or severe adverse effect [FIPS199].

474 Loss scenarios should reflect partial as well as complete losses. It is important to analyze
475 “graceful degradation” scenarios and conditions under which assets continue to function but do
476 so in a diminished or limited capacity. As described above, these “partial” impacts include
477 confidentiality and integrity issues as well as availability. The BIA also offers the opportunity to
478 evaluate the potential impact of the timing of a loss event (e.g., threat event frequency, latency,
479 and duration), which has a significant influence on the harm that may result.

480 Ultimately, these loss scenarios will provide input into the CSRM process, including risk
481 scenario identification. NISTIR 8286A describes the need for risk identification as part of a
482 broader risk assessment, including for information security risk. It frames risk identification in
483 terms of four necessary inputs (parts A through D, as shown in Figure 4) that should be recorded
484 in the risk description cell of a CSRR. Combining these elements into a risk scenario helps to
485 provide the full context of a potential loss event. The use of this scenario-based approach helps
486 ensure comprehensive risk identification by considering many types of physical and logical
487 events that might occur.



488

489 **Figure 4: Elements of Information Risk Identification (from NISTIR 8286A)**

490 The completion of the risk description column is composed of four activities that are detailed in
491 NISTIR 8286A, Subsections 2.2.1 through 2.2.4. The activities include:

- 492 • Part A – Identification of the organization’s relevant assets and their valuation
- 493 • Part B – Determination of potential threats that might jeopardize the confidentiality,
494 integrity, and availability of those assets
- 495 • Part C – Consideration of vulnerabilities or other predisposing conditions of assets that
496 make a threat event possible
- 497 • Part D – High-level evaluation of the potential consequences if the threat source (part B)
498 exploits the weakness (part C) against the organizational asset (part A)

499 Information learned while developing the loss scenarios helps to complete Part D of the risk
500 scenario development, as depicted in Figure 4. By determining the various adverse impacts that
501 might occur – whether by intentional attacks, natural events, or inadvertent errors – the enterprise
502 will be able to support effective assessment, response, communications, and monitoring of
503 information security risks. Notably, the goal is not to determine the probability that such a risk
504 could occur since that exercise is part of risk analysis. Rather, the analysis of business impact is
505 to predetermine what the various effects might be in order to enable risk managers to decide how
506 critical and sensitive a particular business system is. Similar considerations apply to cyber-
507 physical systems and operational technologies.

508 The risk management process relies on this foundation of asset categorization, enabling a tailored
509 and cost-effective approach to balancing risk and reward. Business impact drives categorization
510 (sometimes called asset classification), which drives risk identification, which will later inform
511 risk response, risk monitoring, and communication.

512 Risk managers use their understanding of potential impacts to create the risk identification
513 scenarios that are recorded in the risk description column of the CSRR and to the record impact
514 value in the CSRR impact column. This information is recorded in the risk detail record (RDR),
515 including the primary adverse impact, secondary adverse impact, and other relevant fields within
516 that template.

517 Since business impact is directly based on the effect that uncertainty will have on key enterprise
518 functions, the analyst must gain the guidance of senior leadership regarding the determination of
519 assets that are critical or sensitive. The relative importance of each enterprise asset (and its
520 interdependencies and interconnections) will be a necessary input for considering the impact
521 portion of the risk description (Part D in Figure 4) in the CSRR. Through these processes, a BIA
522 supports communication and the prioritization of an enterprise approach to protecting and
523 monitoring critical and sensitive assets (e.g., high value assets, or HVAs) in light of the
524 enterprise's mission.

525 **2.5 Business Impact Analysis in Terms of Criticality and Sensitivity**

526 Based on the information stored, transmitted, or processed by the asset being analyzed, risk
527 managers can determine the criticality and sensitivity of the system. The level of criticality can
528 be calculated by examining the detailed harms that would result from the loss of availability of
529 that asset. Similarly, the level of sensitivity can be calculated by examining the detailed harms
530 that would result from the loss of integrity or confidentiality of that asset. The factors that
531 determine severity are directly tied to the enterprise strategy (including the risk management
532 strategy).

533 As with all risk management activities, the impact analysis processes are iterative. Value
534 determination will depend on the impact of a loss of the asset, which will be determined by the
535 threat and vulnerability scenarios. Actual risk analysis of a scenario can be performed using
536 many methodologies, including root cause analysis, event trees, fault trees, bowtie diagrams, and
537 failure mode effects analysis (FMEA) or failure modes, effects, and criticality analysis
538 (FMECA). NISTIR 8286A details methods for determining the likelihood of a scenario using
539 these and other methods, as well as for using simulation (e.g., the Monte-Carlo technique) to

540 calculate probability. A key benefit of using such methodologies is the ability to better quantify
541 the criticality and sensitivity of an enterprise asset rather than using vague qualifiers.

542 The BIA does not directly address the identified risks, but the BIA-determined criticality and
543 sensitivity of a system will certainly influence risk management requirements and thereby drive
544 CSRM prioritization and risk remediation. For example, if the risk analysis indicates that failure
545 is probable for aging or obsolescent critical infrastructure, upgrades to or replacement of that
546 infrastructure may become a priority.

547 **2.6 Using a BIA to Record Interdependencies**

548 A valuable benefit of a BIA is that it provides an opportunity to record interdependencies and
549 their influence on enterprise benefits and risks. For example, a network router will have
550 significant enterprise importance if it enables a vital sales website. One of the most common uses
551 of a BIA is to record critical systems and identify the underlying infrastructure on which those
552 systems depend.

553 The BIA enables a much broader understanding, however. In the cybersecurity realm, use of the
554 BIA has historically been limited to calculations of quality-based and time-based objectives for
555 incident handling (including continuity of operations and disaster recovery). Because the BIA
556 serves as a nexus for understanding risk (which is simply the measurement of uncertainty on the
557 “system” impacted), it can be used to:

- 558 • Determine appropriate risk appetite and tolerance values as part of enterprise risk
559 strategy;⁷
- 560 • Develop performance and risk metrics that can be used to communicate and monitor
561 CSRM activities, including those measures that have been determined to be key
562 performance indicators (KPIs) and key risk indicators (KRIs);
- 563 • Aid in the classification or categorization of systems (and components of systems);
- 564 • Enable the escalation of risk notification, response, and related decisions;
- 565 • Support risk management requirements for the systems considered within the BIA; and
- 566 • Enable effective monitoring based on the criticality and sensitivity of the systems
567 recorded.

568 Expanding the use of the BIA to include confidentiality and integrity considerations helps to
569 support a comprehensive risk analysis and, thus, improves CSRM effectiveness. The basis of
570 asset valuation on enterprise impact helps to better align risk decisions with the enterprise risk

⁷ OMB Circular A-123 defines risk appetite as “the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization’s most senior level leadership and serves as the guidepost to set strategy and select objectives.” The same document defines *risk tolerance* as “the acceptable level of variance in performance relative to the achievement of objectives.”

571 strategy. As illustrated in Figure 1, CSRM/ERM integration helps to complete the cycle by
572 informing future iterations of impact analysis based on previous information gained through
573 CSRR aggregation. As organizational and enterprise leaders gain an understanding of the
574 aggregate risk exposure and potential composite impact, they can use that information to adjust
575 risk expectations (and possibly adjust business impact guidance to ensure an ongoing balance
576 between asset value, resource optimization, and risk considerations).

577 **2.7 Consistent Business Impact Analysis Through an Enterprise Approach**

578 The use of a consistent BIA template throughout the enterprise helps ensure that assets are
579 similarly categorized by all parties. Because valuation can be subjective, a documented
580 methodology supports prioritization and risk management by all participants.

581 The use of a common methodology also supports enterprise communication and collaboration to
582 better understand what constitutes sensitivity and criticality in each enterprise's unique context.
583 An example of such a methodology is described in the *Criticality Analysis Process Model*,
584 [\[NISTIR8179\]](#). This model includes top-down and bottom-up analyses, connecting different
585 levels of the enterprise to support consistent and comprehensive assessments. NISTIR 8179 uses
586 the term "baseline criticality," which *Supply Chain Risk Management Practices for Federal*
587 *Information Systems and Organizations*, NIST Special Publication (SP) 800-161, defines as,

588 The identification of system and its components, whether physical or logical, that
589 are considered critical to an organization's mission. The reduced functional
590 capability, incapacity, or destruction of such systems and components would have
591 a significant adverse impact on an organization's operations (including mission,
592 functions, image, or reputation), assets, individuals, other organizations, and the
593 Nation. [\[SP800-161R1\]](#)

594 Similarly, *Security and resilience – Business continuity management systems – Guidelines for*
595 *business impact analysis*, ISO/TS 22317:2021, describes methods for documenting and
596 monitoring business system value, although it focuses primarily on availability considerations.

597 Notably, business impact is based on understanding the impact of losses on a critical or sensitive
598 "system." As described in Section 1, losses can range from a minor inconvenience to a partial
599 disruption to a catastrophic disaster, so it is helpful to use risk analysis techniques to simulate
600 and record these ranges. In many cases, an enterprise will continue to use networked systems
601 even during a compromise. Impact and loss should not be seen as binary states but rather factors
602 to use as inputs to the risk register and outputs to risk monitoring.

603 The term "system" could indicate one of many things comprised of some combination of
604 physical infrastructure, including hardware, software, firmware, communications/data flow, and
605 external equipment or services. Notably, many enterprise assets are "systems of systems."
606 Because these particular systems are complex and interconnected, they are noteworthy from a
607 risk perspective.

608 **2.8 Using a BIA to Support an Enterprise Registry of System Assets**

609 The BIA also enables a centralized registry of important asset management information. This
610 *asset register* enables review, monitoring, and communications about the characteristics of the
611 asset (e.g., system, service, facility). The asset register also enables the documentation of contact
612 information for those in various roles – information that can be helpful during risk assessment
613 and incident handling. Example contact information might include:

- 614 • Sponsor or business owner responsible for the asset
- 615 • System owner
- 616 • System operator or administrator(s)
- 617 • Security contacts
- 618 • Privacy contacts
- 619 • Characteristics of the physical devices (or services)

620 Since asset management is an important element of cybersecurity risk management, this
621 information is quite valuable for protecting the asset, detecting cyber events, responding quickly
622 to potential issues, and recovering services when necessary.

623 Cybersecurity incident responders often need readily available information regarding affected
624 enterprise systems. The enterprise registry of business systems is a vital source of information
625 about the systems and services that might be impacted by a cybersecurity event, the sensitivity
626 and criticality of those assets, and important information about how to contact relevant
627 stakeholders. As system owners and risk practitioners gain knowledge throughout the
628 CSRM/ERM integration cycle, the information in the asset registry must be updated to improve
629 risk identification, accurate exposure consideration (based on realistic calculations of harmful
630 impacts), and effective risk response. Proper maintenance also enables comparison of the asset
631 register information to the CSRR and the enterprise risk register (ERR).

632 **3 Conclusion**

633 While business impact analysis has historically been used to determine availability requirements
634 for business continuity, the process can be extended to provide broad understanding of the
635 potential impacts to the enterprise mission from any type of loss. The management of enterprise
636 risk requires a comprehensive understanding of the mission-essential functions (i.e., what must
637 go right) and the potential risk scenarios that jeopardize those functions (i.e., what might go
638 wrong).

639 Enterprise leaders need a methodology to determine which assets enable the achievement of
640 mission objectives and to evaluate the factors that render assets as critical and sensitive. Based
641 on those factors, enterprise leaders provide risk directives (i.e., risk appetite and tolerance) as
642 input to the BIA. System owners then apply the BIA to developing asset categorization, impact
643 values, and requirements for the protection of critical or sensitive assets. The output of the BIA is
644 the foundation for ERM/CSRM process, as described in the NISTIR 8286 series, and enables
645 consistent prioritization, response, and communication regarding information security risk.

646 Public- and private-sector enterprises must maintain a continual understanding of potential
647 business impacts, the risk conditions that might lead to those impacts, and the steps being taken
648 (as recorded in various risk registers and, ultimately, in the ERP). In many cases, when a
649 company or agency is asked about risks, they are actually being asked to describe potential
650 impacts. An example of this is reflected in publicly traded enterprises' annual reports where the
651 first section describes the mission and business and the next section (Risk Factors) describes
652 potential events that might have a material adverse effect on the enterprise's financial position,
653 its ability to operate, or its corporate cash flow. Similar reports occur among public-sector
654 agencies and their administrative or legislative overseers. Adverse impacts can impair agency
655 funding and missions, so the BIA is equally important for public service enterprises.

656 Use of the BIA methodology to categorize the criticality and sensitivity of enterprise assets
657 enables effective risk management and the subsequent integration of reporting and monitoring at
658 the enterprise level to ensure that risk and resource utilization are optimized in light of the value
659 of those assets.

660 **References**

661 The following external publications were referenced in this report.

- [NISTIR8286] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. <https://doi.org/10.6028/NIST.IR.8286>
- [OCTAVE] Software Engineering Institute (2007) Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. (Software Engineering Institute, Pittsburgh, PA), Technical Report CMU/SEI-2007-TR-012. Available at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf
- [ISO22317] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/TS 22317:2021 *Security and resilience — Business continuity management systems — Guidelines for business impact analysis* (ISO, Geneva, Switzerland). Available at <https://www.iso.org/standard/79000.html>
- [SP800-161R1] Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161r1. <https://doi.org/10.6028/NIST.SP.800-161r1>
- [FIPS199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. <https://doi.org/10.6028/NIST.FIPS.199>
- [NISTIR8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. <https://doi.org/10.6028/NIST.IR.8179>

662

663 **Appendix A—Acronyms**

664 Selected acronyms and abbreviations used in this paper are defined below.

665	ALE	Annualized Loss Expectancy
666	BIA	Business Impact Analysis
667	CSRM	Cybersecurity Risk Management
668	CSRR	Cybersecurity Risk Register
669	DDIL	Denied, Disrupted, Intermittent, and Limited Impact
670	ERM	Enterprise Risk Management
671	ERP	Enterprise Risk Profile
672	FMEA	Failure Mode Effects Analysis
673	FMECA	Failure Modes, Effects, and Criticality Analysis
674	FOIA	Freedom of Information Act
675	ICT	Information and Communications Technology
676	IT	Information Technology
677	ITL	Information Technology Laboratory
678	IRP	Incident Response Plan
679	KPI	Key Performance Indicators
680	NPS	NIST Publication System
681	POC	Points of Contact
682	RDR	Risk Detail Record
683	SSP	System Security Plan