NIST IR 8286D ipd

Using Business Impact Analysis to Inform Risk Prioritization and Response

Initial Public Draft

Stephen Quinn
Nahla Ivy
Matthew Barrett
Larry Feldman
Daniel Topper
Greg Witte
R. K. Gardner

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

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

NIST IR 8286D ipd

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

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

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

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

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

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

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

Reports on Computer Systems Technology

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

Abstract

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

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

Keywords

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

Audience

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

Call for Patent Claims

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

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

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

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

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

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

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

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

Executive Summary

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

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

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

Expanding use of the BIA to include confidentiality and integrity considerations supports comprehensive risk analysis. The basis of asset valuation on enterprise impact helps to better align risk decisions to enterprise risk strategy. CSRM/ERM integration helps to complete the risk cycle by informing future iterations of impact analysis based on previous information gained 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."

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

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

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

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

Table of Contents

List of Appendices

List of Figures

1 Introduction

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

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

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

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

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

1.1 Benefits of Extending the BIA for All Risk Types

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

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

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

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

1.2 Foundational Practices for Business Impact Analysis

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

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

1.3 Document Structure

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

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

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

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

- Appendix A contains acronyms used in the document.

2 Cataloging and Categorizing Assets Based on Enterprise Value

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

2.1 Identification of Enterprise Business Asset Types

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

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)

2.2 The Business Impact Analysis Process

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

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

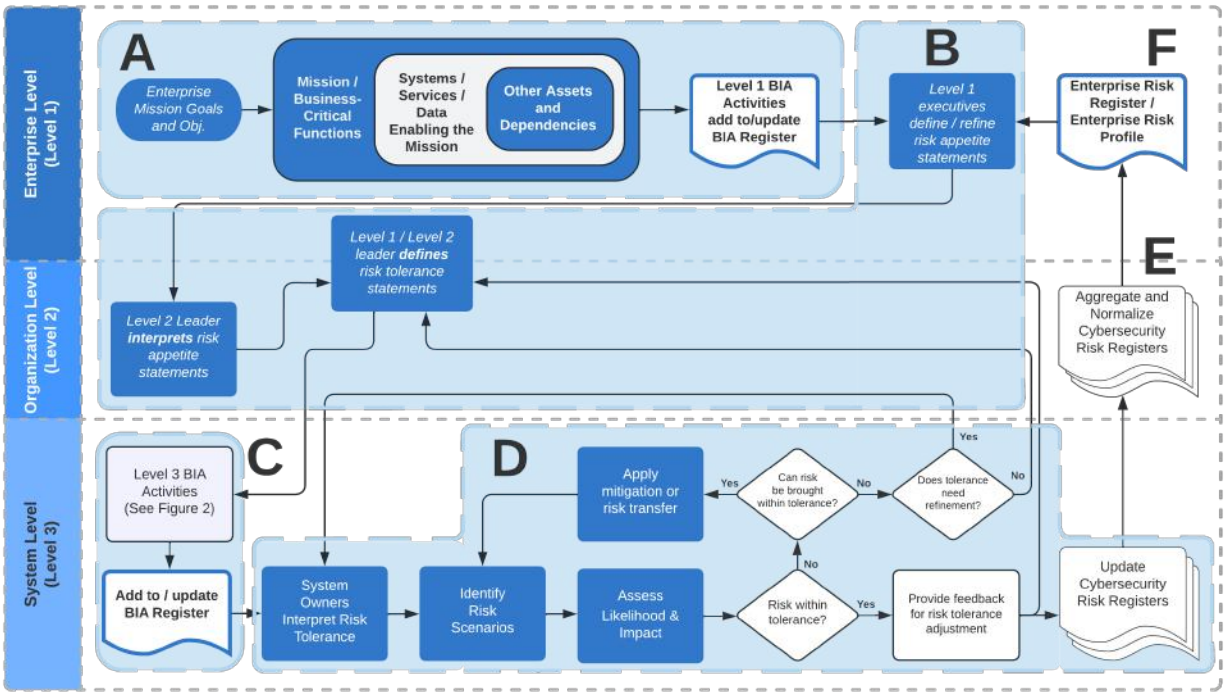

Figure 1: Integration of BIA Process with Cybersecurity Risk Management

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

The process in Figure 1 is described below:

- Step A – Based on the enterprise mission, executives identify the systems and services that represent "mission/business-critical functions" that are essential to the successful operation of the enterprise. Based on that list, the executives and senior leaders identify the enterprise-level assets[4] that enable those functions. Those assets inherit the criticality/priority of the functions they support.

- Step B – Leaders establish and communicate the risk appetite associated with those 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 proceeded by words such as 'high-level' or 'balance sheet' or 'Level 1' to differentiate context.

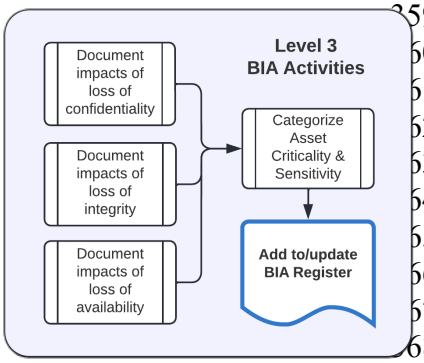

Figure 2: Level 3 BIA Activities

- 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.

- 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.

- 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).

- 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.

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.

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

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

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

2.3 Determining Asset Value to Support CSRM Activities

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

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

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

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

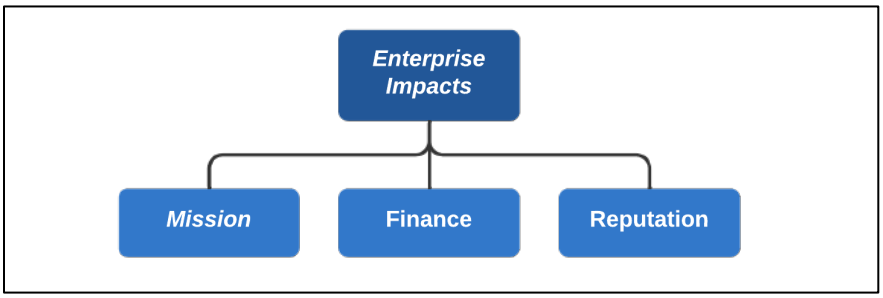

Figure 3: Impacts of Enterprise Assets for a Business or Agency

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

2.4 Determining Loss Scenarios and Their Consequences

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

In preparation for the BIA, the system owner will determine sources of loss to the asset being discussed.[6] Threat modeling processes, such as the OCTAVE Allegro method, may help to develop scenarios about the impacts of critical or sensitive data being disclosed, modified, 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.

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

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

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

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

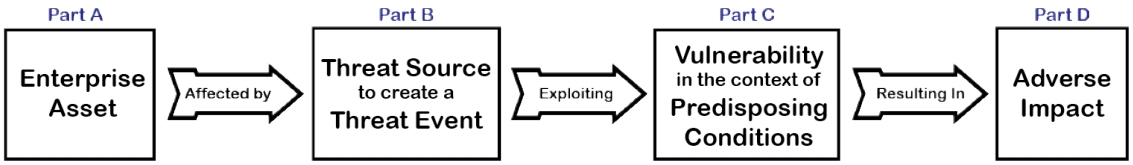

Figure 4: Elements of Information Risk Identification (from NISTIR 8286A)

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

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

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

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

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

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

2.5 Business Impact Analysis in Terms of Criticality and Sensitivity

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

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

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

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

2.6 Using a BIA to Record Interdependencies

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

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

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

Expanding the use of the BIA to include confidentiality and integrity considerations helps to support a comprehensive risk analysis and, thus, improves CSRM effectiveness. The basis of 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."

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

2.7 Consistent Business Impact Analysis Through an Enterprise Approach

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

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

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

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

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

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

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

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

- Sponsor or business owner responsible for the asset
- System owner
- System operator or administrator(s)
- Security contacts
- Privacy contacts
- Characteristics of the physical devices (or services)

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

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

3 Conclusion

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

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

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

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

References

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

Appendix A—Acronyms

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

ALE	Annualized Loss Expectancy
BIA	Business Impact Analysis
CSRM	Cybersecurity Risk Management
CSRR	Cybersecurity Risk Register
DDIL	Denied, Disrupted, Intermittent, and Limited Impact
ERM	Enterprise Risk Management
ERP	Enterprise Risk Profile
FMEA	Failure Mode Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FOIA	Freedom of Information Act
ICT	Information and Communications Technology
IT	Information Technology
ITL	Information Technology Laboratory
IRP	Incident Response Plan
KPI	Key Performance Indicators
NPS	NIST Publication System
POC	Points of Contact
RDR	Risk Detail Record
SSP	System Security Plan