ITL BULLETIN FOR JUNE 2018

PUTTING FIRST THINGS FIRST – A MODEL PROCESS FOR CRITICALITY ANALYSIS

Celia Paulsen, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

In the modern world, where complex systems-of-systems are integral to the functioning of businesses and society, it is increasingly important to be able to understand and manage risks that these systems and components may present to the missions that they support. Where resources are finite, it is not possible to apply equal protection to all assets for every type of risk – especially since those assets are increasingly complex, interdependent, and externally provided. Risk management can be improved with processes and techniques to prioritize assets for a detailed risk analysis and for applying information security and privacy controls. Existing standards and guidelines provide only high-level and scattered guidance about how to prioritize systems and components relative to organizational goals. Additionally, these existing standards and guidelines are most often focused on prioritizing *projects* according to organizational goals, or prioritizing *components* according to system functionality. A broader approach is needed to avoid an incomplete understanding of the potentially critical nature of a component to organizational goals.

NIST Internal Report (NISTIR) 8179, *Criticality Analysis Process Model*, describes a comprehensive model ("the Model") for prioritizing programs, systems, and components based on their importance to the goals of an organization and the impact that their inadequate operation or loss may present to those goals. The Model adopts and adapts concepts presented in publications regarding business and risk management, engineering principles, safety applications, and cyber supply chain. The authors of NISTIR 8179 researched and compared various existing methods to develop an approach specifically to the needs of information security and privacy risk management.

A criticality analysis is especially relevant to the current technology environment where organizations rely on third-party products and service providers for the development, integration, and management of the information technology (IT) and operational technology (OT) they use. A criticality analysis can help organizations identify and better understand the systems, subsystems, components, and subcomponents that are most essential to their operations and the environment in which they operate.

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

That understanding facilitates better decision making related to the management of an organization's assets, including information security and privacy risk management, project management, acquisition, maintenance, and upgrade decisions.

The Criticality Analysis Process Model

NISTIR 8179 describes the methodology that was used to develop the Model, presents the Model itself, and gives two examples of use cases.

The Model was developed by conducting four main activities:

- A broad review of dozens of models for deciding criticality, from medicine (triage) to safety (hazard analysis) to systems engineering (failure analysis);
- Comparative analysis and synthesis of the reviewed methodologies to derive a common set of steps for a criticality analysis;
- Identification of any potential steps relevant to information security and privacy that were not described in the existing literature; and
- Translation and transformation of the steps into language relevant to information security and privacy practitioners.

The Criticality Analysis Process Model is structured to logically follow the manner used by organizations to design, acquire, and implement projects and systems. Traditionally, organizations establish projects and programs to accomplish mission and business objectives and to guide the performance of corresponding activities. They design and/or deploy information systems to support those activities. These systems are often a loosely defined, complex mixture of hardware, software, network infrastructure, data, humans, and other elements, and may be composed of numerous subsystems (This architecture is often called "systems of systems.").

The Model consists of five main processes as depicted in Figure 1. Process A is expected to be completed before other processes. Processes B, C, and D ideally will be performed in sequence to provide a comprehensive top-down analysis, but may be performed at the same time, or out of sequence, as shown in the model with dashed lines. These three processes have iterative sub-processes and can be conducted at increasing levels of detail to refine the results and accept additional inputs. Process E is a bottom-up analysis using inputs from, and cutting across, Processes B, C, and D. It is performed at the very end to finalize criticality levels for programs, systems/subsystems, and components/subcomponents.

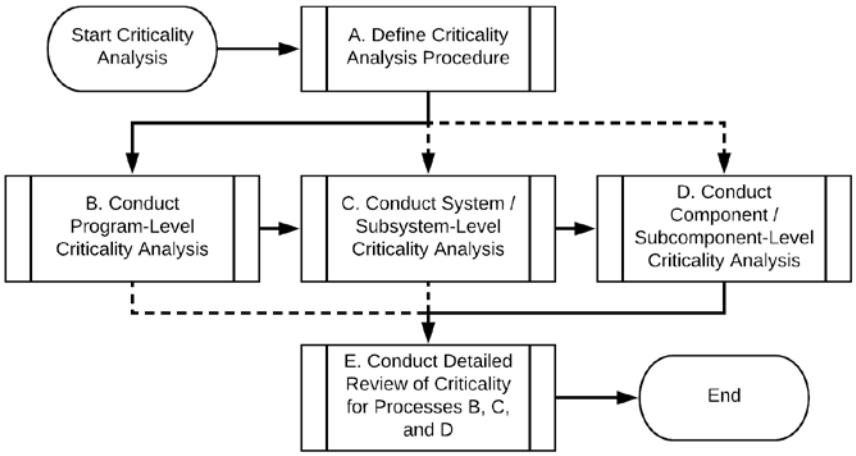

Figure 1: High-Level Criticality Analysis Process Model

Model Process and Sub-Process Description

Section 3 of the NISTIR provides a detailed description of the Model processes and guidance for their application. This description is supplemented by Appendix D, which provides two examples of how the Model can be used and adapted, and Appendix E, which includes detailed diagrams of each process and associated sub-processes. The authors note that organizations do not need to complete each process or sub-process exactly as described in this document to complete a criticality analysis. Rather, it is expected that organizations will tailor the Model to their own needs, capabilities, and operating environment.

The first process, *A. Define Criticality Analysis Procedure,* provides guidance, structure, and continuity for performing a criticality analysis, which is necessary due to the number of different people and groups involved in completing a criticality analysis.

The next three processes, B. Conduct Program-Level Criticality Analysis, C. Conduct System/Subsystem-Level Criticality Analysis, and D. Conduct Component/Subcomponent-Level Criticality Analysis, act as a top-down means of mapping and prioritizing activities, associated systems/subsystems, and finally, components/subcomponents of those systems. These three processes are very similar to each other conceptually, but are described separately because they require different methods for completion and are typically done by separate groups of people with differing areas of expertise. They are iterative and can be conducted at increasing level of detail to refine the results and accept additional inputs.

The last process, *E. Conduct Detailed Review of Criticality for Processes B, C, and D*, is performed after Processes *B*, *C*, and *D* have been completed and cuts across these three processes. This process is performed in a bottom-up manner for tracing dependencies and impact/risk from subcomponents to

components, components to subsystems, subsystems to systems, systems to programs, and programs to higher-level programs using the information gathered in the previous three processes. It provides connective tissue between Processes *B*, *C*, and *D*, and ensures that the criticality determination is consistent across all layers of the Model – program, system/subsystem, and component/subcomponent – in terms of considering impacts, dependencies, and risks across the entire program. As such, Process E requires a high level of coordination and collaboration between the actors in those other processes. Baseline Criticality levels assigned in Processes *C* and *D* are finalized in Process *E*; the Baseline Criticality levels determined in Process *B* are typically sufficient for the program level and so do not need to be finalized in Process *E*.

Conclusion

Determination of the criticality of various systems is a cornerstone of many risk management approaches, including the Risk Management Framework and the Framework for Improving Critical Infrastructure Cybersecurity. Application of the Criticality Analysis Process Model can help organizations to better understand factors that are most essential to their operations. Having this information will facilitate holistic information security and privacy risk management, including integration of these considerations into project management and acquisition processes. The Model helps improve decisions about levels of protection afforded to systems and components during system development and acquisition life cycles, and provides a means for communicating and coordinating priorities with product and service providers.

Additional Resource

An image file of the Criticality Analysis Process Model is available at:
https://csrc.nist.gov/publications/detail/nistir/8179/final

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov