1. NIST 8179 Criticality Analysis

Paulsen, C., Boyens, J. M., Bartol, N., & Winkler, K. (2018). *Criticality analysis process model: prioritizing systems and components*. https://doi.org/10.6028/nist.ir.8179

https://csrc.nist.gov/pubs/ir/8179/final

1. **Purpose of the Criticality Analysis Process Model**: The model is designed to prioritize programs, systems, and components by evaluating their importance to an organization's mission and the risks associated with their ineffective operation or loss.
2. **Integration of Diverse Concepts**: The model incorporates and adapts ideas from various fields including risk management, system engineering, software engineering, security and privacy engineering, safety applications, business and systems analysis, acquisition guidance, and cyber supply chain risk management.
3. **Holistic Risk Management Approach**: It serves as a component of a comprehensive risk management strategy, addressing all risks including information security and privacy risks. The model is compatible with various standards and guidelines, such as the ISO/IEC 27000 family and NIST Special Publications.
4. **Emergence and Evolution in NIST Framework**: The need for criticality analysis within information security has grown with the increasing complexity of systems and the expansion of supply chains. Its first inclusion in NIST publications was in NIST SP 800-53 Revision 4, and it is now a part of several NIST special publications.
5. **Coordination with Existing Organizational Processes**: The model uses outputs and artifacts from existing organizational activities like risk management and system design, aiming to integrate with and avoid duplicating these processes.
6. **Structured and Adaptable Model**: The Criticality Analysis Process Model is logically structured to align with how organizations design and implement projects and systems, and it can be tailored to fit specific organizational practices.
7. **Five Main Processes of the Model**: The model includes defining criticality analysis procedures, conducting program-level analysis, system/subsystem-level analysis, component/subcomponent-level analysis, and a detailed review of criticality for these analyses. This structure aids in understanding and managing the essential elements of an organization's operations, thereby enhancing decision-making regarding protection levels during system development and acquisition.