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

ITL INFORMATION TECHNOLOGY LABORATORY

Identifying Critical Assets for Risk Management

Celia Paulsen

05/16/2018

Disclaimer: "*The identification of any commercial product or trade name is included solely for the purpose of providing examples of publicly-disclosed events, and does not imply any particular position by the National Institute of Standards and Technology.*"

Problem

- Technology
  - Interconnected
  - Sophisticated
  - Integral
- Complex SDLC Ecosystem
- Evolving Threats
- Constant Change
- $$$

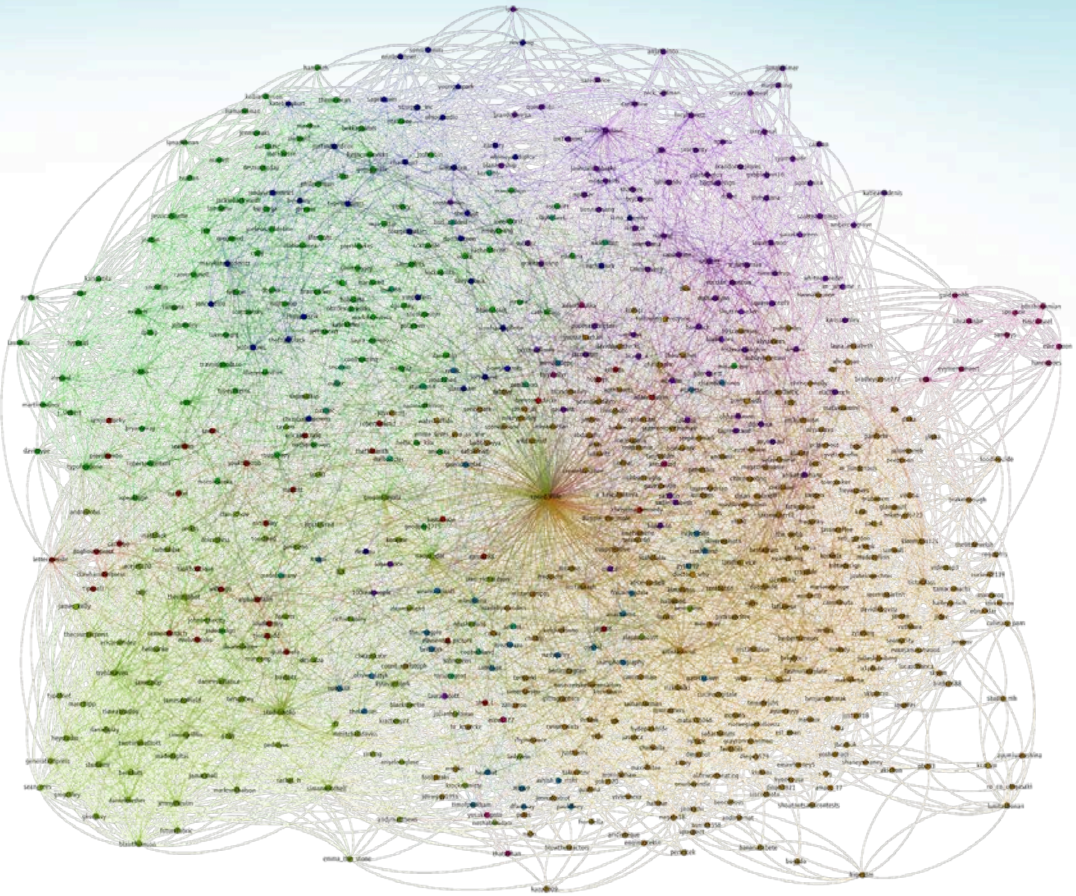


Image by Andy Lamb: https://www.flickr.com/photos/speedoflife/6924482682

NIST IR 8179:
Criticality Analysis Process Model

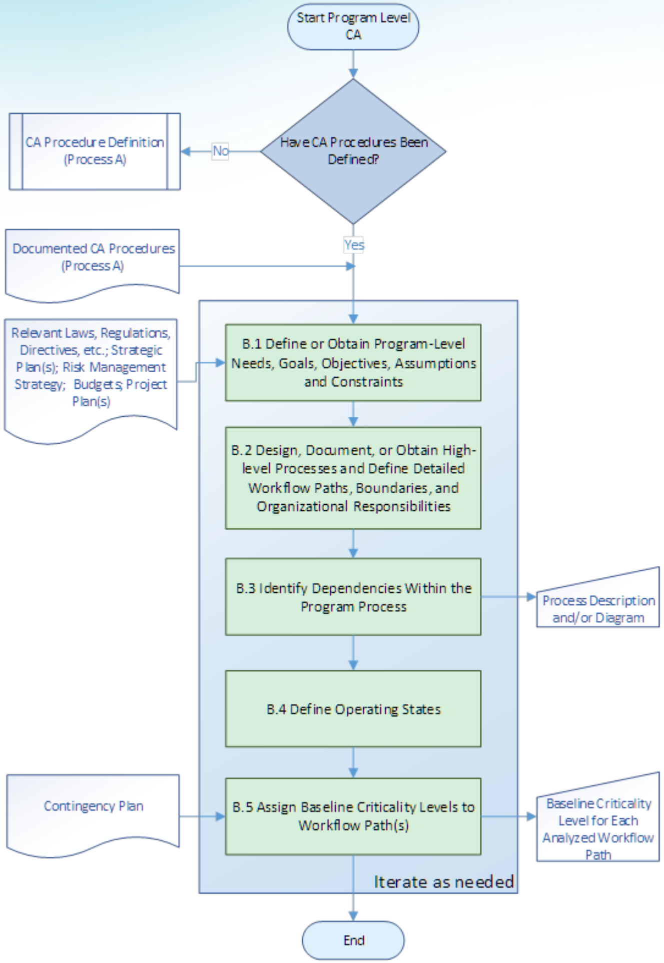
- Method for identifying and prioritizing information systems and components
  - Increase understanding of the organization’s IT/OT (and other) assets
  - Better decision making
    - risk management
    - project management
    - acquisition, maintenance, and upgrade
  - Informed distribution of finite resources

Not Another…

- Failure Mode Effects and Criticality Analysis (FMECA)
- Business Continuity Planning
- FIPS Level / Classification
- Framework (RMF, CSF, etc.)

LEVERAGES AND INFORMS EXISTING PRACTICES – NOT DUPLICATING IT

Reading the Model



Start Program Level CA

Have CA Procedures Been Defined?

No

CA Procedure Definition (Process A)

Yes

Documented CA Procedures (Process A)

Relevant Laws, Regulations, Directives, etc.; Strategic Plan(s); Risk Management Strategy; Budgets; Project Plan(s)

B.1 Define or Obtain Program-Level Needs, Goals, Objectives, Assumptions and Constraints

B.2 Design, Document, or Obtain High-level Processes and Define Detailed Workflow Paths, Boundaries, and Organizational Responsibilities

B.3 Identify Dependencies Within the Program Process

Process Description and/or Diagram

B.4 Define Operating States

Contingency Plan

B.5 Assign Baseline Criticality Levels to Workflow Path(s)

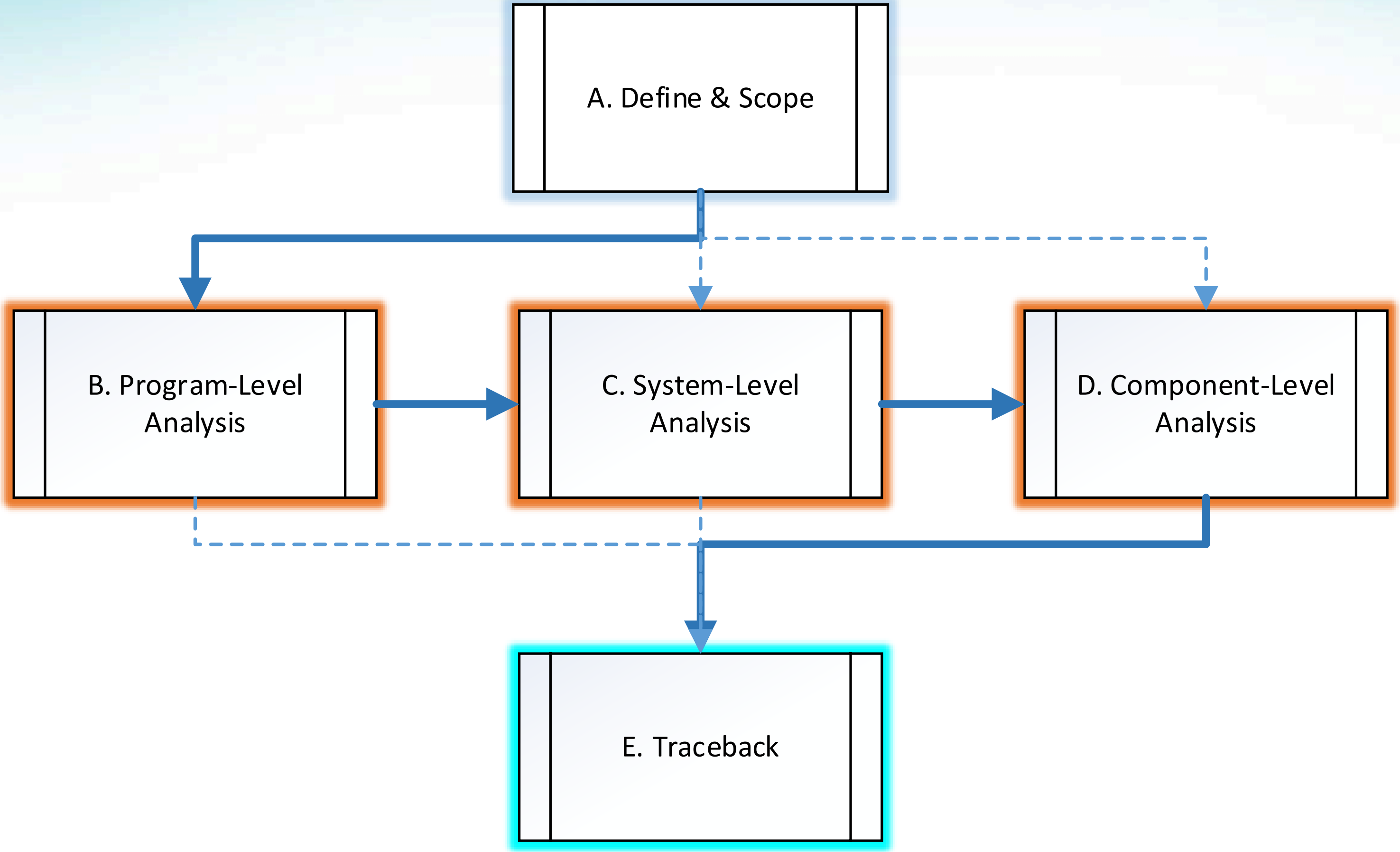
Baseline Criticality Level for Each Analyzed Workflow Path

Iterate as needed

End

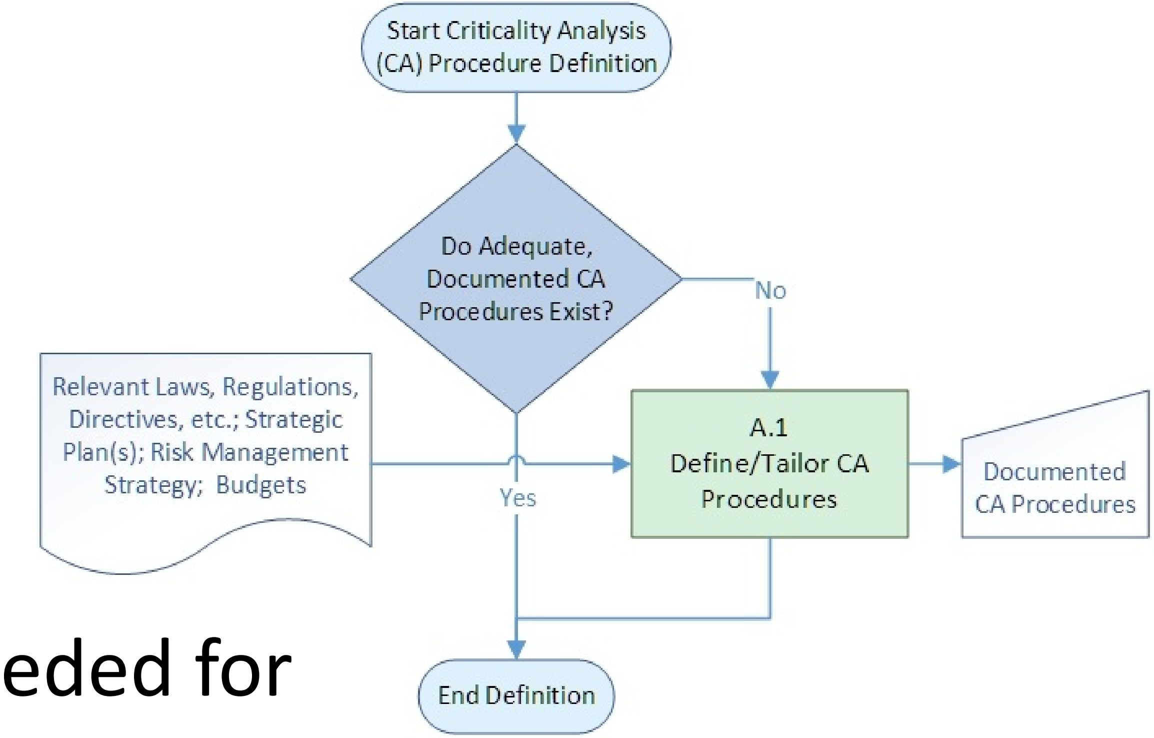
ID	
Name	
Description	
Inputs	
Outputs	
Roles & Responsibilities	(Process only)
Methods	(Sub-process only)
Related Processes	

Criticality Analysis Process



Process A: Define & Scope

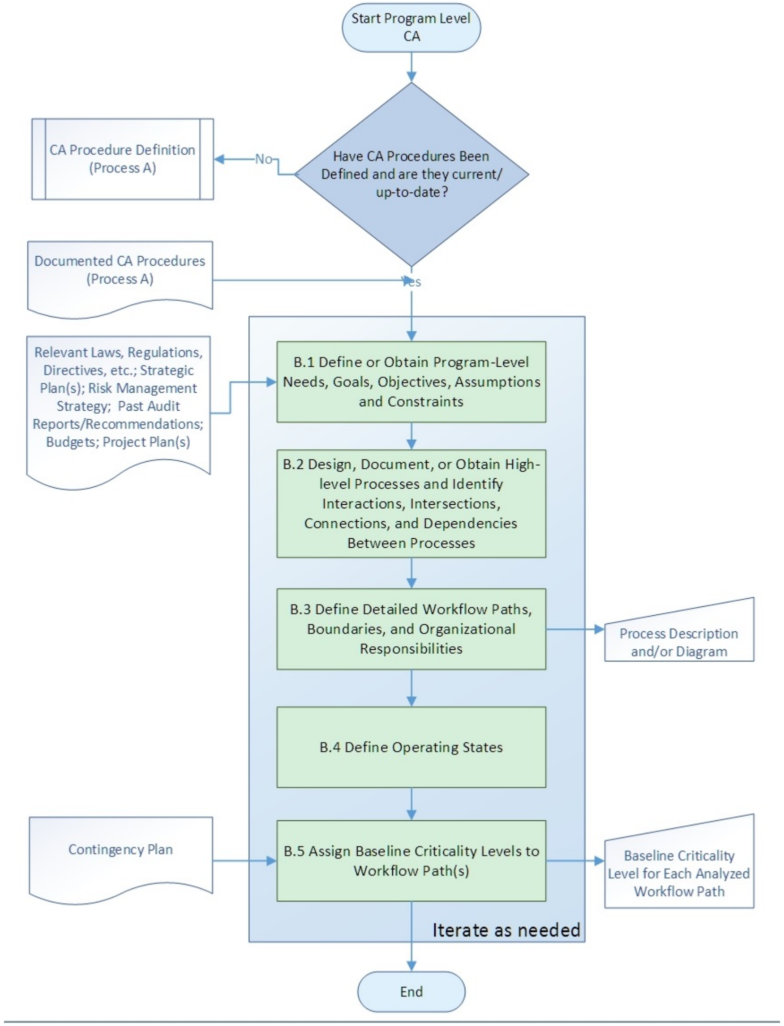
- Define:
  - Who
  - When
  - How


Start Criticality Analysis (CA) Procedure Definition
Do Adequate, Documented CA Procedures Exist?
No
Relevant Laws, Regulations, Directives, etc.; Strategic Plan(s); Risk Management Strategy; Budgets
Yes
A.1 Define/Tailor CA Procedures
Documented CA Procedures
End Definition

- Tailor if needed for each analysis

Process B: Program-Level Analysis

1. Goals, assumptions, constraints, etc.
2. Activities
3. Dependencies
4. Operating States
5. Baseline Criticality Levels



Start Program Level CA

Have CA Procedures Been Defined and are they current/ up-to-date?

No

CA Procedure Definition (Process A)

Yes

Documented CA Procedures (Process A)

Relevant Laws, Regulations, Directives, etc.; Strategic Plan(s); Risk Management Strategy; Past Audit Reports/Recommendations; Budgets; Project Plan(s)

B.1 Define or Obtain Program-Level Needs, Goals, Objectives, Assumptions and Constraints

B.2 Design, Document, or Obtain High-level Processes and Identify Interactions, Intersections, Connections, and Dependencies Between Processes

B.3 Define Detailed Workflow Paths, Boundaries, and Organizational Responsibilities

Process Description and/or Diagram

B.4 Define Operating States

Contingency Plan

B.5 Assign Baseline Criticality Levels to Workflow Path(s)

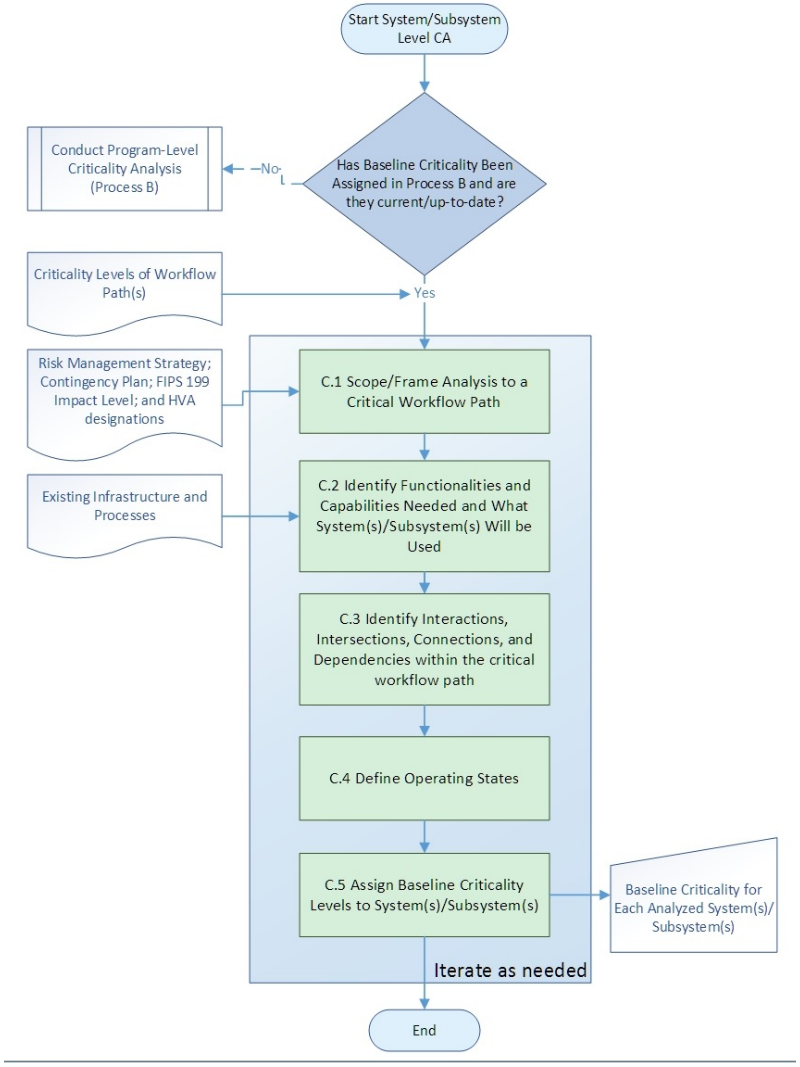
Baseline Criticality Level for Each Analyzed Workflow Path

Iterate as needed

End

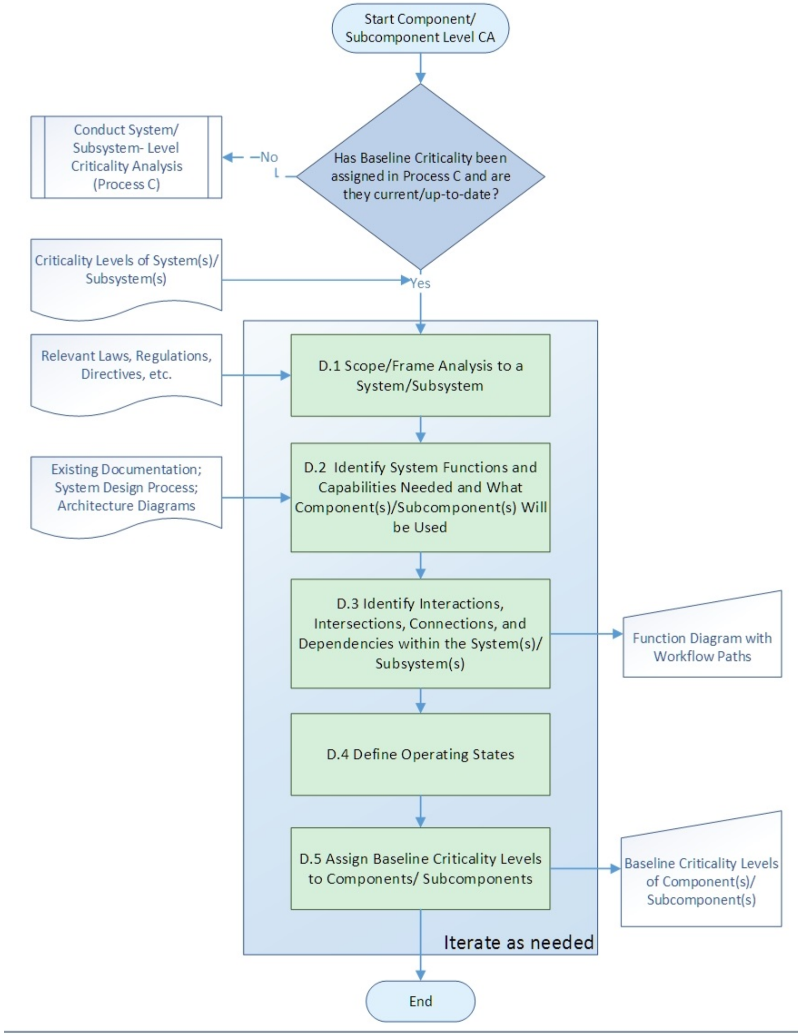
Process C: System/Subsystem-Level Analysis

1. Scope
2. Functions
3. Dependencies
4. Operating States
5. Baseline Criticality Level


Start System/Subsystem Level CA
Has Baseline Criticality Been Assigned in Process B and are they current/up-to-date?
No
Conduct Program-Level Criticality Analysis (Process B)
Yes
Criticality Levels of Workflow Path(s)
Risk Management Strategy; Contingency Plan; FIPS 199 Impact Level; and HVA designations
Existing Infrastructure and Processes
C.1 Scope/Frame Analysis to a Critical Workflow Path
C.2 Identify Functionalities and Capabilities Needed and What System(s)/Subsystem(s) Will be Used
C.3 Identify Interactions, Intersections, Connections, and Dependencies within the critical workflow path
C.4 Define Operating States
C.5 Assign Baseline Criticality Levels to System(s)/Subsystem(s)
Baseline Criticality for Each Analyzed System(s)/ Subsystem(s)
Iterate as needed
End

Process D: Component/ Subcomponent-Level Analysis

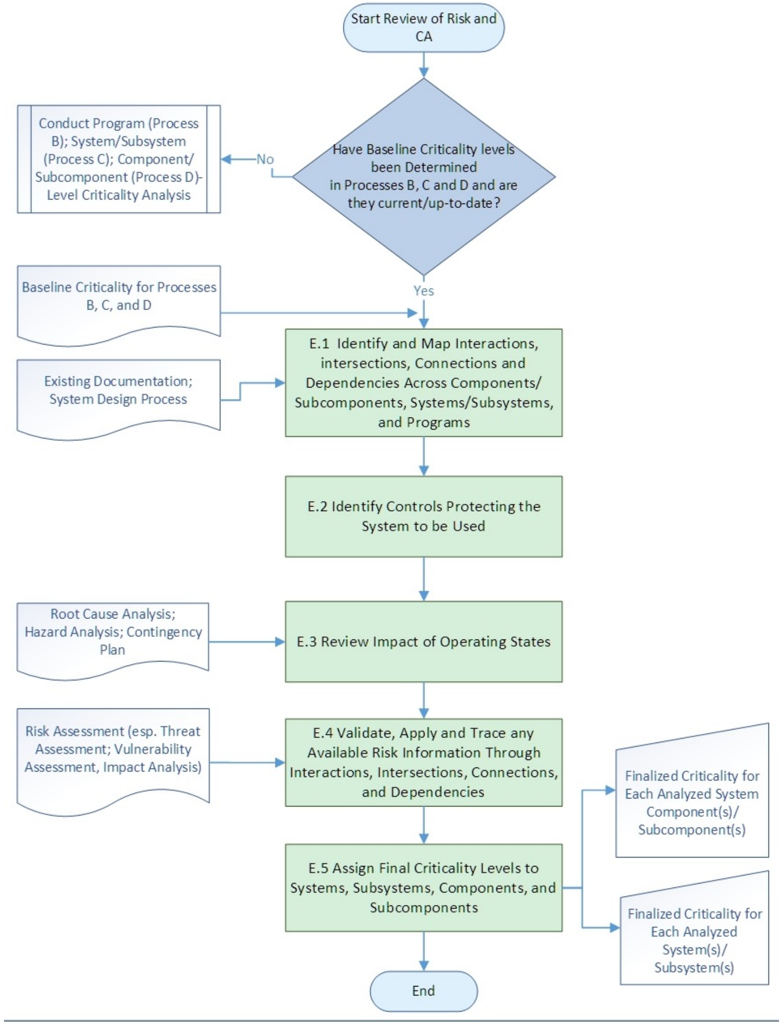
1. Scope
2. Functions
3. Diagram
4. Operating States
5. Baseline Criticality Levels


Start Component/ Subcomponent Level CA
Has Baseline Criticality been assigned in Process C and are they current/up-to-date?
No
Conduct System/ Subsystem- Level Criticality Analysis (Process C)
Yes
Criticality Levels of System(s)/ Subsystem(s)
Relevant Laws, Regulations, Directives, etc.
Existing Documentation; System Design Process; Architecture Diagrams
D.1 Scope/Frame Analysis to a System/Subsystem
D.2 Identify System Functions and Capabilities Needed and What Component(s)/Subcomponent(s) Will be Used
D.3 Identify Interactions, Intersections, Connections, and Dependencies within the System(s)/ Subsystem(s)
Function Diagram with Workflow Paths
D.4 Define Operating States
D.5 Assign Baseline Criticality Levels to Components/ Subcomponents
Baseline Criticality Levels of Component(s)/ Subcomponent(s)
Iterate as needed
End

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

Process E: Traceback

1. Identify connections & dependencies
2. Identify Existing Controls
3. Review Impact of Operating States
4. Apply Risk Info
5. Final Criticality Level



Start Review of Risk and CA

Have Baseline Criticality levels been Determined in Processes B, C and D and are they current/up-to-date?

No

Conduct Program (Process B); System/Subsystem (Process C); Component/ Subcomponent (Process D)-Level Criticality Analysis

Yes

Baseline Criticality for Processes B, C, and D

Existing Documentation; System Design Process

E.1 Identify and Map Interactions, intersections, Connections and Dependencies Across Components/ Subcomponents, Systems/Subsystems, and Programs

E.2 Identify Controls Protecting the System to be Used

Root Cause Analysis; Hazard Analysis; Contingency Plan

E.3 Review Impact of Operating States

Risk Assessment (esp. Threat Assessment; Vulnerability Assessment, Impact Analysis)

E.4 Validate, Apply and Trace any Available Risk Information Through Interactions, Intersections, Connections, and Dependencies

E.5 Assign Final Criticality Levels to Systems, Subsystems, Components, and Subcomponents

Finalized Criticality for Each Analyzed System Component(s)/ Subcomponent(s)

Finalized Criticality for Each Analyzed System(s)/ Subsystem(s)

End

Things to Note

- Iterates throughout
- Analyses are hierarchical
  - Multiple hierarchies of systems (of systems of systems of systems of systems)
  - begin at a high level and repeat at a lower level until desired detail is reached
- FLEXIBLE
  - Meant to work <u>with</u> existing processes, not to replace or duplicate

Related Work

- Cyber-Supply Chain Risk Management

  csrc.nist.gov/scrm

- FISMA

  csrc.nist.gov/Projects/Risk-Management

- Cybersecurity Framework

  www.nist.gov/cyberframework

Questions?

Celia Paulsen

Security Engineering and Risk Management Group

National Institute of Standards and Technology

celia.paulsen@nist.gov