Goal-Based Assessment for the Cybersecurity of Critical Infrastructure

IEEE HST 2010

November 10, 2010

Overview of assurance cases

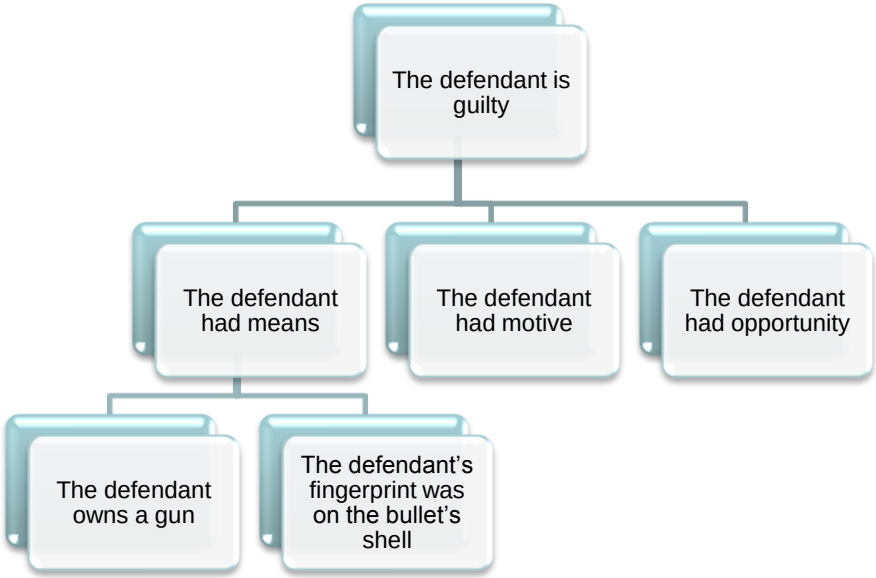
An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system holds – NIST SP 800-53

- Should convince an objective reviewer that:

The goals are valid

Claims are reasonable

Evidence supports the claims



Challenges of assessing cyber security in critical infrastructure

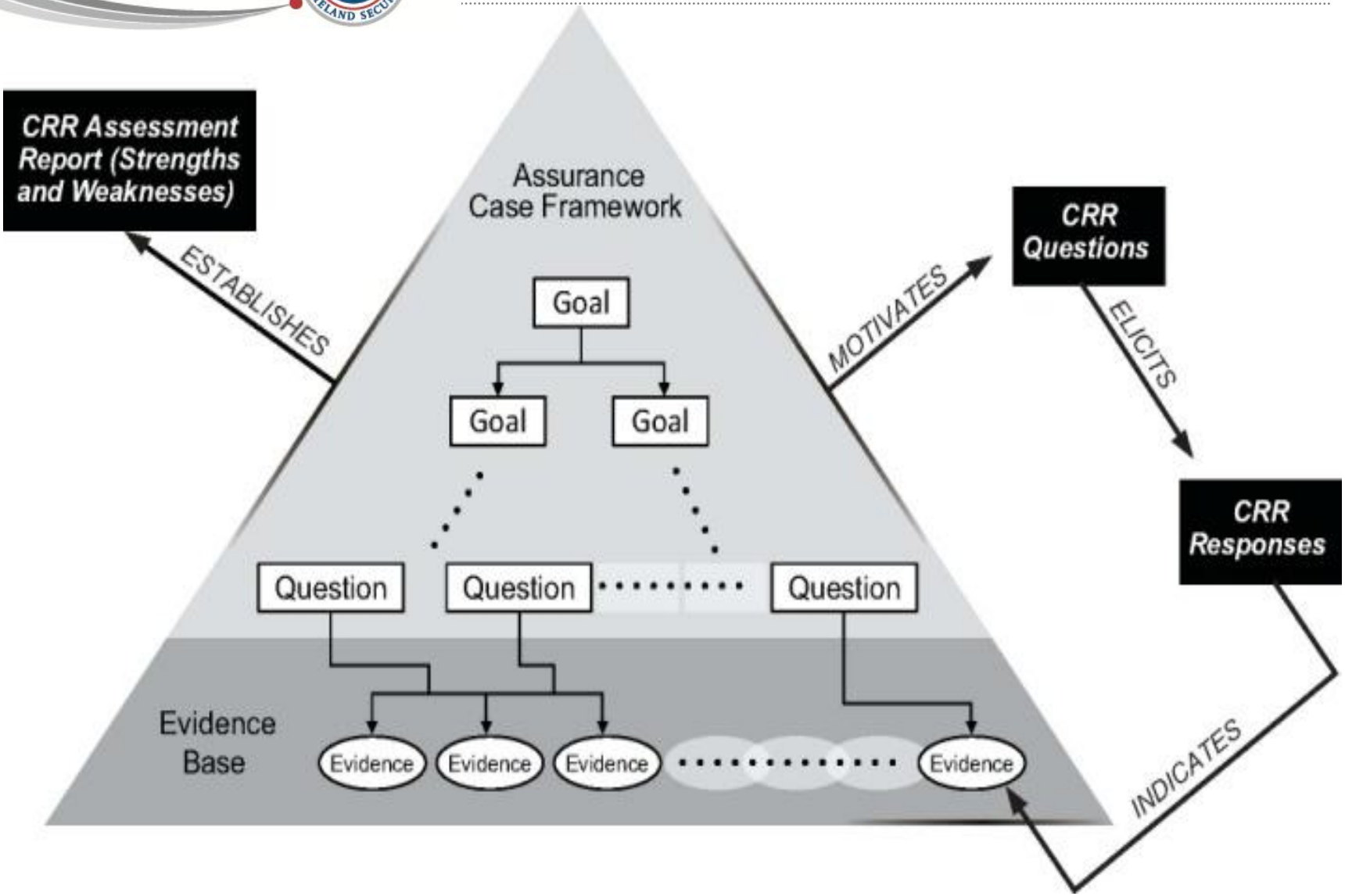
- Limited insight into the cyber security capabilities of owners and operators
- Difficulty evaluating evidence of cyber security performance within the context of national security objectives
- Heterogeneous technologies and practices across infrastructures
- Lack of reference models for national cyber security

Goal-based assessments provide

- Direction for areas of investigation during assessment design
- A means to communicate about the assessment
  - enables scrutiny of the assessment
  - assists in the identification of assumptions and gaps
- Context for analysis and reporting of assessment results
  - analyze sufficiency of evidence obtained during an assessment in terms of goal achievement
  - characterize the impact of weaknesses

CYBER RESILIENCE REVIEW

Assurance case framework



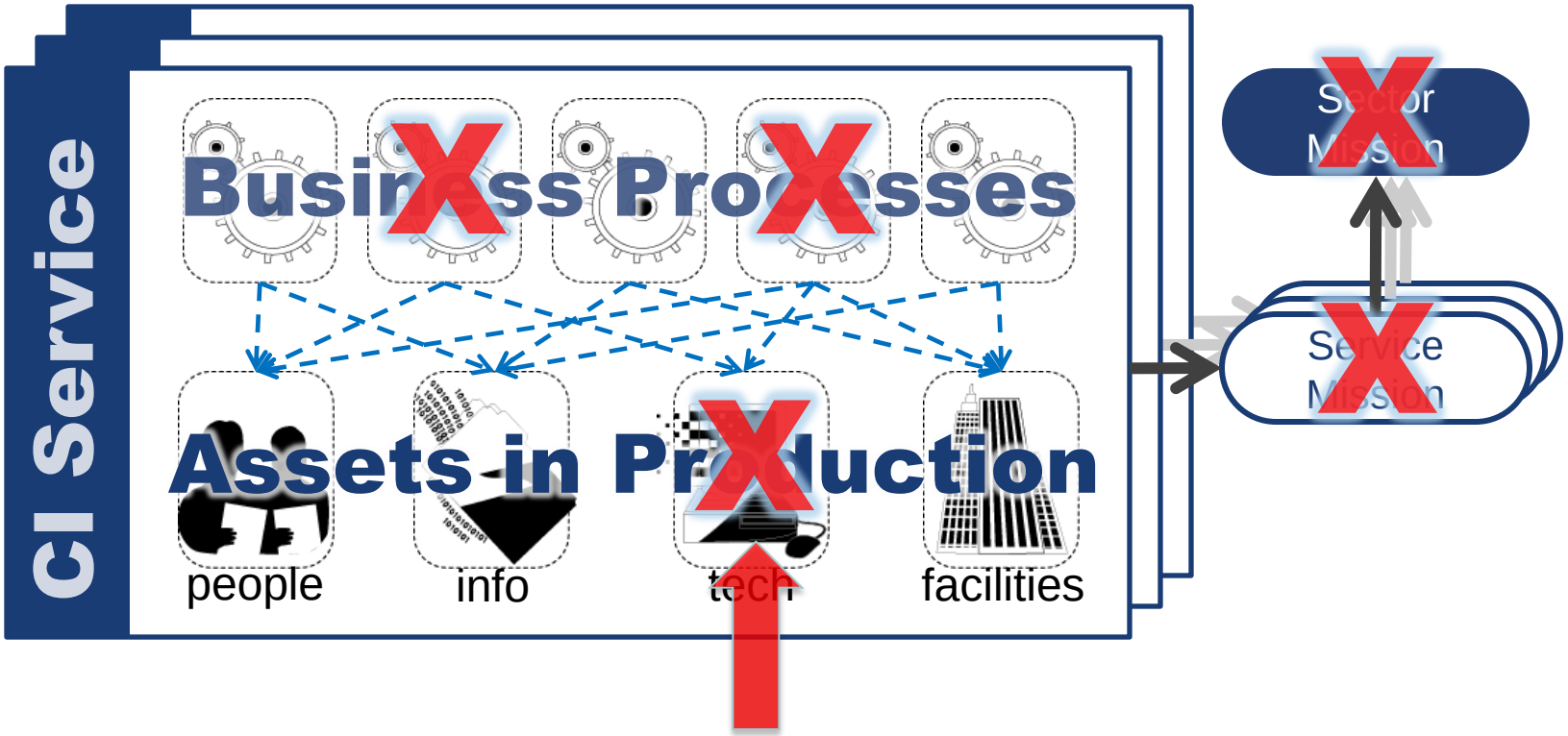
CERT®-RMM as a reference model

The CERT® Resilience Management Model (CERT-RMM) is a capability model for managing and improving operational resilience.

http://www.cert.org/resilience/

- Establishes a **service focus**, aligning an organization's assets to its mission
- Examines the identification and maintenance of **requirements** for protection and sustainment of assets
- Positions **operational resilience** in a process improvement view
- Includes 26 **"process areas"**
- Focuses on the operations phase of the lifecycle
- Uses CMMI architecture for ease of adoption

“Critical infrastructure service” orientation



Operational risk can disrupt an asset

And lead to organizational disruption

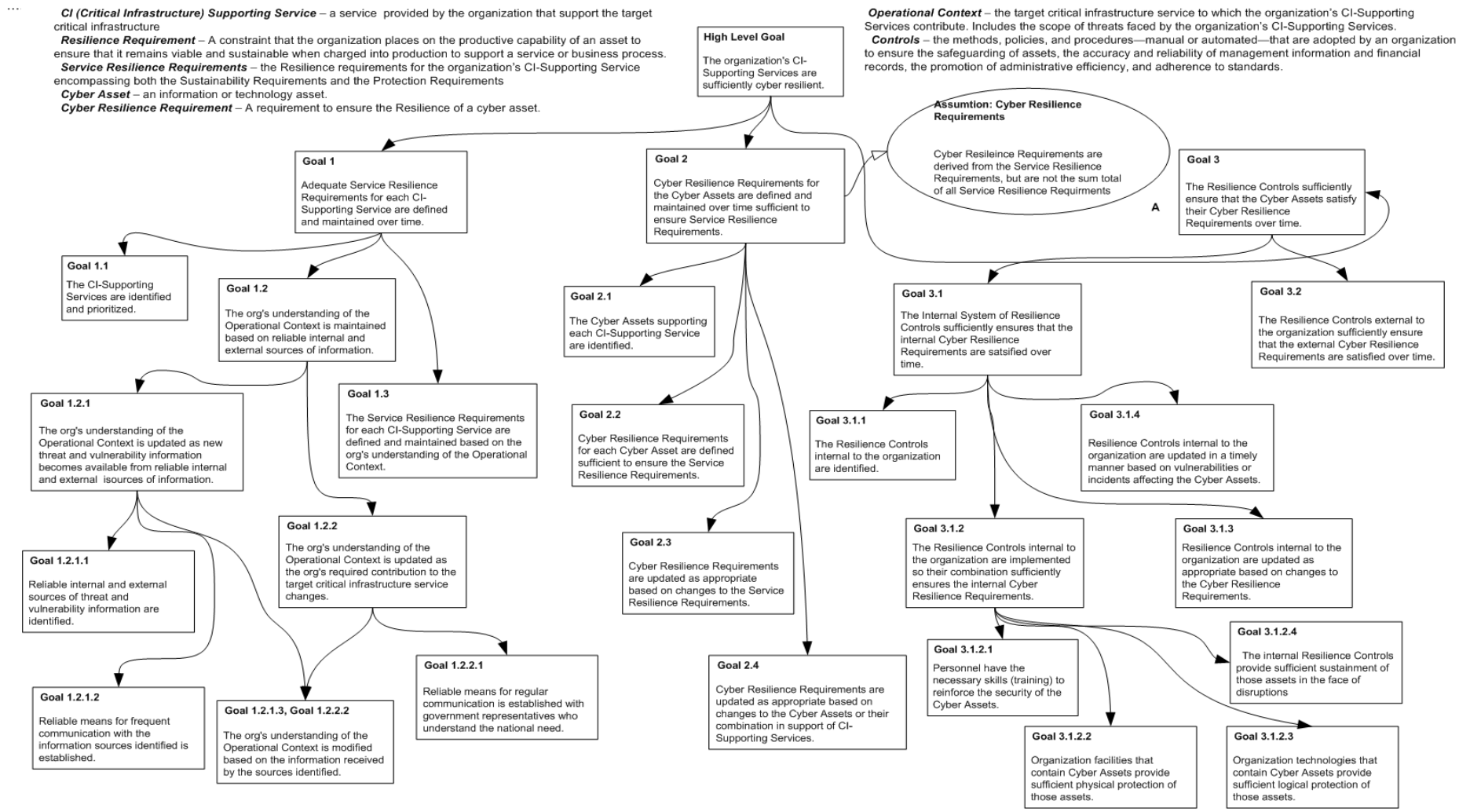
Which leads to CI failure

A case for cyber resilience:

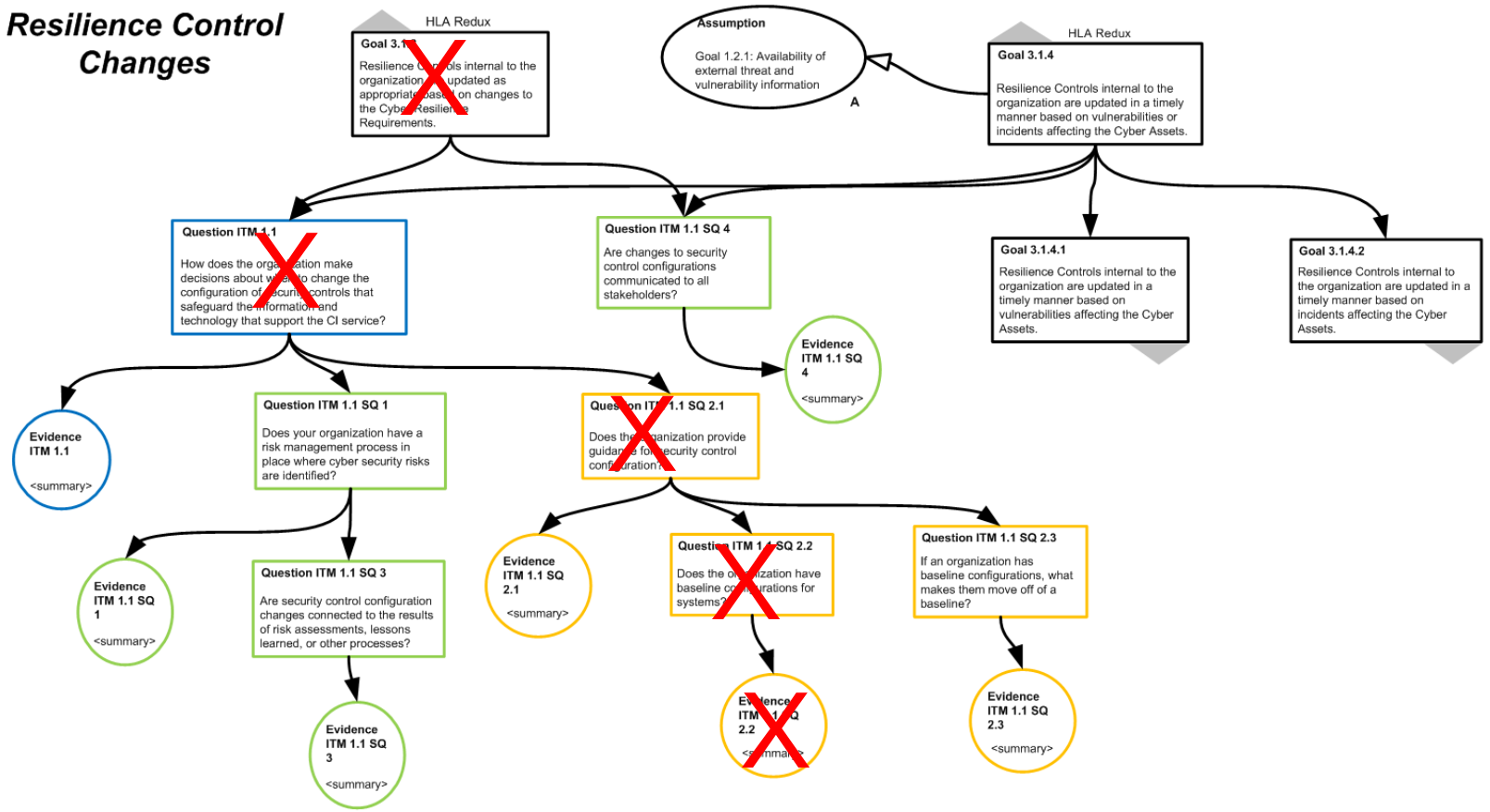
The organization's CI-Supporting Services are sufficiently cyber resilient.

- Adequate service resilience requirements for each CI-supporting service are defined and maintained over time.
- Cyber resilience requirements for the cyber assets are defined and maintained over time sufficient to ensure service resilience requirements.
- The resilience controls sufficiently ensure that the cyber assets satisfy their cyber resilience requirements over time.

The CRR assurance case



Assurance case provides context



Example Cyber Resilience Review goals

- Trace assets to critical infrastructure services
- Develop effective protection and sustainability strategies for information and technology assets.
- Identify criteria for changing the protection strategies for assets that support critical infrastructure.
- Identify and mitigate operational risk.
- Validate the function of security controls.
- Ensure effective cyber security training and awareness.

Example Cyber Resilience Review questions

Goal: Define evaluation criteria for vulnerabilities.

1. Has the organization defined criteria by which vulnerabilities can be evaluated?
2. Are the criteria aligned with the role that a given asset plays in production of the service?
3. How does the organization ensure that it effectively communicates about vulnerability evaluation criteria to its employees?
4. How does the organization ensure that the vulnerability evaluation criteria remain consistent with its operating priorities?

Benefits and challenges of this approach

Benefits

- Establishes objectives for assessment questions
- Enables scrutiny of the assessment
- Facilitates analysis within a specific context

Challenges

- Subjectivity in defining "completeness" of the argument.
- Unidentified assumptions
- Increased need for subject matter expertise on the part of the assessor

CERT contacts

Samuel A. Merrell

smerrell@cert.org

Andrew P. Moore

apm@cert.org

James F. Stevens

jfs@cert.org

Richard Lynch
Public Relations — All Media Inquiries
public-relations@sei.cmu.edu

SEI Customer Relations
customer-relations@sei.cmu.edu
412-268-5800

Mike Greenwood
For info on working with us
mgreenwood@sei.cmu.edu

REFERENCES

J. Goodenough, H. Lipson, and C. Weinstock, “Arguing security- creating assurance cases,” Carnegie Mellon University, 2007, 2008 [Online]. Available: https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.html

S. Lautieri, D. Cooper, D. Jackson, and T. Cockram, “Assurance cases: How assured are you?” in *International Conference on Dependable Systems and Networks 2004*, DSN-2004 [Online]. Available: http://www.praxis-his.com/downloads/whitepapers/AssuranceCase_DSN04.pdf

T. P. Kelly, “Arguing Safety - A systematic approach to safety case management” DPhil Dissertation, Dept. of Computer Science, Univ. of York, UK, 1998.

J. Goodenough and C. Weinstock, “Towards an assurance case practice for medical devices,” Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2009-TN-018, October 2009.

S. Blanchette, “Assurance cases for design analysis of complex system of systems software,” in *Proc. of the AIAA Infotech@Aerospace Conference*, Seattle, WA, 6 - 9 April 2009.

T. Rhodes, F. Boland, E. Fong, and M. Kass, “Software assurance using structured assurance case models,” NIST, May, 2009 [Online]. Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=902688

J. Penny, A. Eaton, P. G. Bishop, and R.E. Bloomfield, “The practicalities of goal-based safety regulation,” in *Aspects of Safety Management: Proceedings of the Ninth Safety-Critical Systems Symposium Bristol*, UK, 6-8 February 2001, F. Redmill and T. Anderson (eds.), London; New York: Springer, 2001, pages 35-48 [Online]. Available: http://www.adelard.com/papers/scsc2001_sw01.pdf

W. Greenwell and J. C. Knight, “Framing analysis of software failure with safety cases,” Department of Computer Science, University of Virginia, Charlottesville, VA, 2006 [Online]. Available: http://www.cs.virginia.edu/~jck/publications/greenwell.ress06.pdf

C. Howell and S. Ankrum, “Looking for a good argument,” Assurance Case Frameworks, May 2003, MITRE [Online]. Available:

http://www.asq509.org/ht/action/GetDocumentAction/id/476

T. P. Kelly and R. A. Weaver, “The goal structuring notation – A safety argument notation,” *Proceed. of the Dependable Systems and Networks 2004 Workshop on Assurance Cases*, Florence, Italy, July 2004.

R. Caralli, J. Allen, P. Curtis, D. White, L. Young, *CERT® Resilience Management Model,Version 1.0*, May 2010, Carnegie Mellon University, Pittsburgh, PA [Online]. Available: http://www.cert.org/resilience