Adapting NIST Cybersecurity Framework for Risk Assessment

Kenny Mesker, ICS Cybersecurity Engineer, Chevron ETC

NIST Conference, October 29, 2014

Overview

We need:

- To align with industry standards
- To provide an efficient method of providing an ICS cybersecurity risk assessment.
- A scorecard to measure business unit ICS cybersecurity posture so that our limited resources can be best focused where they are most needed.
- A common, standardized ICS cybersecurity assessment methodology that will provide a rationalized dashboard to measure enterprise-wide ICS cybersecurity posture.

Goals

Develop an ICS Cybersecurity Risk Assessment methodology that provides the basis for enterprise-wide cybersecurity awareness and analysis that will allow us to:

- Impact the business unit the least
- Utilize fewer resources
- Align with industry standards
- Provide a quantitative view of risk
- Standardize the results
- Align with the tools and capabilities that exist today
- Provide specific and actionable mitigation recommendations
- Show our work

The Two Parts to a Risk Assessment.

- Conformance Assessment
  - Determination of how “conformant” an ICS is to a set of general expectations
  - This is different from “compliance”
- Risk Analysis
  - The identification and prioritization of risks based on the results of the conformance assessment

Preliminary Methodology Before NIST Cybersecurity Framework

First attempt was made in 2013 using DHS CSET Tool

- Provides questionnaires which align with industry standards
- Used 300 “basic” questions based on NIST 800
- Questions are weighted, prioritized, and areas of concern are determined
- However, this is done according to a DHS internal algorithm and cannot be modified
- This provides a quick (though not thorough or custom) solution to the conformance problem

Results of Preliminary Methodology

Stakeholders were pleased with structured interview style

BUT:

- Unable to add company-specific questions
- Binary answers (yes/no) to questions led to “yes bias”
- Results were generally useful, but lacked the granularity needed to focus on specific mitigations
- Results were influenced by the weighting and prioritizations that are hard-coded in the CSET tool by the DHS
- Outcome was good, but not great

Determined a more customizable solution was needed

Framework for Improving Critical Infrastructure Cybersecurity

- February 12, 2014, as a result of the Presidential Executive Order 13636, the Framework for Improving Critical Infrastructure Cybersecurity was published by NIST
- Not a standard, but rather an approach to describing cybersecurity expectations
- Based on many standards, best practices, and guidelines
- Easily relatable between internal and external stakeholders
- The Framework is technology neutral
- Can be applied internationally

Alignment with NIST Cybersecurity Framework

- 22 Categories
- 98 Sub-categories
- Provides common taxonomy
- Alignment with industry and corporate strategy

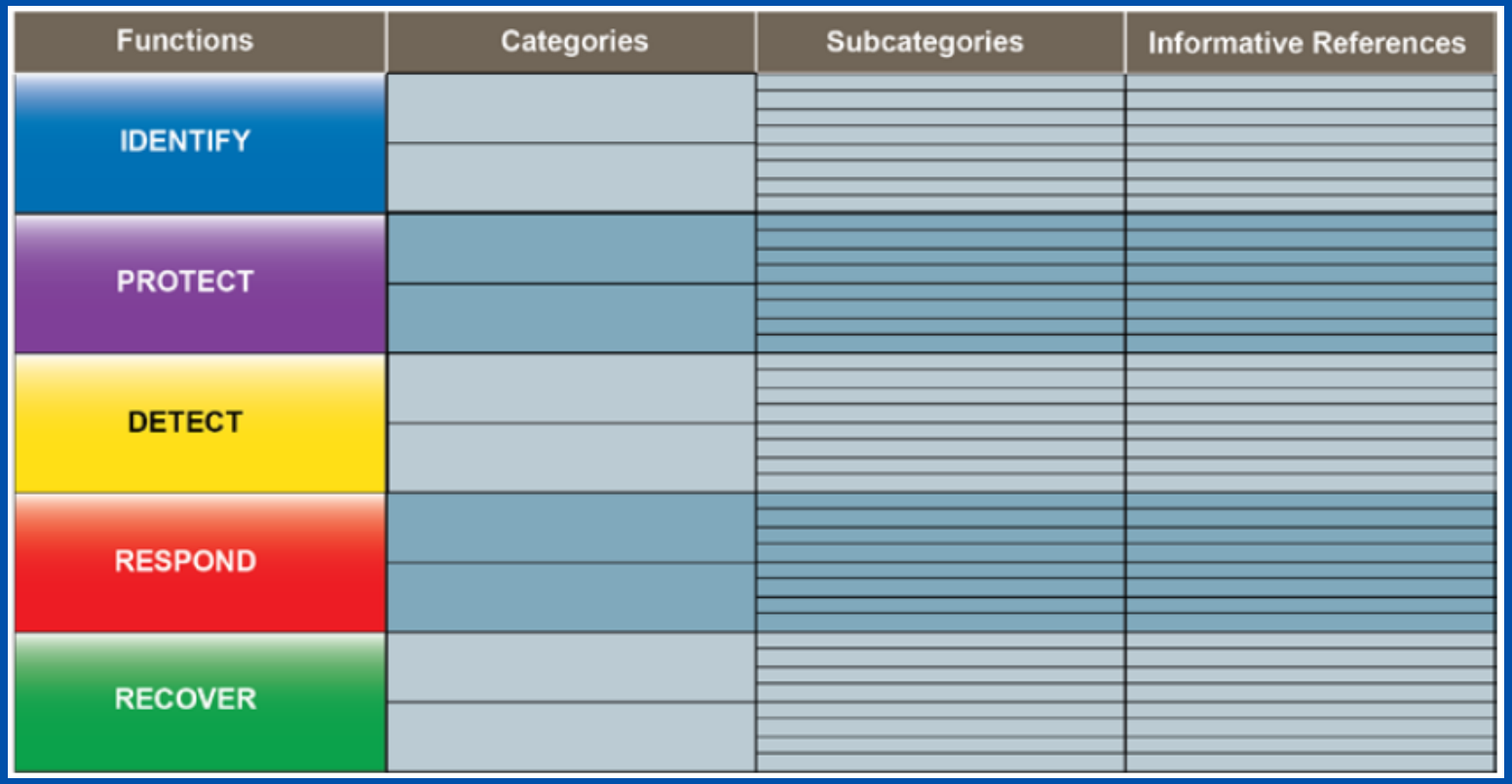


Image Source: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce.
Not copyrightable in the United States.

Original NIST Cybersecurity Framework

FUNCTION	CATEGORY	SUBCATEGORY	INDUSTRY STANDARDS IN ALIGNMENT
PROTECT (PR)	**Data Security (PR.DS)**: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	CCS CSC 17 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 ISO/IEC 27001:2013 A.9.1.1 NIST SP 800-53 Rev. 4 SC-28 IEC/ISA 62443-2-1:2010 4.3.2.5, 4.3.2.6, 4.3.3.3, 4.3.4.3, 4.3.4.4, 4.3.4.5

Add Assessment Criteria to Framework

FROM ORIGINAL FRAMEWORK

SUBCATEGORY

PR.DS-1: Data-at-rest is protected	**PR.DS-1.1:** Are identity and access management policies in place to protect data-at-rest?	ISO 27001:2013 A.9.1.1
	PR.DS-1.2: Has high value information been identified and protected?	IEC 62443-2-2:4.2.3.6 Internal Standards
	PR.DS-1.3: Are processes in place to ensure that sensitive data is adequately protected	NIST 800-53:SC-28 Internal Standards

GENERATED ASSESSMENT QUESTIONS

SPECIFIC STANDARDS/CONTROLS (INCLUDING INTERNAL) USED TO GENERATE QUESTIONS

The Risk Assessment Scorecard

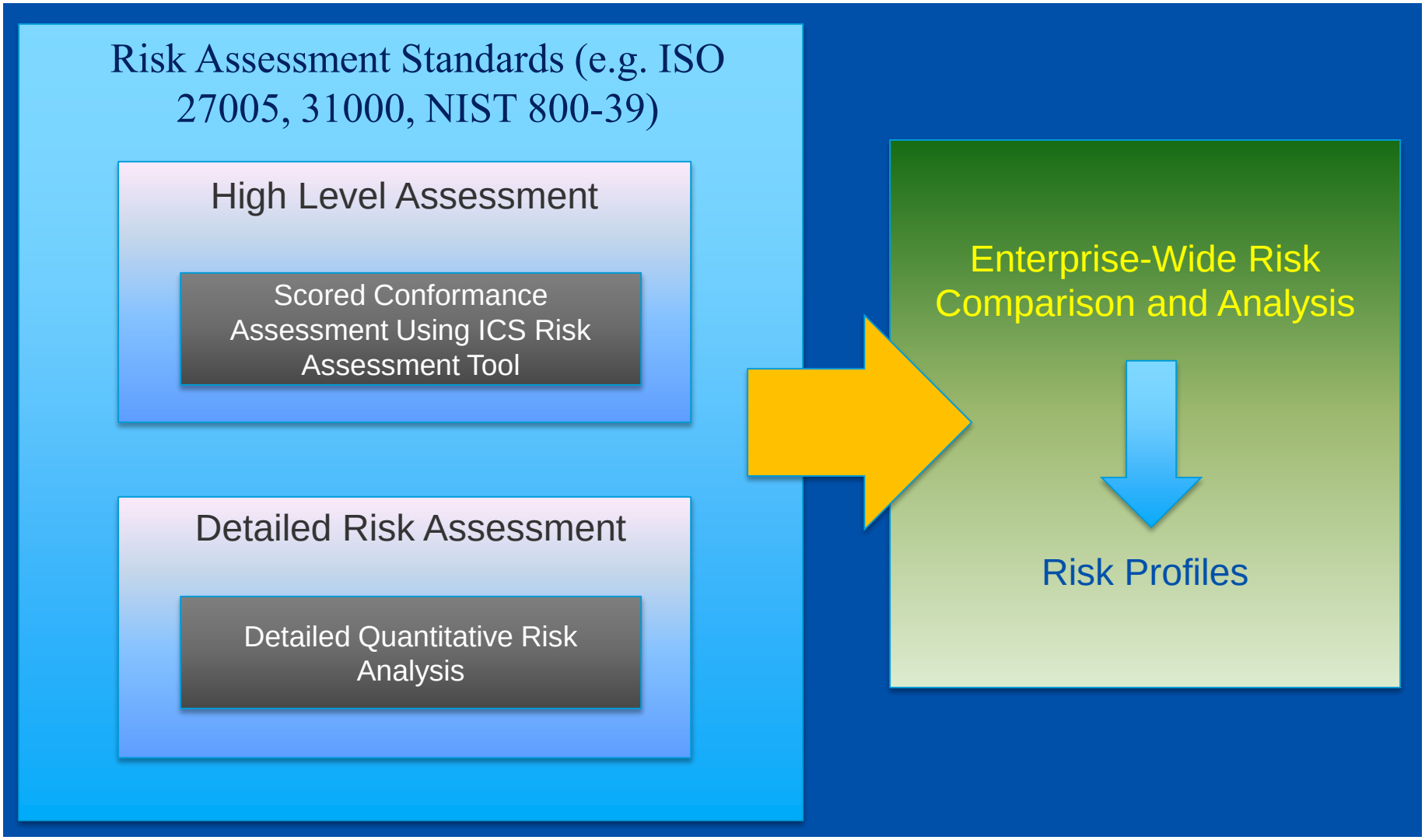
Not Aware	Awareness	Fundamental Application	Skilled Application	Mastery
	Initial	Basic	Advanced	Leader
0	1	2	3	4
No awareness, no knowledge	Processes are usually ad-hoc, not documented (informal), poorly controlled, and not repeatable.	Processes are managed, documented and used most of the time. May still have inconsistent execution.	Processes are standardized, well established, consistently used, repeatable, periodically reviewed and updated.	Processes are continuously assessed for improvement. Could be considered best in class or leading practice. Shareable and adopted by others

DETECT (DE)	1.22	Anomalies and Events (DE.AE)	1.10	**DE.AE-1:** A baseline of network operations and e	1.33
				DE.AE-2: Detected events are analyzed to unders	1.50
				DE.AE-3: Event data are aggregated and correlat	0.00
				DE.AE-4: Impact of events is determined	1.67
				DE.AE-5: Incident alert thresholds are establishe	1.00
		Security Continuous Monitoring (DE.CM)	1.95	network is monitored to detect potential cybers	0.50
				DE.CM-2: The physical environment is monitore	3.00
				DE.CM-3: Personnel activity is monitored to det	2.80
				DE.CM-4: Malicious code is detected	2.00
				DE.CM-5: Unauthorized mobile code is detected	3.00
				DE.CM-6: External service provider activity is mo	3.00
				DE.CM-7: Monitoring for unauthorized personne	1.00
				DE.CM-8: Vulnerability scans are performed	0.33
		Detection Processes (DE.DP)	0.60	**DE.DP-1:** Roles and responsibilities for detection	0.00
				DE.DP-2: Detection activities comply with all app	0.00
				DE.DP-3: Detection processes are tested	0.00
				DE.DP-4: Event detection information is commu	2.00
				DE.DP-5: Detection processes are continuously i	1.00

The Enterprise Risk Assessment Dashboard

Assessment Score	BU's					
Row Labels	PCN N-1	PCN N-2	PCN N-3	N Total	PCN A-1	A Total
Identify	2.37	2.09	2.37	2.28	1.66	1.66
Protect	2.41	2.31	2.46	2.39	1.86	1.86
Access Control	2.31	2.00	2.54	2.28	2.27	2.27
Awareness Training	2.46	2.46	2.46	2.46	1.48	1.48
PR.AT-1: All users are informed and trained	2.46	2.46	2.46	2.46	1.75	1.75
PR.AT-2: Privileged users understand roles & responsibilities	2.46	2.46	2.46	2.46	1.00	1.00
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	2.46	2.46	2.46	2.46	1.67	1.67
PR.AT-4: Senior executives understand roles & responsibilities	2.46	2.46	2.46	2.46	2.00	2.00
PR.AT-5: Physical and information security personnel understand roles & responsibilities	2.46	2.46	2.46	2.46	1.00	1.00
Data Security	2.46	2.37	2.51	2.45	2.19	2.19
Information Protection	2.31	2.23	2.36	2.30	1.53	1.53
Maintenance	2.46	2.46	2.46	2.46	2.50	2.50
Protective Technology	2.58	2.46	2.58	2.54	2.05	2.05
Detect	2.21	2.19	2.31	2.24	1.34	1.34
Respond	2.40	2.11	2.42	2.31	1.54	1.54
Recover	2.15	2.15	2.15	2.15	1.50	1.50
Grand Total	2.35	2.19	2.39	2.31	1.64	1.64

Risk Assessment Methodology Summary



Questions?