From: "DAVIS Peter"
Date: Mar 16, 2017 8:51 AM
Subject: Cybersecurity Framework Version 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc:

I offer the following:

Line 34: I would move to year from version, thus this becomes “Cybersecurity Framework 2017”. This shows the currency of the standard whereas version does not tell me much other than there might have been another. Standards such as ITIL and PRINCE2 are moving there.
Line 109: Missing word after industry. I suggest “discourse.”
Line 204: I would replace “aware” with “informed.”
Line 251: Insert “the” before Framework.
Line 285: “Access Control” s/b “Identity Management and Access Control” due to change in new version.
Line 307: In lines 312 and 313 you list all the categories, so why not list SCRM and take out the word example.
Line 311: Since you listed them all these are not examples.
Line 312: “Access Control” s/b “Identity Management and Access Control” due to change in new version.
Line 316: Since you listed them all these are not examples.
Line 322: Since you listed them all these are not examples.
Line 328: Since you listed them all these are not examples.
Line 402: How does one accurately monitor? I could accurately monitor but this not mean what I am monitoring is accurate.
Line 430 Insert “an” before understanding.
Line 486: Previously you used the term “risk tolerance’ but here you use “risk appetite.” Best not to flip around on these terms as they do have precise meanings. All actions are plural except for “Implements” at the Implementation/Operations level.
Line 502: Curious as to why you would leave out plan in your list, as I would think this is where it provides great value.
Line 508: “purchase” s/b “purchasing.”
Line 562: Would footnoting ISO/IEC TR 27019:2013 be useful?
Line 576: Should “monitors” not be “maps” or “matches”?
Line 582 Capitalize “orient”.
Line 589: Why use the word “interdependent”?
Line 602: “manager” s/b “manage”.
Lines 611/618/619: You use the term OT here whereas you tend to use ICS elsewhere. I would prefer you mention IT, OT and CT (communications technology). I believe it is important to include CT as more and more of it is IP-based.
Line 625: “consume” s/b “purchase”.
Line 633: Insert “e.g.,” after open (.
Line 644: Pre-decided is not something I hear. How about “desired” or “predetermined” instead?
Line 669: I think 3.4 s/b 3.3.
Line 781: Footnote below this line has security spelled wrong. Why would you not reference NIST SP800-55?
Line 830: Aggregate of metrics does not equal a reduction. The metrics might indicate that but the reduction comes from implementation of compensating controls (safeguards)
Line834: %age uptime is a leading indicator as it provides information on whether I will meet my outcome of agreed system availability in the SLA.
Line 835: Communicating a strategy is an outcome or lagging indicator: I either I did or did not communicate, which I can only measure at the end of a period. And since communication is very qualitative, I can only determine whether it was communicated by interviews or surveys: also lagging.
Line 856: “sunset” s/b “subset”.
Line 858: One does not know whether the cloud uses hard drives.
Line 883: Here you flip back to ICS from OT.

Line 864: I did not review the Informative References.
Line 895: Change all CCS to CIS. For ID-SC.2-4, there is a missing reference for CIS CSC. Not sure why you added Authentication in PR.AC as it is part of either IdM or access control. Do not need final "integrity" in PR.DS-8. In PR.IP-1, "concept" s/b "principle". In PR.IP-2, I would change "system development life cycle" to "system development methodology". The former smacks of waterfall or spiral methods and not Agile, prototyping, etc. In RS.MI-3, I would drop "newly".
Line 908: Insert ":2013" after "27001". I am curious why you did not use ISO 27002 and ISO 27019 but went with the information security management system, and not code of practice.
Line 917: See previous comment about buyer. Missing period at the end of Buyer definition. In definition for Critical Infrastructure, I would change "the United States" to "a nation-state". You said you wanted wider acceptance in the world. ☺ Definition of cybersecurity is the definition of information security. You cannot co-opt information security into cybersecurity as not everything is digitized. Why not something like: "Cybersecurity focuses on protecting computers, networks, applications and any other computerized device from unauthorized access, change or destruction. Cybersecurity protects cyberspace. This infers it deals with securing anything that is computerized and networked in the organization, which may include supervisory control and data acquisition (SCADA) systems, process control systems (PCS), industrial control systems (ICS), air conditioning units, thermostats, servers, desktop computers, laptops, cyber-physical systems (CPS) and Internet of Things (IoT) devices, such as smart phones and watches, as well as those connections to public networks. Often, professionals call cyber-physical systems operational technology (OT). Operational technology includes industrial control systems (ICS) as well." In Leading Measurement definition, "achieve" s/b "achieved". Since you mentioned ISO 31000 and ISO 27005, you should use their definition of risk management, which would change "identifying, assessing and responding to" to "identifying, communicating, assessing, treating and monitoring risks". Believe period is missing from end of Supplier definition.
Line 920: You left in CCS and left out CIS.
Line 946: Did not review change table.

Sincerely,
Peter T. Davis