Cyber Security Definition Comparisons

Megan Leonard

ISEC 475

5/21/2023

There are a large number of definitions when it comes to cyber security as no one has come to an agreement on a single one. As technology expands, we are seeing more attacks on our security which can lead to problems. Software assurance lifecycle helps with making sure that our software is secure as we move forward. There are several different cyber security definitions that cover software assurance during its lifecycle. MITRE is one of these definitions as they have the idea of constant evolution as new attacks are found. Woody has a level of confidence in its functions to run as they are intended to and looks more at business risks and use of software. CNSS looks at vulnerabilities with a level of confidence that software is working as intended and is free of vulnerabilities. They also have a planned set of activities to ensure that the software lifecycle runs. ISO/IEC is made up of numerous definitions as it does its best to cover a lot of topics, so it has the most overlap between it and the other definitions.

The definition of Software Assurance has several different ideas that refer to the assurance. The first is having a level of confidence in the software being free of any vulnerabilities. The table 1.1 in section 1.2 of the book shows that everyone has that level of confidence except for NASA-STD -8739.8 that falls under CNSS 2015 as it has more focus on functioning as intended, which everyone has a check for, and activities that conform to product requirements, standards, and procedures which is shared with ISO/IEC but not the other CNS, MITRE, or Woody. Free of vulnerabilities is one that is covered by everyone except for Woody and NASA which makes sense as Woody is looking at predicting software assurance and the business around software assurance while NASA wants to make sure it functions and does as it is needed. Next is the intentional or accidental insertion of vulnerabilities being handled which Woody and NASA do not have marked as their focus is different. Unexpectedly ISO/IEC 27034 only has this one unmarked which is because its focus is on assisting in security application for others. The software lifecycle process is again not marked by only Woody and NASA as it does not align with their focus much, so they do not focus on it more than needed. Acceptable business risks are covered by Woody and ISO/IEC which makes sense as Woody seems more focused on business while the ISO/IEC has a far reach to cover as many points as it can. The same applies for business use of software with only Woody and ISO/IEC. The set of activities conforming to the product requirements, standards, and procedures is only marked by ISO/IEC, with their variety of points, and NASA which makes sense as the NASA-STD was created for NASA itself to use and if the activities do not conform accordingly then there could be problems.

MITRE, CNSS, and DoDI all have the same marks which is shown with how they focus more attention on threats. ISO/IEC seem to be trying to cover all basis which is shown with how their definitions are split into so many different ways and expanding.

At first glance, ISO/ISEC looks to be the best as it covers the most but that also means that its implementation may be harder or more tedious. The NASA definition was made as it would be used by NASA, so they shaped it to fit their needs. Woody is good if you are mostly focused on a one and done job as it focuses on the business and more short term with the software as companies could get software with their definitions and add onto it.

Being that the book is from 2017 it is interesting to see how the definitions have changed over time as some have not been as heard of like Woody while others have expanded like NASA. Between this year and 2017 from the book being released, NASA has already added a lot more standards that are split between the different areas of their work such as human factors having their own while materials are another standard. They have also suspended 3 standards between the six-year difference. The other standards are harder to find specifics for as searching for the woody definition did not show much and a lot of the ISO/IEC standards are behind a pay wall.

It would not be right to say that one definition is better than the other as they have different points of interest and reasons for why they were created. ISO/IEC is the definition that is seen the most as it has such a wide range of points it covers and has many different standards to fit the needs of a lot of different people.

In researching these, I found that the one the was easiest to find information on was in fact the NASA definitions and standards. NASA has a site that has a collection of all of their standards and in-depth documentation for public access. The book did not mention much about the NASA definition and standards. The NASA-STD 8739.8 that is listed in the book under the CNSS April 2015 was quite limited, but it has since been updated in 2022 and expanded upon.

I did not delve farther into the other definitions as much as I did with NASA as I found the number of standards and the different areas they are fascinating to go through. ISO/IEC covers a lot as well, but I found it harder to go through and look at any of the newer documentation without having to do a lot of roundabouts. MITRE has a site, but it is also hard to find more about the definitions and standards. CNSS has a site but each time I go to it, there is an error and a warning about the site not being protected while the rest of the search suggests others to look at.

Overall, each definition has its own focus and reason for being put into place. Everyone has their own thoughts on which one is the best or worse and I believe it is based on your needs if you are choosing a specific definition. I found that the NASA-STD definition has had the most change between the book release and this year.

Citations:

Editor, C. C. (n.d.). *CNSS - glossary: CSRC*. CSRC Content Editor. <https://csrc.nist.gov/glossary/term/cnss>

*ISO/IEC 15408-1:2009*. ISO. (2014, January 1). <https://www.iso.org/standard/50341.html>

*ISO/IEC 27034-1:2011*. ISO. (2022, October 27). <https://www.iso.org/standard/44378.html>

Mead, N. R., & Woody, C. C. (2017). *Cyber Security Engineering: A practical approach for systems and software assurance*. Addison-Wesley.

NASA. (n.d.). *Software assurance and software safety standard*. NASA. <https://standards.nasa.gov/standard/NASA/NASA-STD-87398>

*Software Assurance and Software Safety* . NASA TECHNICAL STANDARD NASA-STD-8739.8B. (2022, September 8). <https://standards.nasa.gov/sites/default/files/standards/NASA/B/0/NASA-STD-87398-Revision-B_1.pdf>

*Software Assurance*. Making security measurable - software assurance. (n.d.). <https://measurablesecurity.mitre.org/directory/areas/softwareassurance.html>

*Solving problems for Safer World*. MITRE. (2023, May 16). <https://www.mitre.org/>

*What is Mitre ATT&CK - definition: Vmware glossary*. VMware. (2023, March 20). <https://www.vmware.com/topics/glossary/content/mitre-attack.html>