February 20th, 2016

Author:
Alberto Piamonte
Senior GRC Consultant
ISACA Rome
ITALY
Email: alberto.piamonte@alice.it
tel: +39 331 459 4015

Submission to NIST RFI for
Critical Infrastructure Cyber Security Framework (CSF)

Use of the Framework

As member of ISACA Rome I was asked to investigate possible solutions to the IoT (Internet of Things) Governance issue.

Having studied and successfully applied in the past the CSF, I was wondering about a possible extension of the framework to IoT.

Going through the Informative References the focus has fallen on the 20 ***CCS CSC Controls***, and I discovered that they have been extended to cover also the IoT area[1]: *great*!

But trying to apply it I was a little disappointed because the content of the control pointed by the CSF framework in many cases made no sense in the specific Subcategory !

The reason was quickly found: the CSF refers to CIS Critical Security Controls (Version 5.1, old): while the present version is Version 6.0 [2]!

Now we are running the first pilot assessment and the results are very encouraging: under the CSF cover COBIT5 and CSC Controls nicely integrate.

The same approach could be extended to Privacy Impact Assessment (topic becoming very popular after the approval of the new European Regulation on Personal Data Protection)

[1] (https://www.cisecurity.org/critical-controls.cfm) CIS Critical Security Controls (Version 6): IoT Security

[2] A correspondence table is available

Possible Framework Update

1. Use the CIS Critical Security Controls (Version 6) numbers.
2. There is a typo error referencing to COBIT5 in Subcategory ID.GV-2 : APO13.12 does not exist, the correct reference is APO13.02. The error is repeated in the pdf doc., in the excel and in the interactive tool.

Regards

Alberto Piamonte