Risk Management Framework for Software Security

Access to research work on risk management by Gray McGraw added to PMWL

Resource provided by [Livinus Nweke](#)

10 February 2018 – Rome, Italy – Access to a new resource has been added to the PM World Library related to the Security of Project Data, Information and Systems. The new resource is titled **Risk Management Framework (RMF)**. This research work published by Gray McGraw on United States Computer Emergency Readiness Team (US-CERT) website.

As observed by the author, a continuous risk management process is a necessary part of any approach to software security. Software security risk includes risks found in artifacts during assurance activities, risks introduced by insufficient processes, and personnel related risks. An overall risk management framework (described here) can help make sense of software security. Note that we are explicitly teasing apart architectural risk analysis (one of the critical software security best practices) and the use of the risk management framework.

To access this great resource, go to the Applications and Hot Topics section of the library at http://pmworldlibrary.net/applications-and-topics/, scroll down and click on "Security of Project Data, Information and Systems". Must be a registered member and logged-in to access.

For post in PMWL:

[Risk Management Framework](#) (RMF) – 2005 research work on life-cycle activities published by Gray McGraw on United States Computer Emergency Readiness Team (US-CERT) website. The RMF described here is a condensed version of the Cigital RMF, a mature process that has been applied in the field for almost ten years. This RMF is designed to manage software-induced business risks. Through the application of five simple activities, analysts use their own technical expertise, relevant tools, and technologies to carry out a reasonable risk management approach. [For more, click here](#). ([Nweke](#))

URL for page in the PMWL for post: https://pmworldlibrary.net/project-data-systems-security/