C4 3.11: Risk Assessment

Created by Purdue University NSF # 1840043

800-171 Rev. 1 Mapping	Control Family	Required Control	Implementation	Program/Policy/Procedure Reference	Control Gaps
3.11.1	C4.3.11.1	Perform periodic risk assessments based on risk and/or regulatory requirements to organizational operations, assets, and individuals in the operation of systems. no less than annually. Recommended assessment tools include those described in NIST 800-53A (ex. vulnerability scanning, security control testing and reviews, configuration testing and reviews, log reviews, and personnel interviews).	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**	Various risk assessments take place including HIPAA, GLBA, vendor security reviews, network and application vulnerability scans also provide risk information. Per the Information Security & Privacy (VII.B.8), security officers are responsible for risk assessments of their respective areas.	
3.11.2	C4.3.11.2	Perform vulnerability scanning no less than monthly.	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**		
3.11.3	C4.3.11.3	**Reference Required Control C4 3.11.2**			