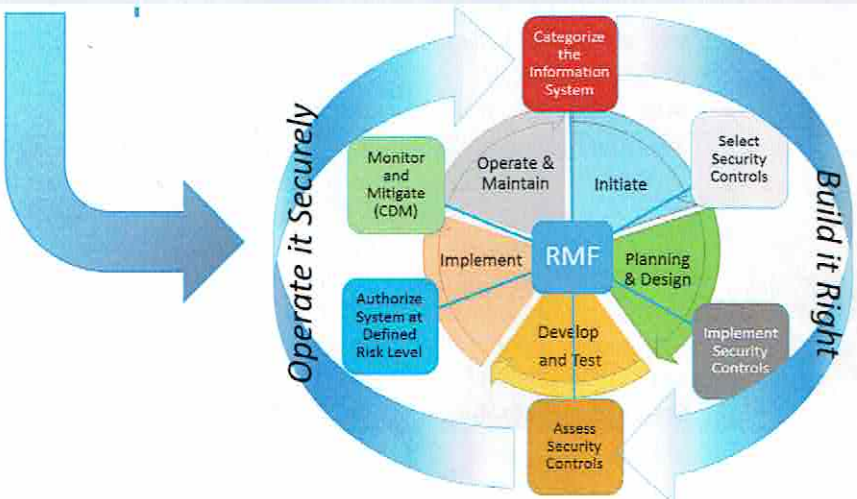
UW-MADISON'S RISK MANAGEMENT FRAMEWORK

The UW-Madison Risk Management Framework (RMF) is designed to provide departmental directors, researchers, and information technologists with a tool to determine risk to data and operations of each network or system connected to or serviced by the campus information technology architecture. The RMF consists of six steps that guide the development of a system with information security controls built in. Once development is completed, a formal risk assessment and continued operating checks ensure maintenance of defined risk levels. The table and graphics below describe the steps:

Step	Activity Title	Description
Pre	Planning	Conducting discovery with the System Owner to aid in their understanding of the RMF and associated tools and processes. Identification of time and resources occurs here.
1	Categorize the System	A data driven process where the security requirements of the system are defined by the highest classification of data handled by, or stored within, the system or processes
2	Select Security Controls	Assignment of the administrative, physical and technical controls required to protect the data are drawn from an agreed security controls framework (e.g., NIST 800-53)
3	Implement and Validate Controls	During design and development, the selected controls are incorporated in the system design, validated to provide the desired protections, and verified as operational.
4	Risk Assessment	Independent to the development team, a documented assessment is performed to test the selected controls. Residual risk is determined with mitigating factors applied. This stage leads to a formal declaration of risk for the system or network.
5	Authorize the System	A final risk review is conducted with a formal declaration of risk provided to the responsible Risk Executive who makes the determination whether to (1) operate the system at the defined risk level; (2) further mitigate risk; or (3) decline to allow continued operation.
	System is Operational	
6	Monitor and Mitigate	Continually assess the operational controls against evolving vulnerability, threat and impact factors. Disruption to operations or loss of data occurs when controls fail, system upgrades occur without proper testing or external factors dictate, determine and implement mitigating controls or return the system to an earlier RMF step. This step is also known as Continuous Diagnostics and Mitigation.



Infographic provided by the UW-Madison Office of Cybersecurity – December 1, 2016

OFFICE OF CYBERSECURITY