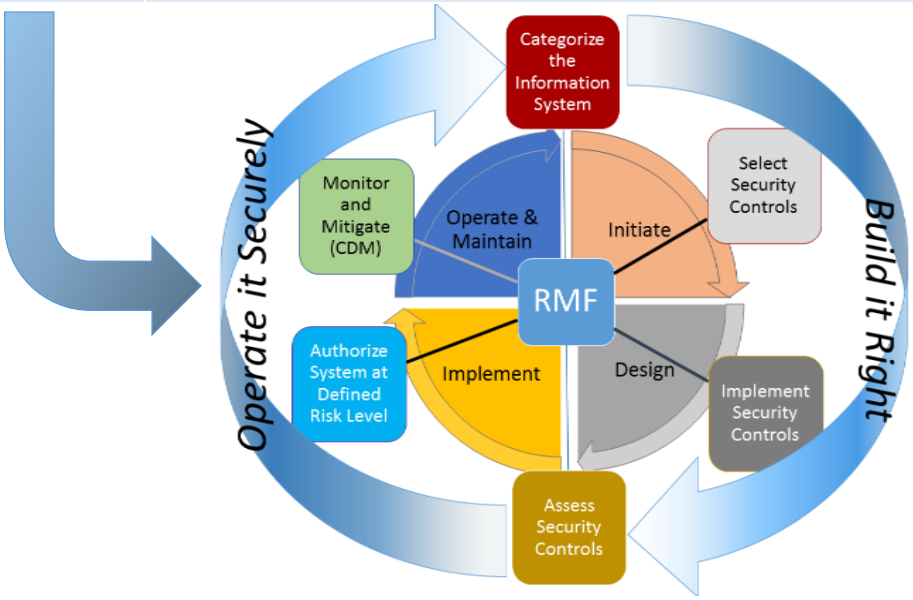
# UW-MADISON'S RISK MANAGEMENT FRAMEWORK

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 |
|---|---|---|
| 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 into 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. |
| 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 – June 1, 2016

OFFICE OF CYBERSECURITY
CIO AND VICE PROVOST FOR INFORMATION TECHNOLOGY
UNIVERSITY OF WISCONSIN-MADISON

# UW-MADISON'S RISK MANAGEMENT FRAMEWORK

Each step of the RMF collects specific input that will deliver outputs as shown in the table below that results in identifying and approving security controls. Specific questions, checklists and data workbooks are completed for each risk assessment. System Owners and Data Stewards will collaborate with the supporting IT staff, the Office of Cybersecurity, and the system operators and managers to ensure continued security for data and systems with compliance documentation is available and current.

| Step | Activity Title | Input Documents and Activities | Output Documents and Activities |
|---|---|---|---|
| 1 | Categorize the System | • Data definition including Classification<br>• FISMA determination from Contract<br>• Data description<br>• System description from SDLC | • Cybersecurity Project Charter<br>• System Security Plan (SSP) Questionnaire checklist<br>• Data Security Triage Form<br>• IT Security Baseline for Research and Academic Computing Template<br>• Interview Checklist(s): e.g., FISMA Controls, HIPPA Test Plan, SA Checklist |
| 2 | Select Security Controls | • Complete and Validated SSP Questionnaire checklist. | • Security Controls Inventory. |
| 3 | Implement and Validate Controls | • Configure Security Controls as determined. | • Completed Package Artifacts<br>  ○ SSP<br>  ○ Topology, Data Flow, System Security Boundary<br>  ○ Ports & Protocols Table<br>• Security Controls Workbook (Pre-Assessment)<br>• Submitted Cybersecurity Risk Acceptance Request Form |
| 4 | Risk Assessment | • Provide All Audit Scan (host based scans & application based testing)<br>• Completed Security Controls Checklist validated by scanning and manual review<br>• Develop and Execute Testing Plans (Artifacts not provided will be created by the Office of Cybersecurity)<br>• Step Three Deliverables | • Scanning tool (i.e., Qualys) generated Risk Assessment Report plus Analyst notes<br>• Executed CCI and NIST checklists<br>• Updated systems POAM<br>• Validated Step Three Artifacts<br>• Residual Risk Report |
| 5 | Authorize System | • Residual Risk Report<br>• Step Four deliverables | • Chief Information Security Officer signed Risk Letter plus Risk Executive's Endorsement/Approval to Operate |
| 6 | Mitigate and Monitor | • Approved scanning tool<br>• Control Validation Plan<br>• Step Five deliverables | • Provide Monthly Risk Reports & POAM updates<br>• Security Control Validation Report |

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

OFFICE OF CYBERSECURITY
CIO AND VICE PROVOST FOR INFORMATION TECHNOLOGY
UNIVERSITY OF WISCONSIN-MADISON