RTAG Working Group on Cybersecurity Policy
January 2018 Feedback on RMF Policy

Background

In December 2017, the RTAG Working Group on Cybersecurity Policy was reconvened and asked to review the most recent version of the Cybersecurity Risk Management Framework Policy and Implementation Plan documents. The feedback was to be given in the context of the feedback given in January 2017 on prior versions of the documents. The feedback below is structured such that individual pieces of feedback are associated with the place in the document that was being reviewed.

The feedback provided in January 2017 is included as the last section of this document for comparison purposes.

Overall Impression

Based on the individual feedback provided, there's consensus that the Policy document (dated 2017-12-11) and Implementation Plan document (dated 2017-11-20) are improvements over the versions reviewed in January 2017. There are still components which could greatly benefit from inclusion of the feedback below from the researcher community.

A good portion of the feedback below is commentary which the working group would appreciate being addressed through increased clarity in the wording of the documents. The feedback highlighted in green are specific elements which are missing or unclear and need to be addressed in the documents for the working group to support the policy.

Working Group Members

Faculty

Caprice Greenberg	Surgery
Garret Suen	Bacteriology
Jee-seon Kim	Education
Jeremy Morris	Communication Arts

Academic Staff

Rick Konopacki	SMPH
Lee Konrad	Libraries
Ryan Moze	OVCRGE
Carol Pech	Human Subjects IRB
Mark Sweet	RSP
Nicholas Tincher	OVCRGE & RTAG Chair

January 2018 Feedback on UW-Madison Cybersecurity Risk Management Policy (dated 2017-12-11) and Implementation Plan (dated 2017-11-20)

Note: The Office of Cybersecurity responses are below the item and highlighted in gray.

Overall

1. Defining the data categorization will present a challenge for various types of research data that is sensitive or restricted but doesn't fall under PHI and HIPAA. Having some working parameters for comparative sensitivity would be useful.

System category is determined primarily by the data classification. Discussions and determination of the data's classification and protection requirements should occur during the Planning activity shown in Appendix A to the Implementation Plan and agreed to during Step 1 of the RMF.

2. The whole document should be reviewed for grammar errors and consistency.

This action was accomplished. There are significant structural changes in order to align the many comments in a coherent manner. Changes to individual approach or policy sections are minimal while there were several additions and changes to the Implementation Plan to add clarity.

3. The tiered risk structure should be useful in helping researchers and the IRB understand what security requirements need to be in place.

The Risk structure should not be confused with data classification. In the Policy section and in the Implementation Plan several edits and additions were made to clarify the concepts and labels. A section was added in the Implementation Plan to address risk structure and identifiers based on NIST descriptions.

4. Speaking as a group that has gone through the RMF over a 2-year period and still not be officially completed (stalled at the Accepting Risk stage in designating a Risk Executive), the concern over available staffing and resources within the Office of Cybersecurity is daunting. The 5-yr staged approach for the timeline to implement somewhat addresses the resource concern. If this is the approach than time estimates should be given for each step within the framework – not for just enforcing the policy (60 days to name a Risk Executive, reduce critical risk within 72-96 hours, reduce high risk within 15 calendar days, reduce moderate risk within 90 calendar days, etc.). Expected response times from the Office of Cybersecurity shows accountability on their part not just for the information system being assessed.

The time within the processes and level of effort will vary for each system. Over time a better breakdown will emerge and the Office of Cybersecurity is well aware of the need to economize wherever possible. Tables were added in the Appendix A to the Implementation Plan showing

the Level of Effort required based on information system size and complexity and the estimated time for each stage of the RMF. These time estimates will be reviewed quarterly and the tables will be adjusted semi-annually and posted as an accessible link on the Cybersecurity web pages (link to be determined and announced once established).

5. The policy and implementation plan are written as more aspirational rather than something practical that can be easily implemented. This is particularly true of the policy document. There is a good amount of text in the policy document which are not policy statements. The success of compliance with this policy may be made better by having a policy that is written in a way that is more compatible with other UW-Madison policies. *This feedback is guided by the working group member's policy style, which is based on making concise policy statements and leaving the background for other documentation. If further follow-up here is welcome, contact information can be provided.*

Significant changes restructuring the Policy were made which eliminate potentially confusing or contradicting passages. Further communications with the Office of Cybersecurity and the Policy Analysis Team is encouraged to resolve issues that are found to be confusing.

6. Classification of data seems mostly reasonable, though policies like this always call into question the interpretation with specific cases. Implicit in the implementation document is a centralized/top down approach which raises the concern about who determines which data needs transitioning to more sensitive/secure handling. The ultimate worry here is the cost/time/resources it might take departments to meet whatever standards get set, and whether or not this would hamper the flexibility and speed with which researchers are currently able to achieve their own IT solutions.

The Office of Cybersecurity is sensitive to this issue. Data handled within each system should be evaluated and the data classification agreed to as noted in the comment to Item #1 above. As research progresses and data is re-evaluated at a higher or lower classification a review should be conducted to determine what, if any, changes need to be made to the assigned security controls. In all cases, the security controls should be appropriate to the data in order to manage risk properly.

Remaining Issues from 2017 Feedback and not sufficiently addressed

1. More information about how the risk level will be certified. What happens if a researcher or funding agency disagrees with the risk level assigned by Cybersecurity?

Explanation was added in the background section of the Implementation Plan. Risk ratings are driven by the Risk Assessment Tool which assigns values to threats, vulnerabilities, and likelihood of exploitation to determine risk. A copy of the Risk Assessment Tool workbook can be made available to those who want to dig deeper. Any disagreements should be resolved through collaboration and mitigation activity during Step 4.

2. What are the functions and the training process for the Risk Executive role?

Item h. added to the Risk Executive role discussion in the RMF Step 5 description in the Implementation Plan (section starts on Page 3). The Chief Information Security Officer will provide this training on an individual or group basis.

3. There is no more information about internal threats included in either of these documents.

Language defining internal and external threat were added to the Background section of the Policy and a more thorough discussion of internal and external threat was added to the RMF description in Appendix A to the Implementation Plan.

4. How are high/moderate/low risk systems determined and by whom?

Discussion added to the Step 1 and Step 2 descriptions in Appendix A of the Implementation Plan. System categorization is made in Step 1 of the RMF and includes a collaborative and data driven decision process jointly arrived at by the System Owner and the Risk Analyst.

5. How will these documents (both the policy and the implementation plan) be regularly updated, approved, and endorsed?

This comment is addressed in the Policy Analysis Team narrative inserted into the Implementation Plan.

Policy Document / Policy Section

1. The policy is currently written as a bunch of statements but should be written to be consistent with the way other campus policies are written.

Significant editing was accomplished to reduce the confusion.

2. There's still no wording about an existing contract or federal sponsoring agency that has approved a researcher for working with sensitive or restricted data – do they still need to go through the RMF? If all data use agreements for sensitive or restricted data need to be reviewed by the Office of Cybersecurity this will undoubtedly generate delays in accessing the data for what is an already time-consuming process (IRB/RSP approval).

Statement added to address that use of data sets owned by others should be covered in data usage agreements. If the data set is applied to a new or different information system, that system should enter the RMF process at the earliest opportunity. If the data set is being incorporated into an information system with an existing RMF package and approval, that package would have to be modified and reassessed (The Office of Cybersecurity will develop a modified workflow for this special situation).

3. Is the term “university assets” defined anywhere? It would be beneficial if this were commonly understood, either by a more clear definition or through a glossary in the documents.

Information technology is defined in Regent Policy Document 25-3: Acceptable Use of Information Technology Resources as:
“UW System IT resources include all electronic equipment, facilities, technologies, and data used for information processing, transfer, storage, display, printing, and communications by the UW System and/or any UW institution. These include, but are not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, modems, email, networks, telephones, voicemail, facsimile transmissions, video, multi-function printing devices, mobile computer devices, data, multimedia and instructional materials. This definition also includes services that are owned, leased, operated, provided by, or otherwise connected to UW System resources, such as cloud computing or any other connected/hosted service provided.” This policy is available at https://www.wisconsin.edu/regents/policies/acceptable-use-of-information-technology-resources/
Similar descriptions are written in to *UW System Administration Policy 1010: Information Technology Acquisitions Approval* and in UW-Madison IT Policies

An appendix was added to the Implementation Plan and a section of the Office of Cybersecurity web pages will be dedicated to maintaining a glossary of terms used in the industry and by the office.

4. It reads that “Any IT governance group or the Office of Cybersecurity may initiate a revision” which implies that no group or office is responsible for regular reviews and updates.

This comment is addressed in the Policy Analysis Team narrative inserted into the Implementation Plan.

Policy Document / Principles Section

1. Policy/Principles refers to High/Medium/Low risk systems while the Implementation Plan refers to Restricted/Sensitive/Internal/Public data classifications – are we to assume the translation between the two policy documents regarding risk level? How will new and existing high risk systems be identified for review in the Implementation timeline? Through self-reporting of restricted and sensitive data or some campus-wide restricted data discovery project (NOTE: This was tried in 2015-16 (??) by narrowly focusing on SSNs). This should be elaborated on in the Risk Registration section of the Implementation plan.

Aligned discussions to describe as best we can. In the Implementation Plan we will have to be flexible as we learn more of the nuances and are able to publish control sets for the different

classifications and nuanced categories of data (i.e., TCGA databases, HITECH configurations, CUI variants that arise as each Federal Department evolves their guidance, etc.)

Policy Document / Enforcement Section

1. Failure to comply with what, specifically?

This section was expanded to clearly identify what failures would invoke the actions listed.

2. It reads that "UW-Madison employees may be subject to disciplinary action up to and including termination of employment." Does this included tenured faculty layoffs?

The statement is common to many policies with the action intended to follow University HR policy. Layoff of faculty is not the intent nor envisioned.

Implementation Document / Implementation

1. Does this only apply to systems? Do we have a risk management framework not only for data and systems, but also for people?
2. Figure 1 in Appendix A does not make sense. The RMF doesn't seem to address all aspects shown in the figure.
3. The background section in Appendix A of the Implementation Plan would be better suited for the background section of the Policy/Principles Plan. It defines risk, describes threats and various attack vectors, and forms a basis for protecting privacy and academic freedom. There is still no wording about where our systems are most vulnerable. This section does a good job of describing what the university is up against and shouldn't be tucked away in an appendix.

All three of these comments are great for additional dialogue.

The human element of risk is included in the NIST Security Controls. There is no separate RMF for people. Added explanation that the figure is an example of defining the system security boundary as shown in the footnote reference from the University of Florida. The CISO is happy to discuss further with the person who made the comment.

The policy and implementation plan is not an appropriate place to level of aggregate the types of vulnerabilities we encounter. The System Security Plan should state those vulnerabilities that may be common to that individual system.

Implementation Document / Implementation / Data Classifications

1. Suggestion to alter the last bullet point in "Restricted" to read "UW-Madison is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed *or disclosed*." Suggestion made because "disclosure" has a very specific HIPAA meaning which would be helpful in this context.

Change made.

2. Terminology is inconsistent between the Policy and the Implementation plan – how is "high risk" in the Policy different from "significant risk" in the Implementation plan?

Passages revised to reduce or remove ambiguity.

3. The meaning of "some risk" for internal data is vague and confusing. It is also now part of the defined risk levels (critical/high/medium/low/no risk).

The word "some" was removed and the risk table improved to better define the concept.

4. The category definitions and criteria should be reviewed and updated periodically. The causes of significant levels of risk may change over the years.

Agreed. The Office of Cybersecurity and the Policy Analysis Team will keep watch on this.

5. Classification criteria for "Internal Data" are unclear and potentially dangerous. Some at-risk data can be categorized as Internal (by not being classified explicitly) and won't receive risk management until 2021 based on the timeline.

Disagree. System Owners are free to address information systems with Internal Data near term. Setting the policy can and should drive improvements now. The focus of the policy and program is to address the issue as we move forward but will not be completed in the short term.

Implementation Document / Implementation / Timeline

1. Time required for classifying all institutional data is not included in the timeline. Is it already completed?

Data classification is a function of the Data Stewardship Council and is an ongoing task.

Implementation Document / Implementation / Training

1. This section seems to be particularly underdeveloped.
2. This section probably needs to have its website updated and simplified.

Training for the RMF is under development with a target of mid-February 2018 for release. The Office of Cybersecurity will publish on their website when training is available for System Owners, technical staff, and IT Security teams. The CISO will provide direct training for Risk Executives.

Implementation Document / Assessing, Accepting and Monitoring Risk

1. Item A (RMF Step 4) currently reads as though it's a two-party negotiation (customer and Cybersecurity). Is this intended? What about cases where another expert would be

needed? Suggestion to append something like “and if needed, consultation with other experts on campus.”

Suggested text added.

2. Item A (RMF Step 4) -- The Office of Cybersecurity (Risk Analyst) must be part of the teaching process for the Risk Executive. If security controls were established in conjunction with OoC staff in order to reduce risk for the information system then they should be involved in describing the system to the Risk Executive.

The CISO will be the primary provider of Risk Executive instruction. Depending on the understanding gained by that executive, the Risk Analyst may be brought in to the discussion.

3. Item C (RMF Step 5) – Still questions about who should be the risk executive. There is still thinking that this should be the CISO, given the way other research compliance programs operate with one “institutional official” but distributed reviews/sign-offs.

The CISO’s role is to validate and properly certify the risk identified during the Step 4 Risk Assessment. The Risk Executive is defined in the revised draft with a list in Appendix B of the Implementation Plan showing the UDDS that should appoint an executive (Dean, Director, Chair, etc.) to function in that role.

4. Item C, 4a – Designation of a Risk Executive should be a joint effort between the Office of Cybersecurity (Risk Analyst) and managing staff of the information system. OoC will know what Risk Executives have been previously designated and therefore most familiar with the RMF. OoC is also in the best position to describe the role and the responsibilities of newly designated Risk Executives.

The answer to Item 3 above discussed designation of the Risk Executive. This comment appears to be related to understanding which Risk Executive will be selected as the signatory for the system being assessed. If that is the intent of the comment, the CISO agrees that should be part of the Planning and Step 1 discussions.

5. Item C, 4e -- What is the turnaround (ie “within X business days”) we can expect from the CISO to certify the assessed risk and provide any recommendations to reduce risk. The concern about appropriate resources and staffing within the Office of Cybersecurity is raised throughout both the Principles/Policy and Implementation documents. An attempt to address this is presented with a 5-year timeline to completely execute the RMF. Lead or response times should then be specified for each step in the RMF to ensure a proper and effective workflow.

The goal for the CISO to sign the package as soon as possible once the Step 4 Risk Assessment is presented for approval. To date, the CISO has averaged no more than two business days to certify the risk assessment. Once certified, the RMF package is made available in the UW Box

folder with communications occurring between the assigned Risk Analyst and the System Owner.

The Five Year timeline is made based on imperfect evidence – the total amount of systems is unknown but roughly estimated to be in the thousands. Additional resources have been requested and a chargeback option is being explored.

Implementation Document / References

1. References should be updated. For example, 32 CFR 2002 (CUI) goes to the Federal Register and not the actual CFR reference, which is where it should go.

All footnotes and references were updated with links correct as of January 15, 2018. The Federal Register reference was chosen as it had a more complete discussion of CUI than the CFR.

January 2017 Feedback on "UW-Madison Cybersecurity Risk Management Policy"

Background Section

1. It would be useful context to provide some statistics or evidence about the current levels and kinds of threats we face and where our systems have not rose to the challenge of protecting our information. Perhaps include various types of threats and threat actors.

Policy Area

1. The document is lacking a clear policy statement around "cybersecurity risk." The policy says that the process in the document must be followed to manage risk, but this should be the policy that says cybersecurity risk needs to be managed for all UW-Madison data. As written, it's asking to be inferred rather than directly stated.
2. It is unclear what the scope of "data" or "information" is within the document. This is a policy around managing risk of *all information systems* that *store or process data* used to carry out the missions of the university. That doesn't clearly articulate external data sets that may be researched, for example. Defined as is, the policy is too broad and vague. IT professionals feel as though they are already following
3. IT professionals feel as though they are already following many/all of the principles but the document doesn't describe (or refer to a document that describes) how to measure this and confirm they are.
4. The policy should discuss who has jurisdiction over the various parts of the technical infrastructure. For example, who has jurisdiction over the campus network, who has jurisdiction over servers that access the campus network, and who has jurisdiction over the software running on those servers? (This is also pertinent to the "Risk Executive Concept" section).

5. The policy should discuss satisfaction of terms and how an acceptable risk level will be certified. If a contract or federal sponsoring agency provides their conditions of satisfaction, and a researcher believes they are satisfying those conditions but the Office of Cybersecurity does not, which entity prevails? The policy discusses "failure to comply," but not within a specific timeframe or what happens with systems that were once in compliance and fell out of compliance.
6. There is a need to distinguish between levels of security, data security paradigms (PCI, HIPAA, PHI, etc.)
7. Specific to "Principles" #4, it would be good to have clarification around due process (can monitoring start any time on anyone, or is there a cause that's needed?). This section, and its implications are not clear.
8. Specific to "Principles" #5a, it would be safest to define this a bit more so that it wouldn't be abused. What is the definition of "temporary" in terms of threat levels and timeframes?
9. Specific to "Policy" #1, it would be helpful to describe (or refer to a document that describes) exactly how risk is determined. The remainder of the process would seem straightforward with a strong definition of how risk is determined.

Risk Executive Concept

1. Roles of the risk executive need to be very clear, and should be written into the policy.
2. The policy should discuss how jurisdiction over the various parts of the technical infrastructure is determined. For example, who has jurisdiction over the campus network, who has jurisdiction over servers that access the campus network, and who has jurisdiction over the software running on those servers? This may be three different risk executives. What is the best way to work through inheritance, and chains of risk executives?
3. The document should describe the role of the Office of Cybersecurity with respect to Risk Executives. What sort of training and compliance is necessary to be a risk executive, and how will the Office of Cybersecurity facilitate and validate this?
4. It should be understood that Data Use Agreements are with the university, not individuals. What will be the expectation of risk executives who are speaking for/on behalf of the university?

Process

1. The presented document assumes an outside attack or outside threat actor and doesn't speak to internal threats, or threats from groups who have some sort of access to the campus network.
2. The document doesn't speak to how to onboard data and systems already within our ecosystem in order to be compliant with the policy – only that the process will be phased in, with high risk systems first. How are "high/moderate/low risk systems" determined and by whom? Is there a target timeframe for campus-wide compliance with the policy? Once this is determined, the process seems straightforward.

3. There is a sense that the document is trying to do too many things in one fell swoop. Perhaps think about breaking out pieces into separate documents. This doesn't seem to be something that can be operationalized as written. Some policies, particularly where HIPAA compliance is involved, can be referenced.

Resources

1. Recognizing that cybersecurity is a changing landscape, how will the document be updated and future proofed?
2. Recognition that Office of Cybersecurity does not have enough staff to adequately meet the aspirations of this policy. The level of resources within Cybersecurity currently cannot not match the needs and demands of the campus even without enacting this policy. What is the best way to adequately make resources available? What additional resources are needed?
3. Approach currently seems to be one-off for each information system. Are there ways to create some economies of scale with like systems?