Higher Education Regulated Research Workshop Series*: A Collective Perspective

July 19, 2021

Erik Deumens¹, Will Drake², Carolyn Ellis³, Cal Frye⁴, Jay Gallman⁵, Henry Glaspie⁶, Kathy Riley⁷, Anurag Shankar², Kyle Smith⁸, Veronica “Ronni” Wilkinson⁹

* Funded by National Science Foundation (NSF) grant #1840043, “Supporting Controlled Unclassified Information with a Campus Awareness and Risk Management Framework”

¹ University of Florida
² Indiana University
³ Purdue University
⁴ Case Western Reserve University
⁵ Duke University
⁶ University of Central Florida
⁷ Clemson University
⁸ Georgia Institute of Technology
⁹ University of South Carolina
Executive Summary

After an eight month effort concluding in June of 2021, research institutions from across the United States gathered in six facilitated workshop sessions to determine if coming together as a community could improve the support of individual programs to secure regulated data in research involving the Department of Defense or health sciences. 155 participants from 84 higher education institutions attended one or more of the sessions. Participants ranged from research computing directors, information security officers, compliance professionals, research administration officers, and personnel that support and train researchers.

Six main pillars of a well managed cybersecurity compliance program for regulated research were identified. Each of the pillars is presented as a chapter in this document with details, peer practices, considerations, and challenges to bring back to the institution. The first pillar describes Ownership and Roles. Institutions that invest in regulated research must have a program champion at the proper levels of influence and support. The second pillar covers Financials and Cost as meeting compliance requirements has a cost including certification, personnel, resources, training, infrastructure, and operations that maintain a framework of compliance. Compliance Training and Education forms the third pillar since materials need to be developed and delivered to a wide range of associated roles so that responsibilities are understood, and compliance requirements met. The fourth pillar explores Auditing the compliance environments. Cybersecurity compliance requires both auditing in the form of logging, log analysis, and having an auditor test if the institution is doing what it claims. Clarity of Controls, the fifth pillar, recognizes that security frameworks are written with flexibility of implementation in mind, but compliance is also evaluated at a pass or fail on implemented controls. The final pillar examines how proper Scoping provides both the boundary of compliance and strategies to contain it.

The workshop series also identified several recommendations for the community to further enhance institutional support for regulated research cybersecurity. Participants found that leveraging community expertise and experiences as a centralized repository is a critical component that could speed up the process to program growth. Another recommendation looked for a solution to address the lack of higher education representation when the regulations affecting it are being rolled out.

This report represents the collective perspective of those who participated in the workshop series and the efforts of volunteer authors who helped put it together. The primary aim of the document is to identify challenges, share best practices, and provide recommendations to the community on how to handle regulated research data on campus.
Introduction

Implementing a cybersecurity compliance program for regulated research data can be transformative. The challenge is to bring diverse research environments into alignment with shifting governmental regulations. To some extent, this is already familiar to those involved with Department of Defense (DOD) or health sciences research, to name two examples, but new entrants facing compliance for the first time have a difficult time determining even where to begin. Another conundrum is to build an ongoing program and strategies designed to handle regulated research data such as Controlled Unclassified Information (CUI) in a secure and compliant manner while simultaneously minimizing the impact on research activities. Finding who should have a place at the table and who should take ownership of the program is also a challenge as there are many parties and offices within a research organization with an interest in the program. Identifying who has responsibility for achieving compliance is particularly challenging in dispersed or shared Information Technology (IT) support models. Even in institutions with central IT, roles and responsibilities can be hard to identify since they may differ for different departments or divisions. A program to handle regulated research data is not itself an IT function either. Besides the IT group, it leans upon other stakeholders, for instance the offices of Counsel and Compliance, Privacy, the Office of Research, and of course the faculty and researchers. Nor is the data monolithic; it exists in many forms, not all of which are electronic. Secure practices must be identified for paper records and other lab operations as well, not just for computers. Training, another key aspect of securing regulated data, can be another obstacle since it is never a one size fits all solution. Successful training requires planning, in particular thinking about the most effective ways to develop, deliver and refresh educational materials. For each of these and countless other aspects of regulated research, institutions must determine what works best for their environment.

To the extent that strategies and practices to tackle management of regulated research data can be standardized on campus, we smooth the path of compliance, allow researchers to spend more time in the lab, and help out peers starting afresh. This served as the prime motivation for a NSF-sponsored Higher Education Regulated Research Workshop Series10, the progenitor of this document. The event, which comprised six virtual sessions between November 2020 and June 2021, was organized by Purdue University with co-organizers from Duke University, University of Florida, and Indiana University, with KnowInnovation providing workshop facilitation. Widespread interest in the topic was readily apparent from the numbers attending. By the end of the workshop, 155 participants from 84 Higher Ed institutions and one standards organization from all across the nation had attended one or more of the sessions. Participants ranged from research computing directors, information security officers, compliance professionals, research administration officers, and personnel that support and train researchers. The following table provides attendance details.

---

10 https://www.rcac.purdue.edu/cuiworkshop
<table>
<thead>
<tr>
<th>#</th>
<th>Session Topic</th>
<th>Workshop Date</th>
<th>Duration</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Challenges within the landscape</td>
<td>Nov. 4, 2020</td>
<td>2 hrs</td>
<td>57</td>
</tr>
<tr>
<td>2</td>
<td>Summary of groupings, topics for possible actions</td>
<td>Dec. 16, 2020</td>
<td>2 hrs</td>
<td>55</td>
</tr>
<tr>
<td>3</td>
<td>Speaker - View of CMMC peer practices</td>
<td>Jan. 27, 2021</td>
<td>2 hrs</td>
<td>44</td>
</tr>
<tr>
<td>4</td>
<td>Gaps, inputs &amp; outputs</td>
<td>Mar. 10, 2021</td>
<td>2.5 hrs</td>
<td>43</td>
</tr>
<tr>
<td>5</td>
<td>Pillar feedback &amp; draft</td>
<td>Apr. 21, 2021</td>
<td>2 hrs</td>
<td>37</td>
</tr>
<tr>
<td>6</td>
<td>Presenting back to the community</td>
<td>Jun. 2, 2021</td>
<td>2 hrs</td>
<td>96</td>
</tr>
</tbody>
</table>

Based on early group discussions, six main pillars of interest were identified: **Ownership and Roles, Financials and Cost, Training and Education, Auditing, Clarity on Controls**, and **Scoping**. Smaller groups then teased out the details of each pillar, including best practices, and challenges. Each of these six pillars is presented as a chapter in this document. Pillars also have an intrinsic order, from the general to the specific. There is some overlap, but in practice, how the pillars are connected becomes quickly clear. To use this document to build a campus program, institutions can start with the first pillar and clarify its goals and objectives specific to the institution, then proceed successively, adding details and filling in blanks, and answering questions raised by the preceding pillars.

This report represents the collective perspective of those who participated in the workshop series and the efforts of volunteer authors who helped put it together. Its primary aim is to identify challenges, share best practices, and provide recommendations to the community on strategies to handle regulated research data on campus. While the compliance regimes of most concern at the moment, namely Defense Federal Acquisition Regulation Supplement (DFARS) and Cybersecurity Maturity Model Certification (CMMC), are often used to guide discussions, the approaches recommended are common to all regulated research data.

This report has been made available by EDUCAUSE on its [Cybersecurity Resources page](https://library.educause.edu/resources/2021/7/higher-education-regulated-research-workshop-series-a-collective-perspective). The authors would like to thank EDUCAUSE for making it available to the broader higher education community.

---

11 The document uses the term “program” to describe the overall effort to tackle cybersecurity compliance for regulated research data undertaken at the institution. “Projects” refer to the individual grants or contracts.
14 [https://library.educause.edu/resources/2021/7/higher-education-regulated-research-workshop-series-a-collective-perspective](https://library.educause.edu/resources/2021/7/higher-education-regulated-research-workshop-series-a-collective-perspective)
1. Ownership and Roles

For a program to tackle regulated research data to be a success, buy-in, planning, and sponsorship at the highest levels is crucial. The program’s champion is not required to take formal ownership, but can still be influential in ensuring the program is comprehensive and continuing. That said, it is more than a mere cliche that successful programs will likely be characterized as those in which every group involved feels they are both invested in and have been given ownership of the process.

Identify Roles

Most institutions that participate in regulated research have established an Office of Research that provides administrative support for the research enterprise. This organization will commonly have a vice-president level resource and a department that oversees research compliance. The Office of Research is involved in the pre- and post-award processes and negotiating Data Use Agreements (DUAs), and holds the authority to reject grant applications, if the regulatory requirements cannot be reasonably met. Typically, it does not have a direct role in cybersecurity but collaborates with others on campus to ensure compliance. Note that one of the most important roles it can play is to negotiate compliance out.

The Information Security Office (ISO) can own the process, assist with policy, control interpretation, implementation, or auditing, but not all of these roles in combination. The ISO can also work with and provide help to security leads in units and departments that are executing projects.

Research Computing or central IT Services (ITS) holds support roles, matching the available technology to the requirements of individual compliance regimes. On some campuses, schools (such as science or engineering) may have their own ITS directly supporting compliance. In these cases, collaboration and coordination between them and the central program is even more critical.

Finance and other business offices are responsible for building charge models and handling any charge-back, and have an integral role in ensuring a program’s success.

In health and social sciences, the Institutional Review Board (IRB) can help align researchers with the compliance process. The IRB is concerned with protecting subject privacy as well as their well-being, and can help identify research projects working with regulated datasets. Their insight into the research process on a campus-wide scale can provide valuable input.

---

15 This and other functions described in this document may be within the scope of offices with a different name. For instance, the Office of Research may be called “Office of Sponsored Research”, “Office of Research Administration”, “Office of Research Innovation”, “Grants and Contracts”, or “Sponsored Research”. On smaller campuses, multiple functions may be consolidated within a single office.
For some compliance issues the Privacy Office and the Office of Licensing and Technology are also stakeholders.

Internal Audit, Compliance and Enterprise Risk Management (ERM) have places at the table, but may choose to not audit or assess the application of technology, preferring to leave that for the ISO. The Audit role needs to remain independent, and should be performed by a group not also involved in technology or program implementation, to limit resulting conflicts of interests. The ISO may have a place both in the development of policies as well as assisting Audit and/or ERM in evaluating the results, but it is preferable if these can be separated. It is important to clarify and document who is responsible for these duties.

Training and Education, which may be located under central IT, the ISO, or schools, is an important role that cannot be overlooked. Researchers come with varying degrees of experience in securing their data, and the field continues to evolve. They are also focused on sharing their results, while regulators seek to control access to sensitive data. These inclinations are often at odds. Researchers beginning their careers need help learning the processes of working with granting agencies, the technologies helpful in securing their data, and the regulations which apply to their research. Those with more experience will often find that practices once commonly accepted are no longer adequate to secure regulated research data without further training and education.

Recognize that implementation of a program will rely on IT personnel and researchers alike. In fact, it is more likely to be successful if researchers are represented from the start. It is also helpful to remember the institutional mission, that the ultimate success is when the researchers are competitive, can easily obtain grants and contracts, get to the science swiftly, and run their labs. Researchers also play a major role in the compliance success. The program’s goal should be to best help them to do their research securely.

Finally, the program is often required to be regularly examined and assessed by external parties. Existing Internal Audit resources can perform trial runs as the program is being developed, not just as practice before bringing in external auditors. See Chapter 4 (Auditing) for more details.

Determine Ownership

An effective program must be assigned ownership that is clear to all stakeholders. It is also essential to have administrative and academic leadership onboard for the program to be successful.

Institutions differ in organization, governance, and distribution of functions. IT can be centralized or highly distributed. Determining which of the many offices should take ownership of a cybersecurity compliance program may not be immediately clear. Indeed, it may be that one office will own the implementation of the program while passing it on to another once established. This is a process where a governance group representing the stakeholders is
advisable. It could for instance comprise senior leaders of the institution who can provide input to the institution’s annual budget cycle, policies, and strategic planning.

In asking who owns the process, consider who also owns the risk. Risk ownership is not always clearly articulated, so this is an important area to clarify.

Ownership is often closely aligned to the flow of funding. Ask if this model fits with local structures. It may be necessary to limit or delay the funding of a project until the questions of its security and compliance are fully answered. It is better that such action be taken internally than in response to either an external audit or an incident. Decide who is empowered to make these decisions for the organization.

Research focus is often in support of the mission statement or strategic plan of the institution. Ownership could potentially fall to the group charged with making decisions around those considerations.

On the compliance and services level, smaller working groups with appropriate expertise that can speak specifically to the needs of the researchers, teams, and research centers on an operational level are needed to develop, implement and maintain the program.

Assemble and Organize the Team

In assembling the team to develop and implement a program, multiple offices will be involved, each with differing roles to play. Some offices, such as Information Technology or Information Security, could fill multiple roles, and it is essential to identify areas where the roles and responsibilities blur or overlap.

It is easy to assume that as much of the compliance centers around IT controls, a decision to have ISO or ITS serve as the owners is a logical one. But it is better to consider an office more directly involved in research contractual obligations and operations who can rely in turn on these groups and Compliance as subject matter experts who will liaise with researchers to address specific needs.

It may be useful to implement a Research Compliance Review Board, similar in operation to the IRB, to organize and manage the process of helping researchers design and implement research projects in a secure and compliant manner. Building on this model guides the institution toward standardizing the process of security review. Secure research should become the default in project design.

The membership and responsibilities of the program team will reflect both the institution's organization and culture, as well as the maturity of the compliance program. Overall, the program team should include representatives who, (a) understand the compliance framework being considered, (b) can produce policies and practices meeting that framework, and (c) are charged with implementing the practices in the research facilities.
To implement the program, it is recommended that a program manager be assigned to oversee the process and ensure a productive and effective operation. Ideally, this manager would be independent of any of the stakeholder groups involved. Once the program is in operation, project management services can be helpful when creating new research lab environments or bringing existing ones into compliance.

Consider beginning with a smaller working group as the project launches, to outline the program and implementation. Add representatives of other departments as the project expands and evolves. The larger groups become the more difficult it is to schedule meetings with the frequency needed to move the project forward.

The project team or owners should determine what tasks should be managed centrally and which, if any, can be delegated or managed at the department or laboratory level. Again, the appropriate demarcation will be specific to the institution.

Be sure to document everything as the program develops. If one is not already in place, build a document repository of policies, procedures, and implementation notes. Choose an active manager for the document repository. Automate the process of maintaining and updating the documentation to the extent possible. The document repository could also contain researchers’ data security plans, training, and educational materials. Review the policies at a minimum of every two years, updating as necessary. The policies that have been documented are the policies the institution will be expected to follow. Make sure they are clear, concise, and compliant.

Give a thought to who trains the faculty and researchers in administration, compliance, and security. This should go beyond periodic “refresher courses” typically administered to all staff by the compliance or security office. If continuing education is available or required for some positions, review what is available to see if it can be tailored to help meet the needs of the environment.

Measure Success

To determine if the institution is on the right track for implementing an effective program, ask the following questions:

- Is senior leadership driving the process to success? Who is its champion?
- Does the institution have offices to handle all the roles described?
- Do the offices work together well enough to be successful?
- Is IT centralized, highly distributed, or a blend of both? If distributed, it will be more important to craft detailed policies and procedures for departmental IT professionals to implement in their areas.
• Is the Office of Research its own office, or combined with Compliance or Counsel? This office is a strong candidate to own the program, but only if they have authority and the capacity from the start.
• Has the institution defined the roles and responsibilities clearly enough so the process can drive itself?

Overall, ownership of the research compliance process should be transparent as stated earlier. Likewise, as tasks are identified and distributed, the assignees should accept ownership and be accountable for their responsibilities for the process to succeed.

Peer Practices

• A common observation is that the process needs someone who can stop projects, like those which cannot be successfully compliant.
• Several institutions are building self-assessment tools to assist investigators and their labs comply with the desired control set. These can range from simple system hardening checklists to outlines also addressing lab practices.
• It may be beneficial for the ISO to refrain from responding to questions and assessments on behalf of investigators and to remain in the assessment role. Others may require more assistance at first, but should not pass the responsibility to the ISO permanently. A separate cybersecurity and compliance service for researchers is being instituted on some campuses, for instance Indiana University’s SecureMyResearch (securemyresearch.iu.edu).
• Training staff earlier in the workflow to identify and route grants and contracts with compliance requirements to all parties that may play a role can reduce researcher confusion.
• An IT/ISO review of contracts and other agreements sufficiently early to negotiate changes or to reject a proposal is extremely useful.
• A tool to manage the workflow that is accessible to all parties is very helpful.
• Purdue developed the figure below to show the various roles and stakeholders involved with their CUI Program.
Challenges

Institutions often identify the ISO as the owner for any situation involving the protection of sensitive data or it is the default assumption. Additionally IT compartmentalization in highly distributed campus IT organizations can result in a reluctance to take ownership or responsibility. This is an opportunity for institutions to rethink old practices. Identify a more appropriate business unit or executive to serve as the executive owner.

In compliance, it is not uncommon for an institution to find itself in a reactive state of scrambling to address security requirements after the research is funded. To become a mature program, the institution must go from being a reactive environment to a proactive one. Successful programs will develop a compliance strategy that aligns with their research objectives. Making sure that all major stakeholders have roles and responsibilities creates the framework that moves the institution from reactive to the proactive state where a continuous compliance design helps to guide research efforts starting at the proposal stage. That said, there will always be cases where there is simply not enough time for front end prep.

Finally, as new compliance models are introduced there will be periods of uncertainty as aspects of the program are introduced, reevaluated, and refined. It is important that someone in the organization keeps abreast of new developments and advises the larger group about potential impacts.
2. Financials and Cost

Meeting compliance requirements has a cost. The federal government has acknowledged this in its estimates in cost for CMMC certification, but no accommodations have been made to account for personnel, resources, training, infrastructure, and operations to maintain a framework of compliance. Unfortunately, institutional budgets have been constrained with cost reductions taking priority in areas that do not have a direct correlation with student services or academic operations. The result of this is cost saving at the expense of compliance. However, this can change, for instance CMMC mandating a different set of administrative compliance and technical controls than NIST 800-171. Institutions that wish to continue their contractual relationships with the federal government in this area will need to find a way to fund the necessary resources to meet these requirements.

It is imperative that Chapter 1 (Ownership and Roles) has been sufficiently addressed prior to this chapter. Commonly at institutions, financials follow the ownership.

With each institution handling the indirect costs, funding, and subsidy differently, how the institution builds a financial model to fund and maintain these specialized compliance requirements depends on factors explored below.

Develop an Inventory of the Research Portfolio

One of the most important ways to get the program’s arms around the financial burden is to begin with a comprehensive research inventory process. Work with the Office of Research to complete a historical inventory of contracts/grant/projects, e.g., with the DFARS 7012 Clause and/or Export Control restrictions (noting if there is a fundamental research exception) since January 1, 2018. This is when the 7012 Clause took effect and gives a view of the amount of research in the organization over the past calendar years. The fundamental research exceptions may be required in the future to meet CMMC Level 1. Note the dollar value to the organization and group the projects by college, department, or research center. Using the information above, complete an inventory of active contracts/grants/projects. This shows the institution’s current exposure and liability for non-compliance (False Claims Act) and can possibly show return on investment. If possible, work with the Office of Research and the Export Control Office to complete an inventory of pending or potential awards and renewals/extension. This may give a view of what may be coming.

Inventory Considerations

- What is the organization’s annual revenue from projects requiring compliance? Is the institution spending more for compliance than it is receiving in contracts and grants? Is that a level of subsidy the institution is willing to provide to meet its research mission?
- Based on the inventory, define the scope of certification. For instance, what CMMC level should be achieved? Is the organization certifying a single enclave, multiple enclaves, or the entire institution? Should focus be placed on certification on an enclave that can be extended or shared across the organization?
● Evaluate the state of compliance in the colleges/departments/research centers identified. Does subject matter expertise reside in these areas?
● What are the cost drivers?
  ○ Personnel: who will create and operate the system/enclave, administer the compliance program?
  ○ Hardware: is a dedicated cluster or enclave being used?
  ○ Software/supporting applications: for compliance and operations.
  ○ External: use of cloud services and managed service providers.
● Does the organization have a distributed, centralized, or hybrid IT support infrastructure?

Right Size the Financial Implications by Institution

There certainly is no one-size-fits-all model for what an institution's financial impact will be for their program. By stepping through many of these considerations, it would become more apparent what may work best at an individual institution.

Developing a Cost Model

Selecting an initial cost model can be made easier by looking at various factors at the institution. For example:
● Is the environment highly centralized or distributed when it comes to IT services for research?
● Are there on-premise environments or cloud enclaves? Note: When running an on-premise environment, recognize it comes with physical controls such as door locks or cameras.
● Are subcontracts involved (example: third party vendors, business partners)?
● What are the expectations on cost recovery?
● What are the institutional goals for growth in this area of research?
● Are there mixed use labs and equipment/instruments (academic use and regulated research with citizenship restrictions in the same lab)? How are they handled? (See Chapter 5 (Scoping).) What are the financial implications?
● In building a financial model, consider what is needed and build in the costs.
● Take into consideration the need to cover the cost of licenses and the restrictions associated with them.
● See the Table on the next page for advantages and challenges of the various cost models.
<table>
<thead>
<tr>
<th>Category</th>
<th>Advantages</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Chargeback</td>
<td>+ Easy to set up</td>
<td>- Cost prohibitive to start-up projects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Duplicative expenses for items like licensing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Defunded projects become homeless</td>
</tr>
<tr>
<td>Overhead or Subsidized</td>
<td>+ Allows for easier access to researchers</td>
<td>- Who is funding this?</td>
</tr>
<tr>
<td></td>
<td>+ Defunded projects can remain secured</td>
<td>- What is the duration?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Decreases willingness to clean-up from trial or projects since the project isn’t affected</td>
</tr>
<tr>
<td>Hybrid (overhead &amp; direct charge back)</td>
<td>+ Policies can encourage strategic growth</td>
<td>- Who is funding this long-term?</td>
</tr>
</tbody>
</table>

After determining the best structure for the cost model, it is important to know where others have seen surprise costs. One of the risk-based expenses that should be considered is the needs that the program introduces on the incident response plan. The financial impact of a breach could be catastrophic if not accommodated by the institution right-sizing its incident responses. While evaluating if contracts are right-sized, licensing requirements could add to the overall cost. Vendors such as Microsoft may have significantly different costs based on the security requirements. For instance, licensing needs for the enterprise may differ from the compliance driven requirements with CUI. Licensing expenditures could also increase based on contracts with fuzzy language around cloud infrastructure or from duplicative contracts in a decentralized organization. In this day of remote and hybrid employees, consider the impact on any additional infrastructure the institution may require such as dedicated VPNs or additional endpoints.

Other chapters of this document will introduce program expenses that may need to be addressed. Chapter 3 (Training and Education) will impact the cost model as it may introduce third-party contracts or internal resources typically allocated for the academic classroom education such as instructional designers. When evaluating the role-based training individual costs, consider rolling the training expenses to the program level. Chapter 4 (Auditing) is straightforward enough until issues are discovered. If gaps are discovered, remediation efforts would likely require additional funds. Consider contingency funds as the institution plans the program, as remediation may come with a higher level of urgency for compliance.

Explore the possibility of unconventional support for the regulated programs, which could help lower the start-up costs through leveraging existing resources. Recognize that the institution may already have resources or experience that could move the compliance needs forward. For example, could a research lab step into a subject matter expert role as the program grows? Pre-award is also an area that can help catch cybersecurity requirements that may result in unexpected costs downstream. By improving process and training, the institution may find less surprises at Post-award.
Peer Practices

Overhead/Subsidized: One of the most praised common peer practices was encouraging continuing resources from involved units from areas such as the Office of Research, Information Technology, or even directly impacted units such as the School of Engineering. This is done by making the case of the importance of these funds as critical to a compliant state.

Direct charge model: Multiple institutions attempted a fully-loaded direct charge model. They each developed rates (including staff time, hardware usage, licensing...) and attempted to charge that rate to relevant projects. This became quickly untenable because the rate was very difficult for the project budgets to absorb. Institutions also noted that this model is very challenging if the institution doesn’t have a strong handle on the projects as they are proposed and budgets are being first developed; projects will then make it to the place where they are awarded without adequate funding to support their cybersecurity compliance requirements.

Elevated indirect costs: One institution is exploring a different indirect cost rate for DOD contracts, which is allowable under federal contracts.

Challenges

Decentralized funding models have shown to be challenging to grow. One institution commented that each project was funding their own enclave, and this made sharing or start-up costs steep for new projects.

Projects will regularly exist in state between funding cycles. When a project is defunded, this does not change the security requirements on the generated CUI. Projects will often pursue follow-on funding, but, during a lapse in funding, the project cannot directly contribute to costs associated with maintaining compliance for existing CUI. Overhead models can move this project into “warm-storage” to keep access controlled while absorbing the costs.

During this process, there have been community-voiced concerns over the possibility that after an assessment has been performed, there is currently a risk that an expensive auditor might disagree that a risk-based implementation of a control is sufficient and meets the requirements, with no third party appeals process available. This possibility ups the ante on “being right” and makes clarity on the controls a highly desirable commodity. To address this, we must get a seat at the table or get access to the appropriate platform to voice this concern or affect change. It is recommended that we find an independent body to broker the conversation around this concern and advocate for the community by reaching out, e.g., to the CMMC Accreditation Body (AB), about establishing an appeals process based on risk. In the future we see a need for an evangelist to get ahead of the rules and regulations to voice our perspective proactively.
3. Training and Education

Compliance training materials need to be developed and delivered to faculty, research team members, IT support personnel, IT systems personnel, grant and contract managers, and executive leadership so that responsibilities are understood, and compliance requirements met. In addition to providing an overview of the compliance regime (e.g., Health Insurance Portability and Accountability Act (HIPAA)) or regulated data (e.g., CUI), these materials will also have function-specific components focused for each of the specific audiences mentioned above. These additional components help to train those groups on their roles and responsibilities in the bigger compliance picture. Some compliance requirements may extend to existing cybersecurity training offerings. The institution will need to review its training materials and compliance requirements on a regular basis to identify and address any changes or gaps.

Identify Roles and Responsibilities

Determining what training is needed, and identifying who needs it can be a complex undertaking. Using CUI as an example, the following are some considerations. Note that the exact responsibilities mentioned can be associated with other groups depending on how things are organized for each individual institution.

Office of Research and Related Offices

Training for this group must prepare them for the following: identifying compliance requirements in contract language, initiating the appropriate negotiation process, and notification of others regarding assessment requirements and incident reporting requirements.

Export Control

CUI research may also have Export Control requirements which may put them in the middle, coordinating between researchers and IT to make sure that technical control requirements are met. They will need a broad understanding of what CUI is, and what it may require. The requirements may include training prior to access, technology control plans, publication and nationality restrictions.

Departmental IT and ITS

Departmental IT must have awareness of the compliance requirements for research being conducted by those they support, and the impact of those requirements on their IT environment. They will need to be involved in project based assessments.

ITS will need awareness of the services that may be in scope for compliance requirements and in turn will need to help develop institutional policies, procedures and standards. Along with research computing, they may have responsibility for the compliance of enclave computing environments.
Gather and Organize Training Materials

Pulling together the appropriate materials for compliance training can be a time consuming effort and there is a cost involved. Most off-the-shelf commercial training offerings do not have content that lends itself to the specific requirements of compliance training. To reduce that burden, training information, expertise, and frameworks may be leveraged from the following resources:

- Information shared between Higher Education Institutions
- EDUCAUSE Library of information
  Website link: https://library.educause.edu
- National Archives and Records Administration (NARA) – CUI Registry
  Website link: https://www.archives.gov/cui
- Center for Development of Security Excellence (CDSE) – DOD CUI Program
  Website link: https://www.dodcui.mil/Home/Training/
- Cybersecurity Collaboration Center Webinars
  Website link: https://www.cybercollaborationcenter.org
- DOD Cyber Awareness Challenge with Insider Threat information
- DOD CDSE CUI training
  Website link: https://securityhub.usalearning.gov/index.html

Note, to effectively share information between higher education partners, an appropriate platform that can be maintained and curated is needed.

No two campuses have the same requirements for a training program, but here are some of the key considerations for gathering information:

- Partner with internal and external stakeholders. Campus partners could include Library Services, Office of Research, Research Compliance, ISO, Data Governance, ERM, and General Counsel. External resources are listed above.
- Refresh training material as policies, procedures, security controls, and responsibilities evolve.
- Evaluate effectiveness of training by conducting surveys or follow-up discussions.
- Determine how to develop basic guidelines for CUI markings and other requirements that apply to specific roles.
- Provide technical training to assist with audits/assessments, and with security control discussions using non-technical language.
• Provide tools to assist with assessments:
  o Brigham Young University (BYU)
    ▪ [https://rc.byu.edu/cmmctool](https://rc.byu.edu/cmmctool)
    ▪ [https://rc.byu.edu/171tool](https://rc.byu.edu/171tool)
  o University of Florida (UF)
    ▪ [https://training.it.ufl.edu/training/items/research-computing-consultant-program.html](https://training.it.ufl.edu/training/items/research-computing-consultant-program.html)
    ▪ [https://training.it.ufl.edu/training/items/introduction-to-research-computing-and-hiperqator.html](https://training.it.ufl.edu/training/items/introduction-to-research-computing-and-hiperqator.html)
    ▪ [https://training.it.ufl.edu/training/items/resvault-training.html](https://training.it.ufl.edu/training/items/resvault-training.html)

Deliver and Track Training

Deliver in-person and on-line training so that it is provided at the appropriate time and includes specific role-based information. Track training so that compliance artifacts can be generated. If the campus has group management capabilities, leverage them to help automate the training requirement and compliance tracking. Those same groups can then be used to make access conditional on a user having met the specific requirements for a research project.

As an example, here are some key considerations for meeting the training requirements for DFARS compliance.

Focused Training Objectives:
• Everyone involved with CUI: General awareness along with specific responsibilities.
• Research teams: System security and technology control requirements, incident response, how to use secure systems
• Contract Officers: How to identify contract clauses for CUI
• Grant Administrators: Overview of security requirements
• IT Support: NIST 800-171 compliance requirements, incident reporting
• Export Control/Research Compliance: NIST 800-171 overview, incident reporting
• Internal Audit: DFARS/NIST 800-171 requirements, audit resources

Delivery Opportunities:
• Leverage IRB training, new faculty orientation, sponsored program newsletters, information security awareness programs, department meetings, and campus publications.
• Consider in-person training, which can enhance the effectiveness beyond on-line training materials.
• Include CUI with Information Security Awareness and other compliance training.
• Consider augmenting annual training with just-in-time training. This could include short, online training segments about specific topics such as "what is CUI and how does it affect me", "what is CMMC", and specific research domains.
Peer Practices

- Use a learning management system (LMS) for on-line training. This can provide reports showing course enrollments and completions. An employee LMS can be leveraged for compliance, departmental and other training requirements.
- Establish banks of quiz questions for courses and require users obtain a passing score of at least 70%.
- Develop customized CUI Overview, Insider Threat, Export Control, and CUI safeguarding courses using information available on government websites.
- Engage a third-party subject matter expert to assist with course development.
- Require training be done before system access is granted to ensure completion of the training.
- Establish an annual requirement for on-line training courses.
- Offer semestery workshops targeting the university's research community. Include guest speakers where possible from federal partners such as Defense CounterIntelligence Security Agency (DCSA), Department of Homeland Security (DHS), and the Federal Bureau of Investigations (FBI).
- Include research compliance information in the University's Data Governance program.
- Require a Data Governance Process form (that includes applicable data flow diagram, network architecture, data exchange with non-University 3rd parties, terms & conditions) be completed.
- Use the DOD CDSE or other external training resources, and have individuals submit certificates to validate completion.

Challenges

Beyond the compliance requirements for research already on campus, it is important that researchers have an understanding of stipulations that will apply to new proposals. It can be helpful to have an online reference that anyone can consult. Maintain up to date records of those assets used in research with compliance requirements. This will help identify both the users and managers of these assets as groups needing appropriate training.

Most institutions will find it necessary to have platforms that can identify and track who requires training and who has completed training. Consider developing dashboards or reports that provide key metrics around compliance training, as it has a direct impact on institutional risk.

Alignment of all compliance requirements for training will help avoid confusion over training requirements for regulated research, export control, and conflict of interest. This is an ongoing effort, and is why those charged with training are identified as one of the roles in Chapter 1 (Ownership and Roles).

Resource limitations, be it funding or people, may prohibit the effective development and delivery of training. Maintain awareness with business and functional owners regarding their roles and responsibilities in this ongoing effort.
4. Auditing

In cybersecurity and compliance, the term auditing is used in two ways. The first is as a security control, referring typically to logging and log analysis. The second is when an auditor is there to test if the institution is doing what it claims. Cybersecurity compliance requires both. Mandated external audits are common and highly likely in compliance. They are already required for, e.g., FISMA\(^{16}\), FedRAMP\(^{17}\), and the upcoming CMMC even adds a certification component. Preparing for external audits requires not only collecting logs and information on the current state of controls, but also copious documentation in a format consumable by the auditor. Audits may also require penetration testing and numerous other artifacts to prove due diligence. Because of these complexities, implementing effective auditing takes careful planning and execution.

Determine Ownership

The first step in establishing an institutional auditing program is to develop an ownership and governance model for the auditing process itself. Some campuses have the Office of Research own the process, with the ISO and Compliance as its principal agents and liaisons. Internal Audit can also be part of the equation. Whatever structure is chosen, ownership and governance should be key first steps in auditing. Both will very likely depend on local circumstances and pre-existing structures and relationships.

An important governance issue to resolve early is to decide who makes remediation decisions for any gaps the audit identifies. Remediation may also require a budget, especially if substantial gaps are uncovered as mentioned in Chapter 2 (Financials and Cost).

Manage the Audit Process

Once auditing ownership and governance has been established, the next step is to develop and implement processes to make audits manageable and efficient. The task can be made easier from the get go by limiting the scope of the audit, for instance by deploying the minimum necessary technology, isolation via enclaves, or using technical means such as network segmentation (see Chapter 6 (Scoping)).

Auditing requires resources. Both auditors and the process of gathering the information and artifacts necessary for the audit come at a cost, making auditing an explicit line item in the budget ideally. Also, bear in mind that auditing costs are slated to grow in the future, especially as we face CMMC. While DOD promises CMMC certification to be a recoverable cost, pre-assessments, which would be highly desirable for this new compliance regime, are not.

---


When building dedicated enclaves, auditing is typically baked in as part of the process, but is often retro-fitted into existing systems and processes when they are leveraged for compliance. Building in auditing controls from the inception into all new research computing systems can save a lot of time later if and when they become subject to an audit.

A common refrain in compliance is, “There is no compliance without documentation”. To launch the documentation effort, develop a coherent, institutional document storage and management strategy. Implement a central document repository, establish proper access management, and make it available to the right stakeholders on campus such as the ISO, Compliance, Internal Audit, and to those submitting auditing information. An obvious, key contribution to the repository is a document describing the institutional auditing process itself. Auditing burden can be lightened further by developing (or borrowing from peers) standardized templates, e.g., to collect auditing information. (A good example is the Higher Education Vendor Assessment Tool or HECVAT\textsuperscript{18} questionnaire for third party assessments.) Be aware that documentation alone is not sufficient; auditors often also use the “examine, test, and interview” approach where they ask for information and artifacts not present in the document repository. Keeping documents current is another key activity, requiring all documentation to be reviewed and updated regularly. Use the audits themselves as an opportunity to review, reorganize, and update documentation.

Make external audits quick and easy for auditors. It pays dividends because (a) auditors often charge by the hour; (b) good organization attests to the program’s maturity, and (c) making life easy for auditors makes them favorably inclined. Storing documents in a single place certainly helps in this regard but it is also important to ensure the documents are well organized and easy to access. Also, use specific control framework audit guidance (e.g., NIST SP 800-171A) to format reports and data as auditors often use those documents to perform their audits. Group related audits together, for example by compliance regime.

A common problem when auditing for compliance is a lack of clarity on the part of various campus stakeholders about the exact steps needed to complete their part of the auditing process. Address this by creating checklists for the various stakeholders that describe precisely what they need to know. For instance, the checklist for system administrators should specify what events they need to log, log retention time, log analysis requirements, reports they need to create for the audit, and where to submit them.

An excellent way to prepare for an audit is to have a mock audit. There are a few, different ways to do this. One is to leverage Internal Audit. This makes efficient use of a pre-existing resource and establishes and/or strengthens the relationship with Internal Audit. (Not too many seek out Internal Audit voluntarily!) The second is to ask peers who have been through the same or a similar audit. They may not have the time to do a detailed audit, but may still be able to review the preparations and provide help. Also, REN-ISAC can perform peer assessments for a number of compliance regimes including DFARS and HIPAA (for a fee).

\textsuperscript{18} https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit
With the government’s focus shifting away from point in time (annual) audits toward continuous monitoring/assessment, it is wise to make that shift now. Review the FedRAMP Program Management Office-provided continuous monitoring guide and template for guidance.

Gather and Organize Evidence

Collecting information to prove due diligence takes time and effort but there are a number of strategies that can help. First and foremost is automation. It is key to reducing duplication and effort. Invest in developing scripts or borrowing them from peers and vendors and use them to collect audit information for standard IT components such as the operating systems, commonly used software, etc.

Another approach to gathering information, or to learn about what information to gather, is to seek help from someone who does audits routinely, for instance Internal Audit. Their questionnaires may not be the same, and they may not ask for all the artifacts an external auditor might, but they may be able to provide sufficient information to get things going.

When creating System Security Plans to document controls, do not only describe where each control is applied but also document how it is audited. This will help the auditor and prove valuable in training new staff members. To make navigation more efficient, create an index with links that points to the documentation, including policies, standards, processes, and procedures created for each requirement. Also, each paragraph in those documents should identify the requirement for which it was written.

If the system being audited is managed by a researcher, or if the researcher is responsible for a set of controls on a centrally managed system, help them create or contribute to a System Security Plan and add it to the document repository.

Leverage and Empower the Community

Mock assessments by peers with compliance programs (such as DFARS) have already been mentioned as a potential audit preparation tool. If a peer does help out in this way, share this experience with the community. Also, share or ask peers to share their audit experiences, including audits by Internal Audit or a third-party assessor. This type of information is extremely valuable for others in the community, especially those facing compliance/auditing for the first time.

Use community forums such as the Slack HigherEdCUI channel, the RSOC-CSR mailing list, EDUCAUSE HEISC 800-171 Community Group mailing list, and Research and Education

---

20 https://www.fedramp.gov/assets/resources/templates/FedRAMP-Continuous-Monitoring-Template.xlsx
21 https://bit.ly/3xmUx1a
22 Email cburrows@ucsd.edu with a request.
23 https://www.educause.edu/community/heisc-800-171-community-group
Networking Information Sharing and Analysis Center (REN-ISAC) CUI mailing list. Use these resources to share information and learn from others. Attend the EDUCAUSE Cybersecurity and Privacy Professionals Conference where cybersecurity compliance and research facilitation are increasingly popular topics. The NSF Cybersecurity Summit organized by Trusted CI is another event where compliance tutorials are standard fare.

Share any templates created to help collect evidence or document controls, for instance questionnaires or System Security Plans. Also, if they are obtained from peers, encourage them to share directly with the community.

When CMMC certification audits begin, share lessons learned if the institution undergoes certification or a pre-assessment. Input on certification from multiple campuses will also help the community hold C3PAOs to a single standard. Also, DOD is developing automated mechanisms for continuous monitoring for other areas which they may also require for CMMC. We need to use the power of community to keep the process sane if and when they decide to subject the rest of the Defense Industrial Base (DIB).

Peer Practices

- **Strategy**
  - A number of campuses are building cloud enclaves, e.g., in Amazon Web Services (AWS) GovCloud/AWS, or Microsoft Azure GCC High, to limit the scope of the audit.

- **Process**
  - Several campuses are interviewing researchers/IT professionals to discover processes and procedures, documentation.
  - Nearly everyone is creating System Security Plans (SSPs), system inventories and personnel lists.
  - Many are reviewing NIST 800-171 requirements, e.g., FIPS 140-2 encryption, and strategizing on how to comply, especially those new to DFARS.
  - One institution is auditing the current state of controls (implemented, partially implemented, incorrectly implemented, not implemented) using NIST 800-53, documenting the controls into an SSP, assessing risk from improper, partial, or unimplemented controls, and crafting a risk response to each. Compliance with specific regulations (DFARS, HIPAA) is then addressed by mapping them to the more comprehensive NIST 800-53 standard.

- **Tools**
  - A few campuses are using PowerShell and other scripts to audit technical controls.

---

24 Email [info@ren-isac.net](mailto:info@ren-isac.net).
25 [https://trustedci.org](https://trustedci.org)
○ One institution is using a Security Information and Event Management (SIEM) tool to check against specific control sets and vulnerability scanning to cover the rest.
○ Some are Implementing NIST 800-171 through Windows GPOs, firewall rules, configuration management (SCCM), log management and analysis.

Challenges

One of the biggest challenges in auditing is a lack of a common audit process across the institution. Units and departments are typically auditing their areas and systems in their own ways and some have little or no auditing to speak of. Imposing a uniform standard is also difficult since very few exist\(^26\) and there are no easy-to-use, standardized tools to audit controls, nor are there checklists or best practices. Most campuses are using homegrown spreadsheets or forging one-off tools.

Another problem with auditing is the “squishiness” of controls. There are different interpretations of what a control might mean or how it should be implemented. It is very difficult to audit controls without knowing precisely what to audit. Picking the wrong interpretation is problematic as it may lead to audit findings and misdirected effort. Chapter 5 (Clarity on Controls) addresses this issue in more detail.

Perhaps the most challenging to audit are legacy technologies, particularly lab instruments with obsolete operating systems and software. Most were not designed with security in mind, and may not even provide sufficient information or logs to make proper auditing possible.

\(^{26}\) A new NIST effort called OSCAL is working on one: https://pages.nist.gov/OSCAL/
5. Clarity on Controls

Security frameworks are written with flexibility of implementation in mind. While rigid controls that specify particular solutions provide 100 percent clarity, it is impractical to think such solutions would work in every environment. The angst over clarity on controls distills down to doubt that a particular implementation of a control will pass muster during an external audit, leading to possibly expensive remediation and the need for another audit. Having no recourse to dispute a finding without incurring possibly significant expenses of hiring another auditor for a second opinion leaves people with a sense of urgency to “get it right” the first time.

Understand the Requirements

The first step in tackling compliance regimes and in providing assurances over them is to understand the requirements. This can be difficult since the language they use is often nebulous, with little guidance from the sponsoring agency and subject to significant interpretation. Even where there is clarity, interpreting controls, namely deriving tangibles (e.g., actions and technologies), especially as they apply to specific research grants and contracts, is highly non-trivial. Knowing requirements is critical as organizations have a need to manage risk and address compliance in the most efficient and effective way possible.

Clarity on What?

There are many aspects of the implementation of security controls, e.g. those meant to protect CUI, which can leave organizations wallowing in a sea of ambivalence or maybe just skimming the surface. Specific security controls may be written very generally either to provide flexibility in implementation or because they are only a part of a greater whole and it is only through a holistic, layered approach that the targeted risk can be neutralized or mitigated. When taken out of the context of a complete security program, security controls in isolation begin to feel less clear and lose the resolution that integration with other controls provides in their implementation.

The certification process introduced by the CMMC program also leaves many organizations feeling unsure about the requirements around reporting. In an ideal world, reporting for each control would have been designed and implemented while the solution for that control was implemented. Many organizations were focused on implementing the security control as part of a NIST 800-171 implementation and were not planning on how to report or prove that each control has been fully implemented, is fully functional, and is working as intended. Organizations who had a mature audit program to draw on likely were thinking about reporting in the initial stages. Other organizations may be faced with retrofitting reporting into the current implementations in the hopes that the data they can provide will be sufficient to get them through the certification process.

The last area of concern in terms of clarity explored is that of uncertainty introduced by having to work within or implement multiple frameworks. In an ideal world, most organizations would choose one security framework to implement and then vary their reports to support how their
implementation supports other frameworks. In the real world, there are typically some controls that do not overlap, or its documentation differs significantly from the compliance regime at hand, causing organizations to have to track multiple frameworks, complicated crosswalks, and track and implement subsets of controls that were not covered in their chosen implementation.

Adopt a Risk-based, Holistic Approach

Rather than seeking perfect clarity on individual controls, adopt a risk-based, holistic approach to implementing a security program. Interpreting controls is not as simple as it sounds. Controls, as written, are too broad to be easily equatable to actual implementation. The same control may be implemented differently depending on the context of the project, environment, or architecture. The correct way to interpret a control is in the context of risk. The question to ask is, “In what form should the control be implemented so it addresses the risk of not having the control in place while keeping the research mission front and center?” And to answer this question, one needs an understanding of what risks, threats and vulnerabilities a control is attempting to mitigate, and how likely are those risks in the environment in question with the other controls already in place.

For example: Carnegie Mellon University has been through a DOD audit (NIST 800-171) with a "perfect" score. Administrative controls were acceptable to DOD and satisfied the requirements. The DOD accepted a risk based assessment based on their interpretation of the controls. For example, FIPS 140-2 validated cryptography is only required if cryptography is the only thing protecting that data, but at the other extreme, one most likely does not need a data center with guards and guns protecting it. Using a holistic approach when accepting risk on a particular control is asking the question, “When you fit this in with other controls, in context, is this control strong enough?”

Collaborate

There is strength in collaboration and other points of view are a panacea to controls that seem vague or opaque. Collaborate with others to define standardized and assured control interpretations. This includes working with experts or authorities within the institution, such as general counsel, contract officers, etc. as well as reaching outside of one’s institution. Using community resources is a tried and true technique that all of Higher Ed is familiar with. Do not hesitate to hire consultants if lack of subject matter expertise is a concern and then share what was learned back to the community. Become a community resource.

Manage Compliance Efficiently

Finally, make every effort to manage compliance efficiently. Compliance regimes are complicated, expensive, and resource intensive. Consider combining different regimes into one security program (e.g., HIPAA and CUI) and adopt an “Assess Once, Report Many” approach. There is significant overlap in most frameworks which makes leveraging the crossover key to this approach. Ensuring that the security program addresses all unique controls under one
umbrella or System Security Plan means that one can assess compliance once and tailor reports to whichever framework one is examining, whether the reports are results of assessments, System Security Plans, or even a reporting framework of a particular standard or taxonomy.

Do not forget to consider the audience when striving for efficiency. Security controls can leave even the most seasoned security professional grasping after clarity and looking for guidance. Do not forget that the faculty and researchers will need help understanding the requirements even more so. Consider publishing checklists relevant to their environment based on local policies, implementations, and the frameworks. Having a clear list of what controls are already taken care of through existing institutional policies, procedures, and resources can save valuable research time and money. Providing a template for controls that the faculty will be responsible for implementing will help assure that controls are not missed by busy faculty.

Consider whether a centralized vs decentralized approach would drive efficiencies in implementation or inhibit them, making sure to consider local environments, funding, governance, scope, need, or other institution-specific resources or limitations. The first consideration should be deciding who is responsible for interpreting various controls in a centralized vs decentralized implementation and where governance lies. These decisions will impact how reporting works and what processes need to be in place during assessments.

Whether a centralized or decentralized approach is chosen, consider appointing or creating a group that helps those within the institution be compliant. This group should be involved in the community and should work alongside institutional authorities to define controls and compliant workflows. This group would then work with system owners and others, providing standardized controls, preventing siloed interpretations, and making it easier to align with institutional standards.

Peer Practices

Case Western Reserve University created a set of lab and host security checklists based on their published policies and tailored to the security level of the data handled by the host. The checklists are simple, but cover the majority of controls they want the researchers or their sysadmins to implement. The checklists were mostly based on a similar inventory/attestation set of documents, like the Cybersecurity Certification Process27 used at University of California, San Diego (UCSD), leveraging resources in the community.

Several institutions are building self-assessment tools to ensure investigators and their labs comply with the desired control set. These can range from simple system hardening checklists to outlines also addressing lab practices.

27 https://blink.ucsd.edu/technology/security/certification/certification-process.html#1.-Collect-Project-Information
Resources:
- Free Guides, Templates and resources to get started in CMMC from NIST 800-171
  https://www.complianceforge.com/cmmc-certification-dfars-252-204-7021/
- Self-Assessment Handbook For Assessing NIST SP 800-171
- CMMC Level 3
- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- CMMC Appendices
  https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf

Challenges

There is a risk that after an assessment has been performed, that an auditor may disagree that a risk-based implementation of a control is sufficient and meets the requirements. At this time the appeals process is still unclear. This possibility ups the ante on “being right” and makes clarity on the controls a highly desirable commodity (see also Chapter 4 (Auditing)).
6. Scoping

Scoping is a key component of any compliance program, as it provides the boundary of compliance. Once the scope is set, the audience for policies, the activities of enforcing the controls, and the impact of compliance on the research activities becomes clearer. However, while the scope can change in size, aspects of scope such as the security boundary are harder to change once the program is running.

All decisions on scoping should balance cost, risk, and institutional mission. To inform such decisions, scoping involves analysis of systems, controls, and business processes to ensure proper calibration of the lens of compliance. Such analysis will reveal connections between systems, controls, and business processes. Once those connections are found, it is important to correctly decide the components that need to be inside the security boundary, and those that need to be outside of the security boundary. The security boundary should quantify where systems and resources store, process, and transmit data that is under the contractual responsibility and accountability of the institution.

Address Stakeholder Requirements

The initial actions to scope the environment and personnel for regulatory requirements are to address needs of the stakeholders involved. An understanding of the stakeholder requirements will inform the scoping expectations for the regulations with which the institution needs to comply. Researchers will be the primary stakeholder in many cases, as they are the ones focusing on the storing, processing, and transmission of regulated data. The additional stakeholders will be those that operate in support of the researchers and those that operate in support of the institutional mission [Figure 1]. Defining scope in terms of need-to-know and data integrity, IT structure, admin structure and policy may create boundaries.

To ensure that all the stakeholders have an equal understanding, unified language around the regulated or non-regulated systems is important. Additionally, compliance and security efforts need to be incorporated into the pre-award process so that funding controllers are aware of regulatory requirement changes. As the program evolves, stakeholders’ requirements will evolve as well. The initial discussions should seek to compile a standardized set of questions to confirm researcher workflows to streamline the process, which can then be adjusted as requirements change. Involve stakeholders in discussions exploring if it is feasible for researchers to comply with the regulation at hand. Leadership may want to weigh in on whether the benefits outweigh the costs to the institution. Ask questions of leadership to confirm whether they are willing to invest in the Governance, Risk, and Compliance teams necessary to guide the community as well as to catalog risks found. Consider working with other institutions to see if they have similar approaches and aligning approaches to “future-proof” the questions list.
When stakeholder discussions have been completed and there is a list of requirements and questions to ask, the next step is to discuss approaches to match the requirements found. This can be broken into a few major steps:

1. To begin, sort the stakeholder requirements and the regulation requirements, and then perform a gap analysis to discover compliance concerns or institutional process holes.
2. Discuss with researchers the various regulations for which their projects require compliance, e.g., even above contracts that include the 7012 Clause. Based on researcher response, deduce if there are regulation commonalities that can be leveraged into a more robust solution that meets more of their needs at once.
3. Next, group together the researcher demands and the solutions at the institution to meet those requirements. The goal here is to look for common solutions that will meet an acceptable margin of demand. That margin should be selected by the institution, with a general guideline being 70% to 80% of researchers covered for a regulation, with the additional 20% to 30% to account for outlying concessions needed for unique equipment, for example.
4. Based on the responses in the previous steps, discuss the approach of an enclave where researchers can work on their projects based on the agreed upon stakeholder requirements and the regulations met by the implementation.

Confirm Secured Data Workflow and Data Boundaries

Now that the requirements are known, it is time to discuss the workflow and boundaries. When beginning to confirm the secured data workflow and data boundaries, it is critical to narrow the discussion to the context of Higher Education when considering scoping. The goal is to ensure the flow will meet culture and business processes while still making it possible for researchers to comply with the regulations at hand. Many regulations are written with an enterprise infrastructure in mind rather than an academic one with many different user types, and so culture change is a major aspect of the scoping discussion. There is a strong importance on keeping a keen mind on “scope creep” during these discussions. Should there be systems, personnel, or services found in the discovery that do not fit into the scope of the regulations in play, they should be removed from the discussion.

To begin mapping the workflows and boundaries, consider developing a responsibility assignment matrix (RACI) to notate each party responsible for each portion of the flow, and group those parties as applicable. This should include discussions of what is required from each party from an HR perspective. Then, confirm owners for each of those parties or groups, respectively, as well as owners for each portion of the workflow. Then, once the workflow is clear for where data is stored, processed, and transmitted within the boundary, the next step is to confirm ingress and egress of data to and from the workflow. This could become a template for requirements that can be presented to vendors in the future to ensure that their solutions meet the workflow, for example. Then finally, present all findings to leadership to discuss the workflow and potential accepted solutions to meet that workflow.
Once the workflow and parties involved have been accepted by leadership, the next step is to be sure the workflow is formatted in a way that is easily added to the researchers’ System Security Plan as applicable. This addition will help to define scope for the System Security Plan or Plans. As part of this step, consider discussion with leadership about implementation of a data classification structure accounting for available secure environments and/or workflows, as the addition of the workflow to the System Security Plan can help drive those classification discussions. This process is known as inheritance: one can build a System Security Plan by leveraging the System Security Plan of infrastructure that is used without the need to re-invent or rewrite the document. That will ensure that the total System Security Plan is always up-to-date as the people responsible for the leveraged system maintain their part of the system and its System Security Plan.

Confirm Third Party Involvement (Vendors and Contractors)

The final step in the process of scoping is to confirm third party solutions and services used to advance the Institution’s research initiatives. There should be a process to ensure that third-party vendors or contractors dealing in regulated data such as CUI have gone through a thorough risk assessment via HECVAT or some other security questionnaire. Be sure to detail any third party responsibilities that go beyond the standard requirement to comply, e.g., with NIST 800-171 controls, and be sure that the selected vendors either meet or exceed FedRAMP Moderate Authorization and can meet the reporting requirements of DFARS 7012 parts (c) – (g). Some of these conversations with vendors can take time and resources, so definitely work with vendors that have a proven track record and vendors that understand compliance requirements. Vendors with lesser knowledge about compliance requirements may be less equipped to protect the data to a sufficient level, and may not be willing to cover their responsibilities in a contract. Contracts with third party vendors need to detail their responsibilities in handling institutional data, and need to be clear on the expectations of protection and reporting based on the data that will be stored, processed, and transmitted via the solution or service in question. Be especially careful of trusting vendors too much and build processes to compartmentalize their influence.

Peer Practices

- Involve leadership as soon as possible, and discuss an institution-wide initiative since regulations are most always long-term commitments. If regulated research is to remain an institutional priority, it should be designated as a strategic priority. Therefore, be sure that the right leadership is involved to ensure that decisions are made to meet or exceed the requirements of the regulation.
- If action is required in the short-term with a regulation, consider a tiered approach to scoping, starting with a project-based, lab-based, or environment-based scope. Then, use a preliminary discovery form to gauge the equipment used in that boundary. This can help to gain acceptance of the process as a more comprehensive strategy is built. However, be sure that all parties have a clear understanding of their responsibilities with
each implementation. Researchers should have a clear understanding of their responsibilities to report any changes to their environment or personnel, for example.

- Consider using existing enclave architecture if there is a resource at the institution that meets or exceeds the requirements, e.g., of the 7012 Clause.
- Discussions with stakeholders may reveal that the scale requires resources like Azure and AWS. Be sure to have those conversations as early as reasonable to ensure they are considered as options, especially the federal compliance, level, and/or certification (e.g., HIPAA, FedRAMP Moderate, etc.) of the services. This can help with some of the heavy lift of compliance, especially by confirming protections by third party vendors via contracts.
- Consider bringing in those that can provide outside and impartial opinions like REN-ISAC to confirm if the solutions in place at the institution are meeting the spirit of the regulation, e.g., NIST 800-171 controls, as well as the DFARS 252.204-7019 and 7020 interim rules. This could also be used for the purposes of CMMC.
- Consider pairing functions in ways that will advance the compliance program. For example, ensuring that the Governance, Risk, and Compliance teams are frequently in contact with the primary executives of research will help to ensure the right people are talking about the same strategic direction. Also consider working closely with Research Compliance officials to get visibility as soon as possible to interpretations of controls, scoping expectations, and more to ensure that discussions internally are productive.
- Consider IT signoff as well as researcher signoff on security plans so that the parties closest to the data all understand their responsibilities, but be sure to run the document by the counsel to be sure it can operate in that capacity.

**Challenges**

There are various challenges purely due to the fact that many institutions do not operate like an enterprise. Many Contracting Officers and prime contractors themselves do not understand that a university is much more heterogeneous than many of the organizations they are used to working with. Much explanation may be required to contracting officers that certifying an entire institution at a particular level or "score" is an extremely difficult, if not impossible, endeavor. This challenge can be mitigated by involving leadership early in discussions and ensuring that cybersecurity compliance for DOD funded research is part of the strategic plan of the institution.

There can be difficulty in some situations with fiefdoms at institutions since many of them run more like a city than an enterprise. Having individual IT staff in the colleges owning their respective systems can create an aversion to central solutions, which affects scoping. Conversely, researchers may also have solutions they prefer, causing user acceptance to be a major challenge with scoping. To mitigate this challenge, it is once again important to have leadership involved in discussions at all points. To get some of the users to accept the process, there may need to be heavy discussions at all personnel levels on scoping in various contexts, whether talking about air-gapping old operating systems, scoping cloud as a resource rather than a system, or other potential mitigations. Using the NIST 800-171 Self-Assessment Handbook to ensure approaches are defensible can be an option, but remember that auditors
for regulations are operating from *their* interpretation, and not ours. Think of this as an advantage, however, as having an external audit can provide “teeth” to show end users that external entities have defined true requirements.

Contracts requiring compliance that depend on hardware or services that have not yet been purchased can pose another challenge. Situations like these should be discussed as part of process planning, and there should be business discussions concerning when there are not enough funds in the research award to handle these extra requirements. This can also affect scoping decisions, as well as whether projects should even be taken on. Notably, sometimes external storage is the preferred file transfer mechanism between services and user systems, which results in malware making its way onto the systems. This may not just be a funding decision, but also a policy discussion that must be in line with institutional strategy.

Some researchers may feel that they can accomplish their research objectives with personal equipment, and there should be significant discussions around whether this should be allowed to happen. However, it is best to caution that it is generally not possible or even appropriate to try and make a personally owned system NIST 800-171 compliant, since that would violate ‘least use’. This practice may also muddy institutional risk acceptance processes or cyber insurance coverage.

Finally, there may be challenges in scoping responsibility internally versus responsibility undertaken by third parties or vendors. Understanding the nature of services and responsibilities that are shared between organizations and their third parties is critical to understanding the scope of what we need to provide assurances over. Leveraging tools such as shared responsibilities matrices, especially within the cloud domain, is effective in helping organizations better define this. This can also help to see where the institution or its vendors may be taking on more or less responsibility than what would be reasonable. For example, the institution may not leverage the assurances that its business partners have already provided and flow those assurances down to researchers. If a vendor attests that they are FedRAMP Moderate Authorized and can carry out DFARS 7012 parts (c) – (g), and that’s written into the contract with that vendor, then that meets the clause provided the proper users are granted access to the data. Essentially, the contract with a vendor can inform the scope immensely via the contract.
Community Recommendations

Upon registering for the Workshop Series, participants were asked to respond to a number of survey questions. Below is the word cloud result from, “What do you see as the biggest value from bringing this community together?”

Higher Ed institutions excel at community collaboration and have historically capitalized on this strength. We see value in establishing a permanent virtual home for this community with resources around regulated research, security controls, and compliance. To help institutions with clarity concerns, we think a repository to publish standard community interpretations and solutions would be invaluable. We would also like to create a community database or repository of implementation and audit outcomes, including an examination or providing context on why some solutions did work or did not work.

We must get a seat at the table or get access to the appropriate platform to voice this concern or affect change. It is recommended that we find an independent body to broker the conversation around this concern and advocate for the community by reaching out to CMMC AB about establishing an appeals process based on risk. In the future we see a need for an evangelist to get ahead of the rules and regulations to voice our perspective proactively.

What’s Next

As a community it would help to hone the known peer practices into vetted best practices. This can happen as others try them in their unique institutions. Develop metrics that can be used to measure program maturity.

This document will serve as an input into newly funded NSF #2115087 Regulated Research Community of Practice (RRCoP) grant. RRCoP will serve as this central repository for templates, training materials, and best practices. RRCoP also will strategically partner with organizations that will advocate for our unique intersection of research compliance. We believe that the creation of RRCoP will have a tremendous impact on the national participation in regulated research programs.