DOI:10.1145/3704286

Erik Deumens and Carolyn Ellis

Security Compliance Requirements in Research

Cyberinfrastructure for research needs to meet growing lists of requirements.

SCIENTIFIC RESEARCH HAS traditionally been conducted in a culture of openness. However, increasingly in the last decade, various concerns have resulted in more regulations about keeping research data and processes secure from accidental corruption and loss and—more importantly—from theft. While the data is the primary asset of value that needs to be protected, various flavors of data are part of workflows that can be complex and require special infrastructure to support. Examples include raw data from measurement devices and sensors, intermediate data in the form of lab notes, computer software and simulation datasets, and final reports and publications. To keep data secure, laboratory spaces, instruments, computer systems, and data networks are in scope for protection.

IMAGE BY IURII MOTOV

While no system design can eliminate the possibility of unauthorized access, the risk of data theft can be managed and mitigated. This is done by formulating policies, procedures, and technical controls to safeguard the data and ensuring these safeguards are followed by everyone involved with the data. Federal and state governments and companies require in contractual agreements that these controls are followed. Recently, it has become clear that just requiring this is not sufficient. Institutions are required to prove their implementation and operation of safeguarding controls. We list a few examples of new and pending requirements, including the National Security Presidential Memorandum[a] NSPM-33 of Jan. 14, 2021 with the recently published[b] follow-on *Guidelines for Research Security Programs at Covered Institutions*. It requires institutions to define a comprehensive security plan for sponsored research. Most widely known is the Cybersecurity Maturity Model Certification 2.0 program that has been developed since 2020 and will soon be required for Department of Defense contracts and subcontracts as specified in the Defense Acquisition Rules Supplement (DFARS) as clarified in the rule[c] published on Oct. 15, 2024. On another side of research funding organizations, NIH announced[d] that DbGaP (genomics and phenotyping) data will need to be handled according to NIST 800-171 starting Jan. 25, 2025.

This short list of examples demonstrates that various agencies are not aligned in their requirements. Academic institutions have contracts with state and federal agencies and private companies—all of which are creating their

[a] See https://bit.ly/3Z2563q
[b] See https://bit.ly/3YNbpqb
[c] See https://bit.ly/4fIjNON
[d] See https://bit.ly/3ClETUC

own requirements. This puts a serious burden on institutions because it takes time to study the details of each set of requirements and then verify they are implemented at the institution. More often than not, requirements for different contracts are conflicting, putting an enormous burden on the contract and system administrators charged with implementing them.

Security and Compliance

Because these requirements are stated as requirements on managing data, it is natural to turn to the chief information officer (CIO) and the chief information security officer (CISO) to implement the required compliance program. However, the technical controls in these compliance frameworks are only a small part of the complete list of controls. Security and compliance are not the same thing. Security focuses on defending and protecting the data assets while compliance is the specific set of controls implemented to improve security. Systems that support operations carried out by humans and interact with other systems and organizations can never be 100% secure. As a result, a risk management approach must be taken to balance the mission of the organization and the cyberinfrastructure supporting that mission with security controls and budget constraints. Compliance frameworks specify an agreed-upon set of activities and practices that provide due diligence to manage risk to an acceptable level.

Compliance Is a Teamsport

As a result, implementing a compliance program involves many people and offices at an institution, as shown in Figure 1. The team involved in a compliance program does not live in one office by the very nature of compliance. It involves policymakers, procedure developers, contracting officers, legal counsel, information security as facilities security, computer system administrators, trainers, faculty, students, and staff.

To make a compliance program work, these offices and their staff need to establish an efficient working relationship with each other so that issues can be dealt with quickly when they occur. Traditionally, the researchers have been the ones who were expected to carry out the activities of safeguarding. Within the complex computing and shared communication infrastructure of today, the safeguarding controls are intertwined into multiple support teams and systems required to support the institution's entire research portfolio. The researchers, faculty and their students, and collaborators must do their part after taking appropriate training, but they should not have the full oversight to deal with overarching controls like continuous monitoring and reporting of systems and procedures. The researchers on their own cannot develop and deploy a compliance program for their lab in isolation: The institution must own the compliance program that incorporates individual labs.

While no system design can eliminate the possibility of unauthorized access, the risk of data theft can be managed and mitigated.

Resources and Community

Since 2021 with funding from NSF, the Regulated Research Community of Practice (RRCoP) has become the primary resource for those supporting regulated research.[e] RRCoP has grown to be a very useful place to go for all individuals involved in regulated research programs to learn from each other, share experiences through the monthly webinars, and build resources encoding vetted practices through workshops. RRCoP has participants from more than 300 institutions in all 50 U.S. states and several institutions from around the world. Monthly webinars typically have approximately 130 attendees.

Slack is used for quick communication and sharing of relevant information as soon as it comes out. Not everybody can watch all sources of input, so this way the community knows as soon as the first member sees anything relevant. Everyone can then be prepared to manage any changes, which are happening more often and tend to carry greater consequences for an institution.

With security practices now mandated across so many activities, organizations that were never very focused on regulations have become interested in adopting necessary approaches. As a result, RRCoP is a useful connector for organizations like EDUCAUSE, primarily focused on teaching and learning. The Association of University Export Control Officers (AUECO), is another RRCoP partner organization because of the connection through regulation and compliance. See Figure 2 for some of the partner organizations in the arena of regulated research.

With the increase in awareness around protecting data, we have seen

[e] See https://bit.ly/4fI7eTI

Figure 1. Regulated research programs involve many agents to implement and operate.

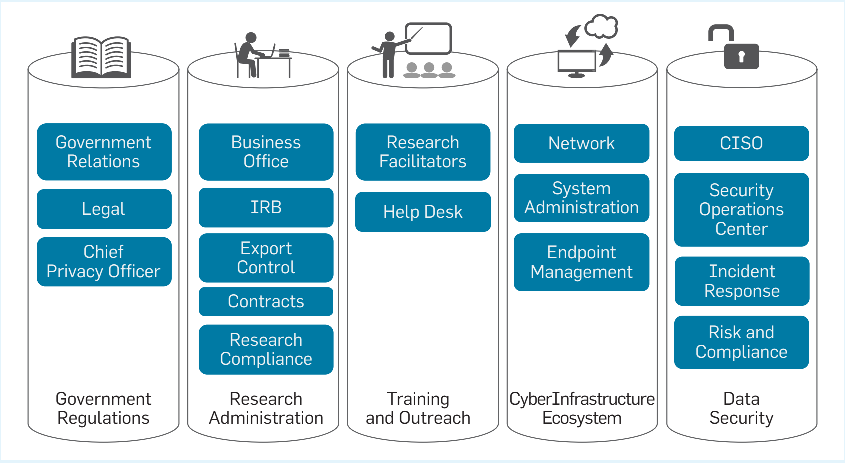
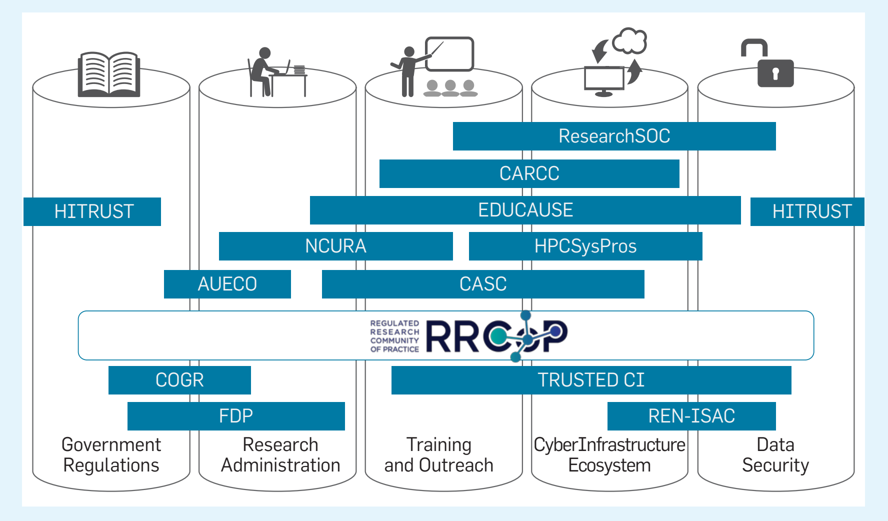


Figure 2. The community of regulated research encompasses many organizations.



a multitude of approaches to add safeguarding of data in contractual language, all listing different sets of controls. This puts a heavy burden on institutions to figure out whether existing procedures meet the stated requirements. This is especially frustrating if an institution has gone through the effort to obtain an assessment by an external auditor of their controls for relevant cyberinfrastructure. The optimal situation would be that such an assessment report can be used to meet the requirements of all contracts. For that reason, it is important that federal and state agencies join together to use a single standard.

This is where a community can help. As a community, we have a stronger and more credible voice to negotiate with agencies to come to a workable solution that meets the shared goal of safeguarding data without imposing undue burden on institutions to meet the required controls. The Council of Government Relations (COGR) can help as a partner of the RRCoP community to open a conversation with lawmakers to move to a single safeguarding standard.

There may be a perception that these compliance requirements and controls are at odds with academic freedom.

The community has collected a set of resources on the RRCoP website for any organization that is beginning with building a compliance program.[f] One resource is a template for a system security plan (SSP) for a system that is compliant with NIST Special Publication 800-171 developed in a workshop in May 2023. In 2024, we developed a report from the workshop on “A Day With The CMMC Assessors,” which gives very useful information on how implementation of controls is viewed by auditors.

Building compliant cyberinfrastructure is not easy and not cheap. Many smaller institutions will not be able to establish a successful and sustainable program. This is where it may be worthwhile for universities to build a regional resource, just like the regional network providers have managed over the past few decades to build stable and cost-effective network infrastructure advancing all institutions in a region. This way, smaller institutions can have access to compliant cyberinfrastructure for a manageable contribution to the regional organization. Some planning will be needed and legal agreements will have to be worked out, but the benefit would be substantial.

Outlook

Security concerns and ensuing controls from compliance frameworks with some procedure to prove you are compliant are going to be with us in the world of academic research. While researchers must be aware of this need and do their part to secure their research until it is published, academic institutions that want to have competitive research programs must provide the cyberinfrastructure and staff resources to develop and run the compliance programs. This complex activity should not be an undue burden on the researchers.

There may be a perception that these compliance requirements and controls are at odds with academic freedom. Protecting the research data from corruption from infrastructure failures, unauthorized modification, and theft by malicious actors should be considered a necessary activity to ensure that the research is valid and trustworthy. No researcher wants to find their results published or used with someone else taking the reputational or financial credit. Until it is published with your name, you want the fruits of your work protected. The protections put no limitation on what subject is being studied or restrict the reporting of validated findings, which is what the principle of academic freedom guarantees.

Maybe the most urgent issue to address is the proliferation of requirements from all federal and state agencies and private companies as they share awareness of the need for security but add different security requirements in awards and contracts. The goal we should strive for is one standard set of security requirements that gets reviewed or certified once. The results can then be used in all contracts as evidence that an institution meets the requirements. The negotiation of a standard is what the RRCoP and all its partners are striving to leverage their voices to. C

Erik Deumens (deumens@ufl.edu) is senior director, Information Technology, University of Florida, Gainesville, FL, USA.

Carolyn Ellis (carolynellis@asu.edu) is director, Research Cybersecurity and Compliance, Knowledge Enterprise, Arizona State University, Tempe, AZ, USA.

This Opinion column is based upon activities supported by the National Science Foundation under Grant #2409859 and Interagency Agreement #A2407-049-089-064206.0. Any opinions, findings, and conclusions or recommendations expressed are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

[f] See https://bit.ly/3CjRzLK