Compliance? We don’t need no stinking compliance!

Jeffrey Miller
Senior Systems Administrator – ITS Research Services

Introduction

It should come as no surprise to a researcher or systems administrator that keeping data safe is a challenging process due to the number of vectors for attack. While the statement in the title is probably something that we have thought on our own (or heard expressed by our colleagues), it is not tenable with the increasing number of laws, regulations, and funding agency requirements. Depending on the source of the requirements, being in a state of noncompliance could result in:
- Loss of grant funding
- Loss of accreditation
- Civil and/or criminal court actions resulting in fines and/or confinement
- Closure of a facility or disbandment of a group

The stakes are very high in many cases and cannot be ignored without repercussions. In this paper, some ideas for consideration are presented based on experiences with the ITS Research Services (ITS-RS) team at The University of Iowa (UI).

Challenges Faced

When considering compliance in the research technology arena, the largest challenges faced by the UI community were not technical ones. Rather, it was the lack of clarity concerning standards, lack of communication between the stakeholders involved in the various parts of campus involved with information technology and research data, and process and personnel bottlenecks resulting in delays to the research process. Researchers didn’t know who to talk to figure out what compliance regulations to follow. Often, they faced the situation where different sets of compliance standards conflicted with each other resulting in the lack of clarity for how to handle it.

To face these challenges, a cross functional position (Research Compliance Technology Specialist – RCTS) was created to act as the go to person for whom could assist in interpretation of the standards and how to meet them. Additionally, the RCTS would act as a facilitator of communication between researchers and technical groups providing IT services. For further information details concerning the RCTS, please see the PEARC18 technical paper referenced later.

Facing the Challenges

Compliance standards are numerous. Depending on the type of data and end customers, one could be required to adhere to:
- DISA STIG
- NIST 800-171
- NIST 800-53
- HIPAA
- PCI-DSS

Regardless of which standard(s) one fall(s) under, being in compliance boils down to:
- Identifying what controls are present in the standard
- Determining requirements for each control
- Determining actions to be taken in either organization processes or systems configuration

To provide user accessible guidance and documentation, the RCTS worked primarily with the Information Technology and Security Policy (ISPO) group to identify what controls were met with existing UI processes, policies and procedures and perform a gap analysis on what wasn’t addressed in those arenas. UI systems administrators were engaged to determine what infrastructure needed to be put in place to meet the needs of both systems and security configuration. For example, the UI has a robust puppet infrastructure with which to manage the configuration of research data systems. However, integration with a host intrusion detection was lacking. Looking at the technical solutions available to address this missing component, Wazuh was chosen for its capabilities and interoperability with other existing security systems.

Configuration of information systems in a consistent manner is essential for meeting any of the compliance standards. While it is possible to manually configure systems using a checklist, use a configuration management system such as Puppet, Ansible, or Chef to automate the process is highly recommended in order to ensure consistency and eliminate the inherent human error in the use of a checklist.

Conclusions

Compliance doesn’t have to be the pink elephant in the room. When taken systematically, one can achieve accreditation, survive audits, and provide better systems and data security.

With a collaborative effort in conjunction with technical solutions, the landscape for researchers at the UI for conducting research while meeting varied aspects of differing compliance requirements has improved. While we still face challenges with more regulations and standards being added (GDPR anyone?), we are in the position now where we can build off of what has already been started to provide flexible frameworks that enable research data generation.

References and Resources


SIMP Project: https://simp-project.com/

Wazuh: https://wazuh.com/
Puppet: https://puppet.com/
Ansible: https://www.ansible.com/
OpenSCAP: https://www.open-scap.org/
InSpec: https://www.inspec.io/

Contact

Jeffrey Miller
Email: jeff-miller@uiowa.edu
Freenode: millerjl1701
GitHub: https://github.com/millerjl1701

Acknowledgements

I would like to thank the following for supporting attendance at GCC 2018 and the development of this work:
- Dr. Richard Smith, Director, Iowa Institute of Human Genetics, and the IIHG Team
- Ben Rogers, Senior IT Director, ITS Research Services and the ITS RS Team
- The University of Iowa Carver College of Medicine