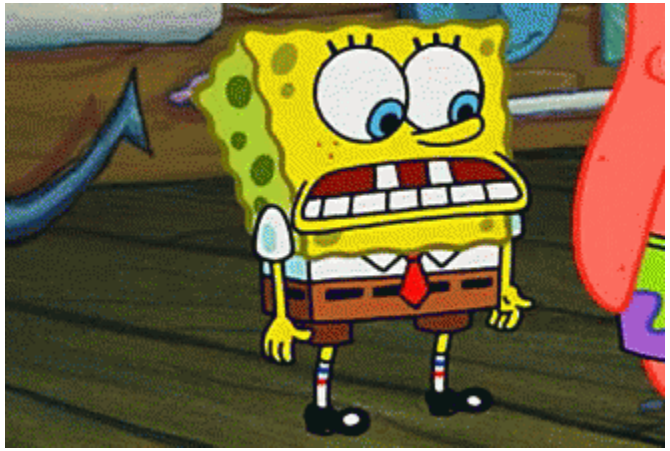
Flexible and Scalable Process for Assessing, Validating, Auditing, and Authorizing a HPC for Controlled Data

Colin Glover
Sera-Brynn, Principal
colin.glover@sera-Brynn.com

Earth

Mean?

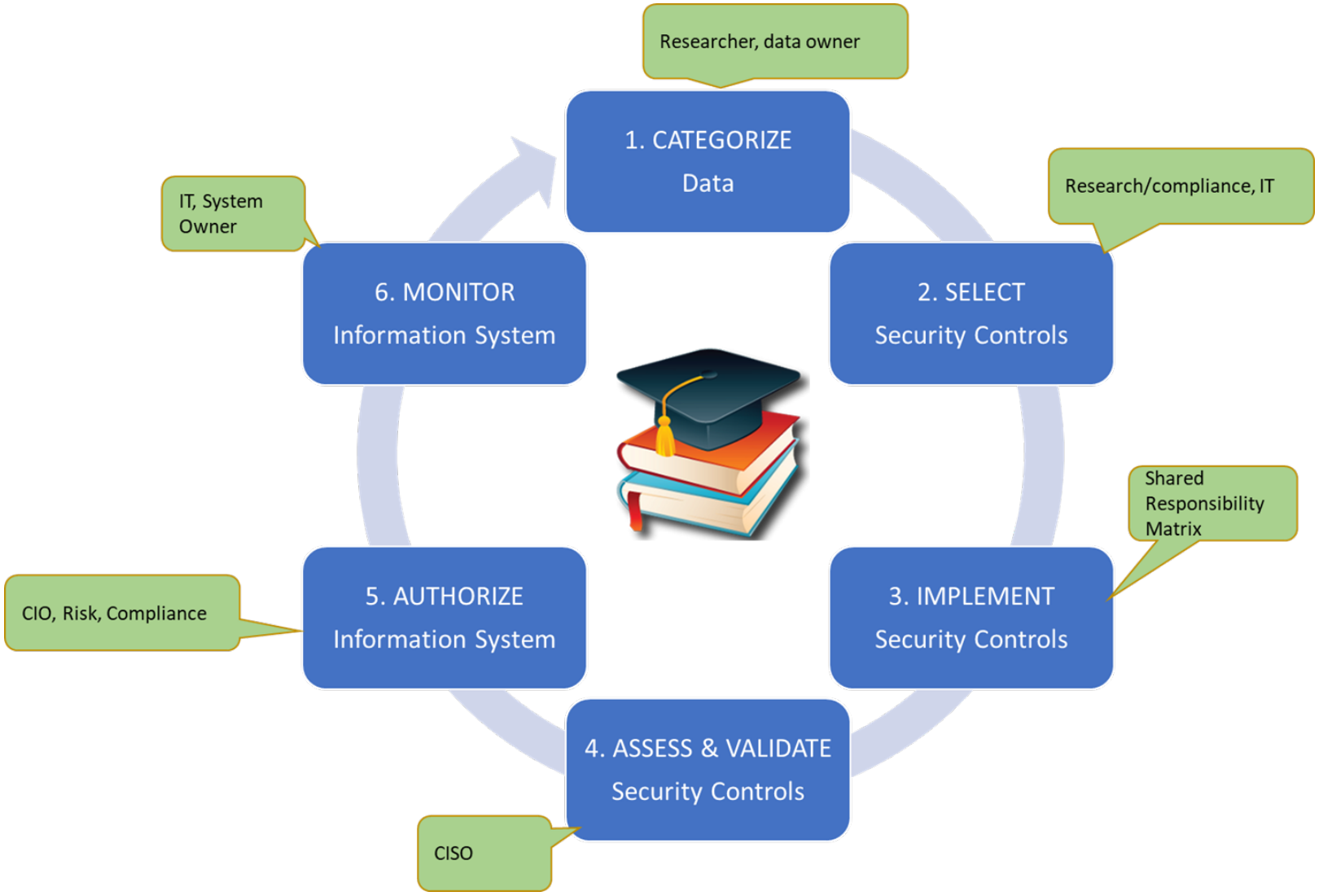
Risk Management Framework -Based Approach



Sera-Brynn – A certified cyber audit and assessment firm.

- We are a FedRAMP Third Party Assessment Organization (3PAO) and PCI QSA specializing in cyber risk management and compliance.
- Sera-Brynn was founded in 2011 by former members of the U.S. intelligence community. Since then, we have grown into the highest-ranked, pure-play cybersecurity compliance and advisory firm in the world.
- Sera-Brynn is focused on assisting higher education and the defense industrial base with cyber compliance needs.
- **Our goal is to help you create a secure environment with minimal impact on the end user.**

RMF-Based approach



The Risk Management Framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

- Continuous monitoring of security controls and their effectiveness
- Audit trail collection and reporting
- Determining acceptability of security controls in terms of risk
- Enabling assessment of implementation and effectiveness of controls
- Collecting and reporting on logs from all assets and activities

Risk Management Framework Fundamentals

Step 1: Categorize

- In this step, the Office of Research and the researcher will identify the computing requirements, type of data, and protections required for a new or existing project.
- Example types of data could include:
  - Export Control, HIPAA, PII, CUI, etc.

FIPS and NIST provide excellent guides on how to categorize data and systems

Step 2: Select Security Controls

- Based on the environment selected, identify controls necessary to meet the specific requirements,
- Identify any other extenuating requirements
- Assign responsibility for control implementation to the appropriate person or organization

Key to having a compliant system is the concept of shared responsibilities. IT cannot be fully responsible for full compliance.

Step 3: Implement Security Controls

- Using the appropriate System Security Plan, and as guided by the selected framework, data requirements, and the IT environment; security controls are implemented according to the Shared Responsibility Matrix.

The NIST assessment guides can be of significance assistance to ensure you are hitting the mark.

Step 4: Assess Security Controls

- Using the Security Assessment Plan, IT and the HPC team will validate the control implementation. Controls unable to be implemented as defined by the System Security Plan may require a compensating control. Use of a compensating control may require additional review or approval to determine residual risk. Any controls marked as partially or not implemented must be further assessed to determine additional risk to the project, program, or IT System.

Step 5: Authorize

- Informed by the materials generated in #4, the Office of Research as the data owner reviews concerns raised and accepts risk for any unresolved controls. If residual or additional risk exceeds risk tolerance, IT may request additional information, or suggest additional controls and mitigations.
- Once the project and supporting system is approved, the Monitoring Phase begins.

Step 6: Monitor

- IT will continuously monitor technical controls to ensure the controls in the environment are functioning as intended and to detect potential indicators of compromise.
- A variety of tools may be used to accomplish this step.
- Monitoring may also include audits and revalidation by compliance personnel

Recommended Roles & Responsibilities

1 Determine compliance requirements that may apply

Responsible: Office of Research

2 Identify environment appropriate for project

Responsible: Office of Research, IT, HPC Team

3 Implement required security controls

Responsible: Researcher, IT, HPC Team

4 Assess Security Controls

Responsible: IT, HPC Team

5 Authorize system for use

Responsible: Office of Research

6 Continuous Monitoring

Responsible: IT, HPC Team, Compliance

Hard Parts

- In a multitenant HPC, determining who is ultimately responsible for the security of system involves quite a bit of politicking
- Understanding and defining the network boundaries is exceedingly important
- Specific controls can be fairly confusing, don’t try to read too much into it
- Each specific control can be gotten around, it’s the totality of the controls which secures the environment
- Risk and compliance may not mean the same thing
- Monitoring compliance across the enterprise

Questions?