SAINT LOUIS UNIVERSITY

Secure Research Environment & FISMA 101

Saint Louis University
Information Technology Services
service. technology. leadership.

Higher Purpose. Greater Good.™

SAINT LOUIS UNIVERSITY

AGENDA

- FISMA and NIST RMF
- Six specific processes
- Portable Computing Devices and Media
- Getting Help

SAINT LOUIS UNIVERSITY

FISMA AND NIST RMF

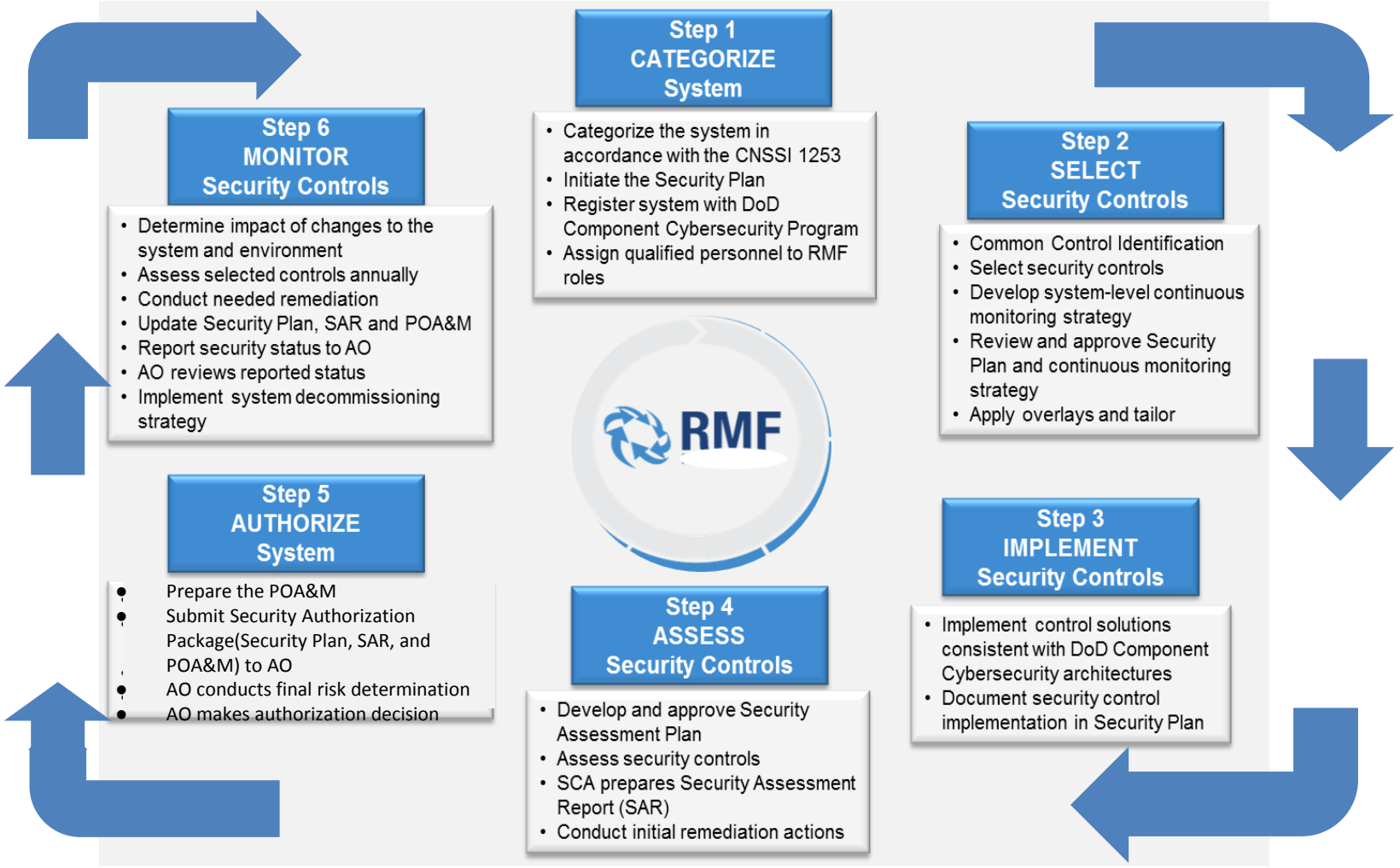
SAINT LOUIS UNIVERSITY

WHAT IS FISMA?

- **Federal Information Security Management Act (FISMA) of 2002**
  - **Included by Congress as part of the E-Government Act of 2002**
  - **Establishes security guidelines for federal agencies or *those providing services* to federal agencies**
  - **Sets forth:**
    - **Specific requirements for security programs**
    - **Specific documentation, policies and procedures**
    - **Defined processes required to be in place in accordance with NIST 800-53 – a national security standard**

SAINT LOUIS UNIVERSITY

NIST RISK MANAGEMENT FRAMEWORK (RMF)



SAINT LOUIS UNIVERSITY

SIX SPECIFIC PROCESSES

SAINT LOUIS UNIVERSITY

1. GETTING AN ACCOUNT

Non-FISMA

Accounts were provided on an ad hoc basis (phone, email, etc.): accounts maintained as necessary

FISMA

Accounts have to be formally authorized and approved by project lead as appointed by PI: processes need to ensure account list is current and appropriate

Why?

Additional controls implement appropriate accountability and assurance of minimum necessary access rights

2. REMOTE ACCESS & LOG-IN

Non-FISMA

Access was available through a variety of means and mechanisms simply requiring a username and password (RDP, telnet, SSH, web portals, etc.)

FISMA

Two-factor authorization: remote access into the environment has to be secured with both something you know (a password) and something you have (a token)

Why?

Passwords are easily stolen (Target, Home Depot, Anthem, Premera, etc.), so best practices and compliance require additional verification

3. DATA TRANSFERS

Non-FISMA

Systems allow whatever means for data transfer most convenient or available to users

FISMA

Sensitive data are regulated and therefore must have controlled mechanisms to allow data in and out

Why?

Complexity and lack of control provide opportunities for loss or misuse

4. CHANGE MANAGEMENT

Non-FISMA

Changes are made on an ad hoc basis, not formally tracked or reviewed for security impact (updates to applications, databases, etc.)

FISMA

Changes must be formally reviewed, approved and tracked

Why?

Oversight is necessary to ensure changes do not impact the integrity of the system's security and tracking is necessary for audit purposes

SAINT LOUIS UNIVERSITY

5. LOGGING AND MONITORING

Non-FISMA

Logs and review of logs are performed on an ad hoc basis

FISMA

All systems enforce required logging measures to ensure they remain secure

Why?

Logs are necessary to both detect adverse events (breaches, misuse of data, etc.) and for audit purposes

SAINT LOUIS UNIVERSITY

6. SECURITY ASSESSMENTS

Non-FISMA

No formal security assessments are performed

FISMA

Regular security assessments for vulnerabilities and compliance are conducted

Why?

To ensure ongoing security of the environment

SAINT LOUIS UNIVERSITY

PORTABLE COMPUTING DEVICES AND MEDIA: DATA PROTECTION AND PRIVACY

Higher Purpose. Greater Good.™

PORTABLE COMPUTING DEVICES

- Must comply with current SLU policy:
  - Full disk encryption to protect the confidentiality and integrity of systems and data
- Data is contained fully within the protected environment
- Users traveling to areas deemed as high risk are advised not to access the FISMA environment from those locations
- Portable devices taken to high risk areas will be completely erased and restored to the baseline configuration upon return and before being allowed to access the FISMA environment again

MEDIA ACCESS

- No ability is provided for users to use or access data on removable media as part of the Secure Research Environment
- Privileged users are authorized to use removable media for the purpose of system installation and maintenance activities, as approved by the Change Control Board (CCB)
- No restricted data is stored on removable media, and media is scanned for malware before use with the Secure Research Environment

MEDIA ENCRYPTION

- SLU Policy allows the use of unencrypted removable media only when encryption interferes with the media's essential function
- As removable media is only used with the Secure Research Environment for system installation and maintenance (which is usually not possible with encrypted media) encryption is not required for removable media
- If Restricted Data is stored on removable media, the media will be fully encrypted with FIPS 140-2 compliant products

INSIDER THREATS

- What is an Insider Threat?
  - A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems
- What are some signs of this type of behavior and/or activities that you may encounter?
  - Job dissatisfaction that may be in the form of verbal complaints against the university
  - Harassment of fellow co-workers (which should be reported immediately)
  - Violations of other university policies
- What should you do if you suspect Insider Threat Activity? Report it!
  - Call the Anonymous Compliance Hotline: 877-525-KNOW
  - Contact the IT Security & Compliance Hotline: 977-5499

SAINT LOUIS UNIVERSITY

GETTING HELP

WHAT IF I NEED HELP?

- Nothing changes with your workstation support: contact the SLU service desk as you normally do
- For questions regarding FISMA and the Secure Research Environment, please contact the Research Technology Group at rtg@slu.edu or visit slu.edu/rtg

SAINT LOUIS UNIVERSITY

APPENDIX

NIST REFERENCES

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment)
- NIST Special Publication 800-39 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-60 (Information Types Mapping)

SAINT LOUIS
UNIVERSITY

EST. 1818