THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

Knowledge that will change your world

FISMA Compliance and Research

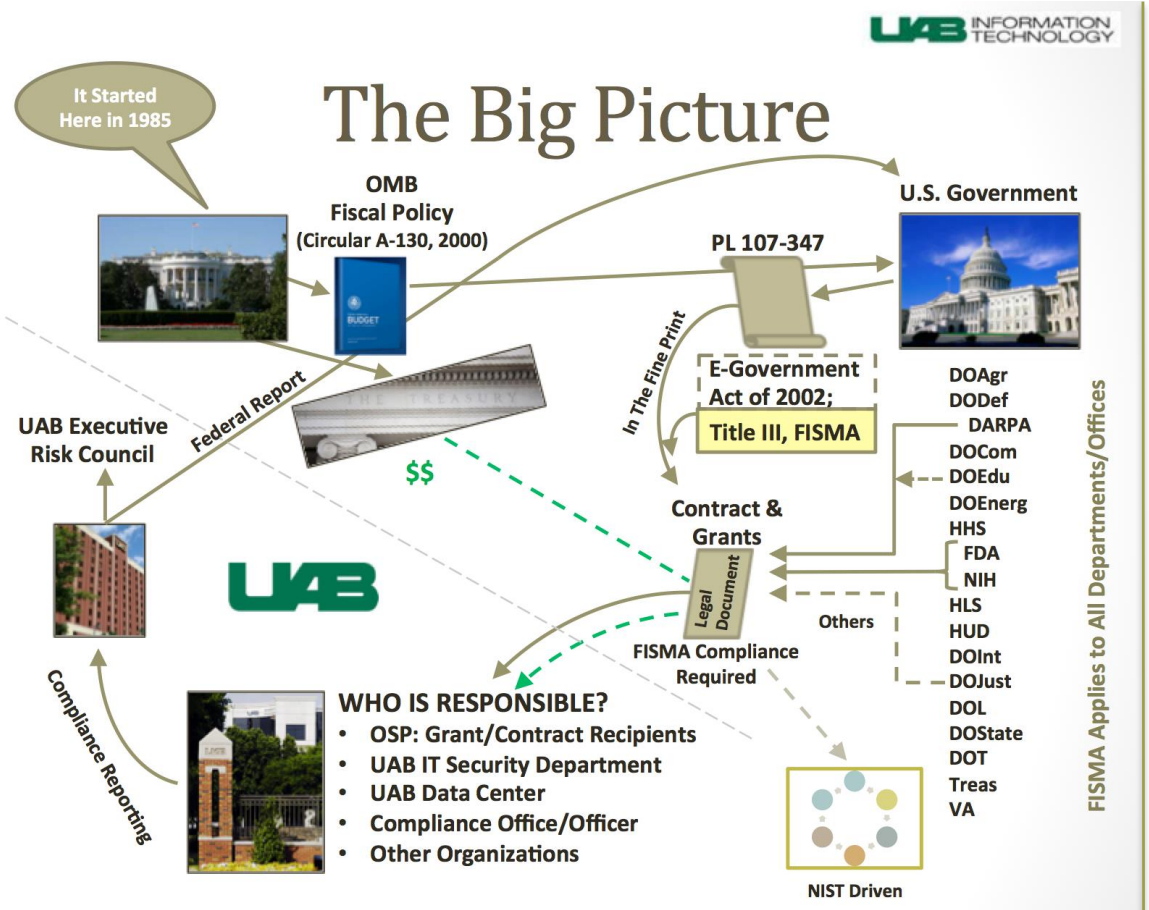
UAB Enterprise Information Security

September 2013

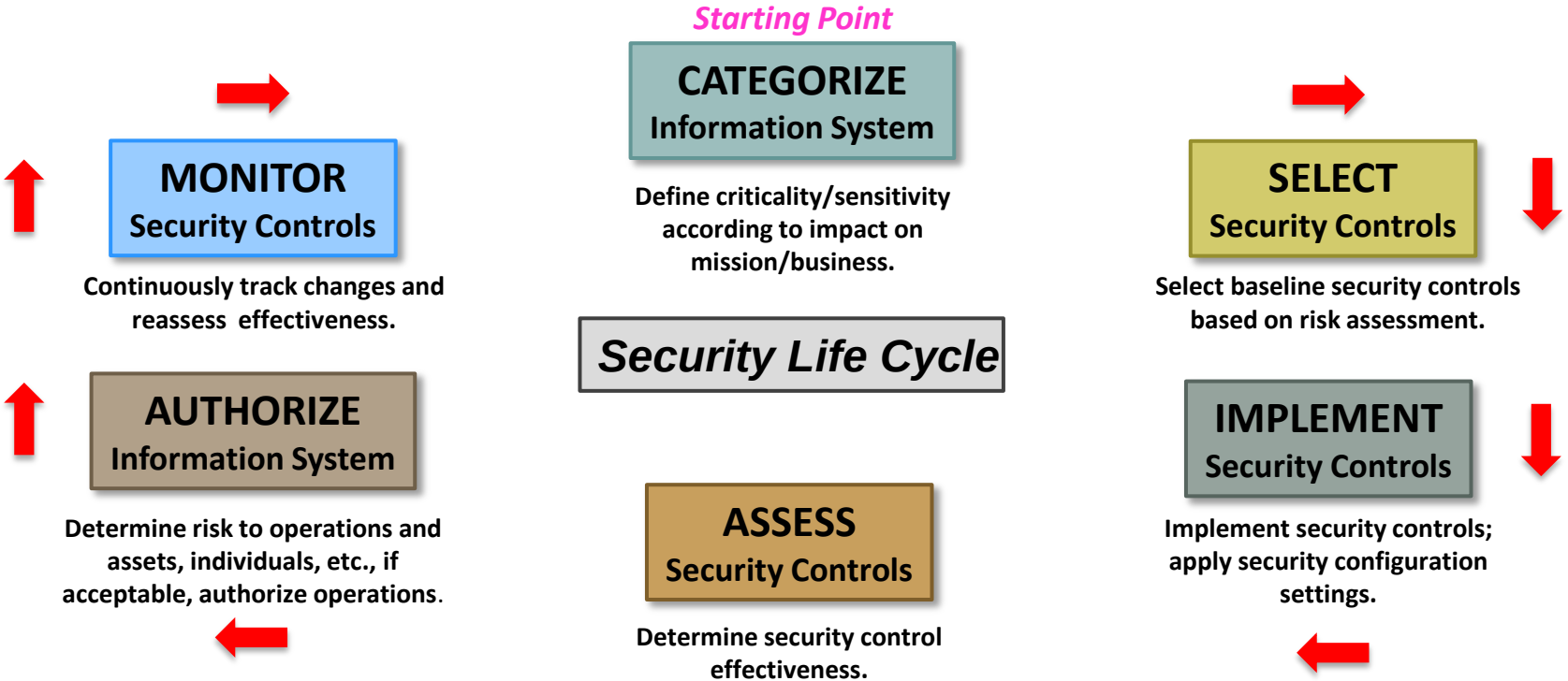
What's FISMA?

"… provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets"

PL 107-347 §3541(1)



The NIST Risk Management Framework



Ref: NIST SP 800-37

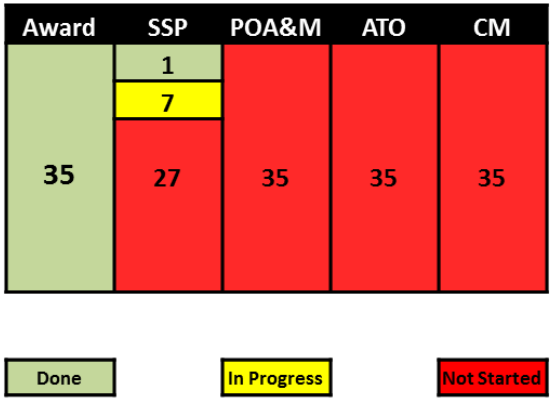
Who Is Impacted by FISMA at UAB?

- **Applies to all Federal Contracts, Grants, and Data Usage Agreements**
- **Covers Data, People, Facilities, Computers, Privacy, & Services**
- **Researchers responsible for monitoring compliance; start to finish**
  - Requires Risk Management Process from data gathering, to input, to analysis, to storage, to archiving, to closeout

What's at Risk?

Risk Assessment → System Boundaries → Control Implementation → Control Assessment → System Authorization → Ongoing Monitoring

- **Over $87 million in active contracts/grants (today)**
  - ✓ Plus an additional $45+ million available in current awards
- **35 Projects Across Three Schools**
  - ✓ (19 Contracts, 16 Grants)



as of 8/31/13

Challenges We Face!

Risk Assessment → System Boundaries → Control Implementation → Control Assessment → System Authorization → Ongoing Monitoring

- **NIH has >20 Information Security Offices**
  - Some highly formalized, some just getting started
- **Our past experience doesn't apply very well**
- **Wait and see approach not sufficient, must be more responsive and agile**
- **FISMA is a long term effort!**

Researcher/Primary Investigator Responsibilities (1)

- **Primary Investigator responsible for compliance; assisted by consulting from Information Security Office, OSP, Compliance and others**
- **Defining and implementing appropriate security controls; assisted by consulting from Information Security Office**
- **Clearly identify and describe scope of research and related work**
- **Identify all personnel & subcontractors and their scope of work**
- **Collaborate with OSP, IRB, IT, & Compliance to include FISMA allocations in budget line for grant applications and contract documents**

Researcher/Primary Investigator Responsibilities (2)

- **Collaborate with key personnel (CISO, Administration, IT Staff, Compliance, IRB, etc.) to ensure compliance**
- **Clearly describe all data flows & systems involved in research work**
- **Develop System Security Plan (including boundary diagram) coordinating with Information Owners, System Administrators, Security Officers, Agency/Sponsor, and end users**
- **Maintain System Security Plan to ensure consistent actions with prior agreements**

Researcher/Primary Investigator Responsibilities (3)

- **Ensure users have appropriate security training; with assistance from Information Security Office**
- **Designate an Information System Security Officer (grant/contract specific) to perform responsibilities.**
- **Provide data for measurement of compliance as needed.**
- **Others**

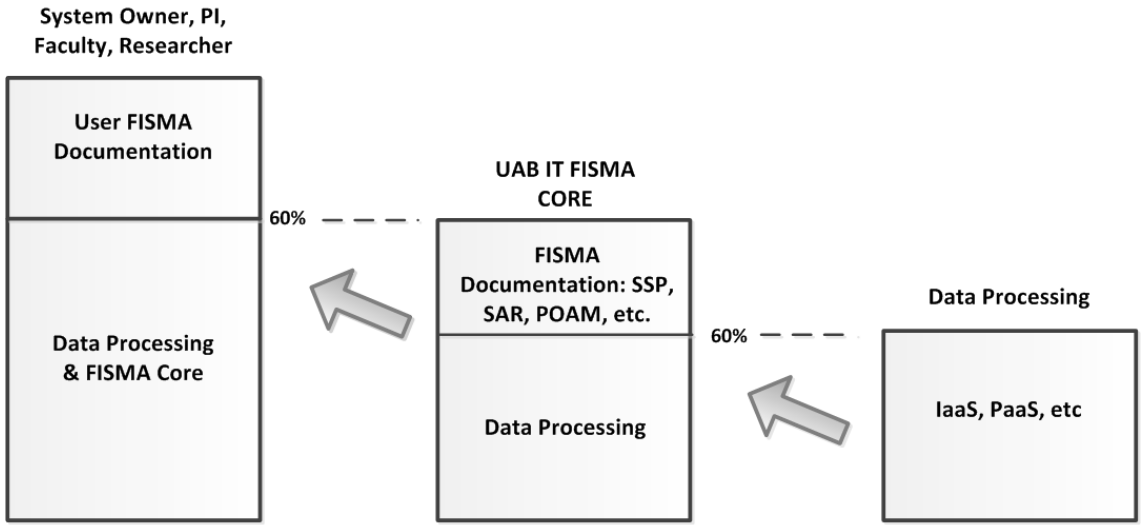
Role and Responsibilities?

Role	Current	Recommendation
System Owner	Dependent on Effort -- UAB PI or Federal Govt	No change
Governance Risk Compliance (GRC) Framework Leader (UAB)	---	UAB to establish position* to coordinate/manage GRC; IT to assist as needed (tool, advice, assistance, etc.)
Chief Information Officer (UAB)	VP IT	Formally designate CISO to manage/coordinate activities
Information System Security Officer	PI Designee	Centralized IT function with dotted line reporting to PI
Authorizing Official	Federal Govt Funding Agency No known UAB ATOs	UAB VP of Research to serve as UAB's Authorizing Officer: Fed Gov't to have their own AO

* In UAB Compliance Office

SSP Inheritance Process

Risk Assessment → System Boundaries → Control Implementation → Control Assessment → System Authorization → Ongoing Monitoring



UAB System Owner employs FISMA CORE from UAB IT and inherits the CORE SSP controls and documentation.

UAB IT FISMA CORE provides System Owner with a compliant IT system including documentation, SSP, Audits, POA&M, etc.

Data Processing provided either internally by UAB IT or outsourced (IaaS, PaaS, etc.)

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
Knowledge that will change your world

Next Steps…

- **Learn more about FISMA compliance requirements**
- **Initiate dialog with OSP, Compliance, IRB, and IT to begin the process early including provision of security efforts funding**
- **“FISMA Playbook” being developed for researchers including appropriate training**
  - ✓ Required for all PI’s & staff