WEBER STATE UNIVERSITY

NIST RMF vs CSF: Which is Better for Higher Ed?

NIST RMF vs CSF: Which is Better for Higher Education?

- Agenda
  - Definitions of security policies
  - Definitions of RMF
  - Definitions of CSF
  - Research conducted re: RMF vs CSF
  - Discussion

What is a Security Policy?

- An information security policy is a set of documents outlining the organization's view on a security matter
- Policies can exist for:
  - Acceptable information resource usage
  - Protection of sensitive information

    Inclusion of best practices in the organization

NIST Risk Management Framework (RMF)

- NIST = National Institute of Standards and Technology
- The Risk Management Framework is a series of standards and guidelines that can protect an information system
- Required for all federal systems; recommended for all non-federal systems

NIST Cyber Security Framework (CSF)

- NIST has also devised a Cyber Security Framework (CSF)
- CSF can be used by any sized company in any industry
- CSF has security objectives, then points to industry best practices to achieve those objectives

Which is Better for Higher Education?

- Either RMF or CSF could be used to help secure higher education systems
- RMF Pros: All controls are already defined. Implementation becomes a matter of executing the controls
- RMF Cons: RMF is *very* exhaustive and expensive. May be overkill for higher ed

Which is Better for Higher Education? (cont)

- CSF Pros: Baseline of information security best practices that can be implemented at any level
- CSF Cons: CSF draws from many sources; implementers need to be familiar with many frameworks, not just one

Which is Better for Higher Education? (cont)

- Research was conducted to determine how RMF was implemented in higher education
- Research showed that most higher ed institutions are using CSF rather than RMF
- Infosec officers reported that CSF was more flexible and easier to work with
- According to them, RMF is very rigid when implemented properly

Discussion

- Is RMF a “one-size-fits-all” solution?
  - Probably not
- Is CSF a “one-size-fits-all” solution?
  - Probably not, but closer than RMF
- Does CSF more closely align with higher education functions and data protection needs?
  - Generally, yes
- Is CSF recommended for use at higher edu institutions?
  - Generally, yes