Top 10 Myths

FISMA, RMF, 800-53, Continuous Monitoring, and Life

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory
First, a quick refresher course.
Risk management 101.
Risk.

**Function** (threat, vulnerability, impact, likelihood)
The unlikely threat.

Our three-year old adopted pit bull.

Cute.
Lovable.
Smart.

Hi. I’m Sophie. Welcome to the Forum!
The vulnerability.
The impact.
and the likelihood?

100%
And a few family photos.
Our newest addition.

7-week old kitten rescued yesterday from a storm drain next to Starbucks...

Named him “Bucks”
Now on to business.
Myth #1
FISMA focuses more on compliance than effective security.
Myth #2
Organizations have to implement all security controls in NIST SP 800-53.
Myth #3
NIST does not prioritize the security controls in SP 800-53.
Myth #4

FISMA is just a paperwork exercise.
Myth #5

The new Cybersecurity Framework is going to replace the RMF.
Myth #6

Organizations cannot obtain FISMA certifications for their products, systems, and services.
Myth #7

FISMA requires organizations to assess every security control annually.
Myth #8
The DHS Continuous Diagnostics and Mitigation Program is intended to replace the current CM efforts.
Myth #9

Hiring more people with hacking skills is the best way to improve your cybersecurity work force.
Myth #10
Mitigating vulnerabilities is the best way to ensure that your critical systems are resilient.
We the People
Contact Information

100 Bureau Drive  Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader
Dr. Ron Ross  
(301) 975-5390  
ron.ross@nist.gov

Administrative Support
Peggy Himes  
(301) 975-2489  
peggy.himes@nist.gov

LinkedIn
http://www.linkedin.com/in/ronrossnist

Senior Information Security Researchers and Technical Support
Pat Toth  
(301) 975-5140  
patricia.toth@nist.gov

Kelley Dempsey  
(301) 975-2827  
kelly.dempsey@nist.gov

Web: csrc.nist.gov

Comments: sec-cert@nist.gov