

Trick-or-Treat - Be Complete

Avoiding the Trick of
Compliance Issues
by a Risk-based Program



Greg Witte, G2 Inc.
Greg.Witte@g2-inc.com

There's a Tension Between Compliance and "Just Doing the Right Thing"

- Many organizations are subject to a broad range of compliance requirements and contractual obligations
- It is tempting to chase compliance as the end goal, thinking that if we've checked the right boxes then we should be OK
- Some leaders want to reactively just keep up with the latest headline-based issues
- It is hard to plan strategically when being driven by winds from different directions without clear vision of the destination

Positive incentives are always encouraged

- In our work at NIST, we frequently have organizations stress the need for voluntary approaches to managing risk
- Many organizations want to do the right thing but need a flexible approach
- Some of the “old ways” forced prescriptive rules with criteria that didn’t even apply



Those of us who are parents understand that “voluntary” isn’t always enough



- Sometimes we need ways to exert a little encouragement
- There’s often good intent, but hard to justify expending resources without a driving force
- We often hear concerns from orgs that want reassurance that they are doing “enough”, both for their own due diligence and also to avoid penalties

Regulations do help ensure consistent and reliable achievement



- Effective pressure to “do the right thing”
- We often hear concerns from organizations that want assurance that they are doing “enough”, both for their own due diligence and also to avoid penalties

Organizations get “tricked” when compliance alone is the end goal

- Example: Payment Card Industry Security Standards Council (PCI SSC) Data Security Standard (DSS)
 - Est. in Dec 2004 to provide a minimum set of required security controls to protect cardholder data
 - Many well-known breaches occurred on orgs that had achieved PCI compliance
 - Many orgs see compliance as a milestone to achieve and move on rather than a state to be maintained, improved, and updated
 - Verizon 2015 PCI Compliance Report states, “Of all the companies investigated by our forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach” (Verizon, 2015).
- We have similar challenges with NIST 800-53 – over 900 controls & enhancements in Revision 5, and confusion over baselines & tailoring

Audience Poll:

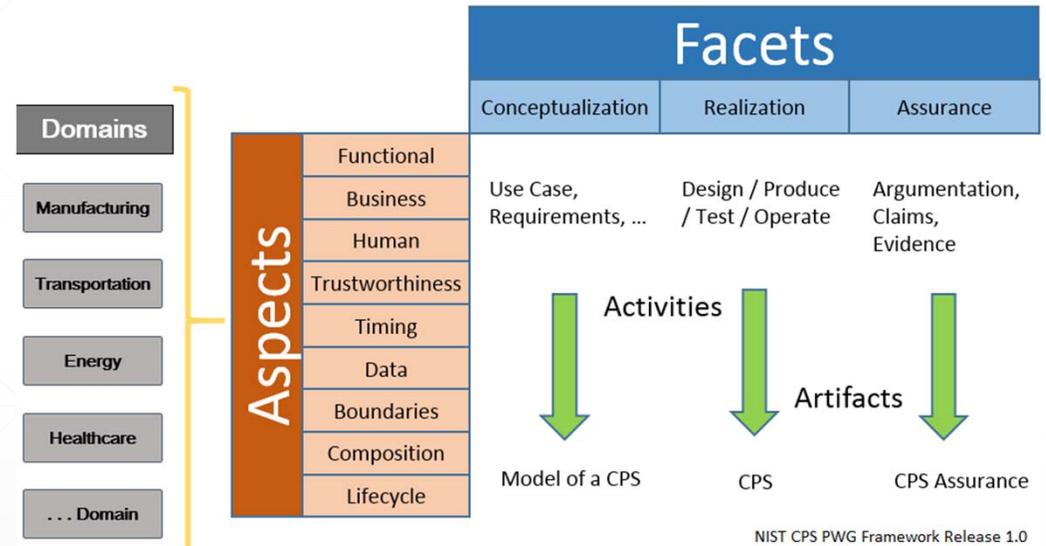
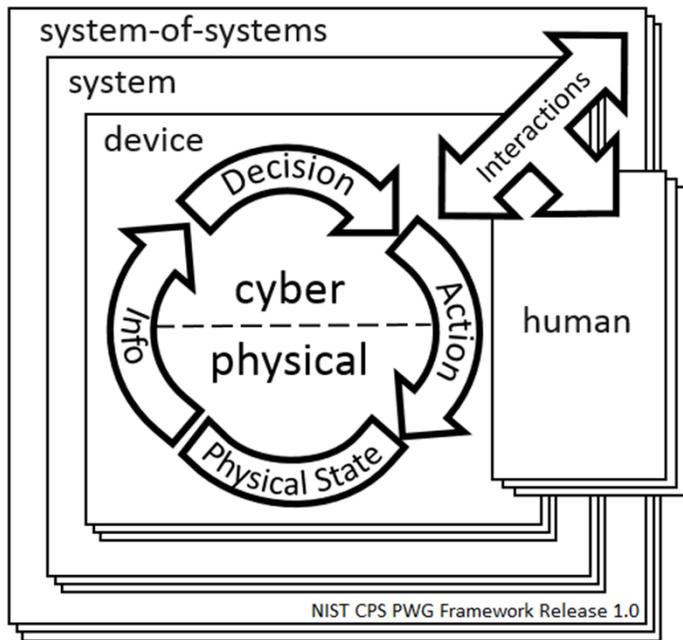
**How many here are using
the NIST Framework?**

It's a "Trick"!

NIST has multiple frameworks to leverage

- Cyber-Physical Systems (CPS) Framework
- Baldrige Excellence Framework
- Cybersecurity Framework
(aka the Framework for Improving Critical Infrastructure Cybersecurity)
- Risk Management Framework
- NICE Framework (Workforce)
- Privacy Engineering Framework

Cyber-Physical Systems Framework



Available from: <https://pages.nist.gov/cpspwg/>

Baldrige Excellence Framework



Cybersecurity Excellence Builder available from:
<https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative>

NICE (Cybersecurity Workforce) Framework



Accelerate Learning and Skills Development



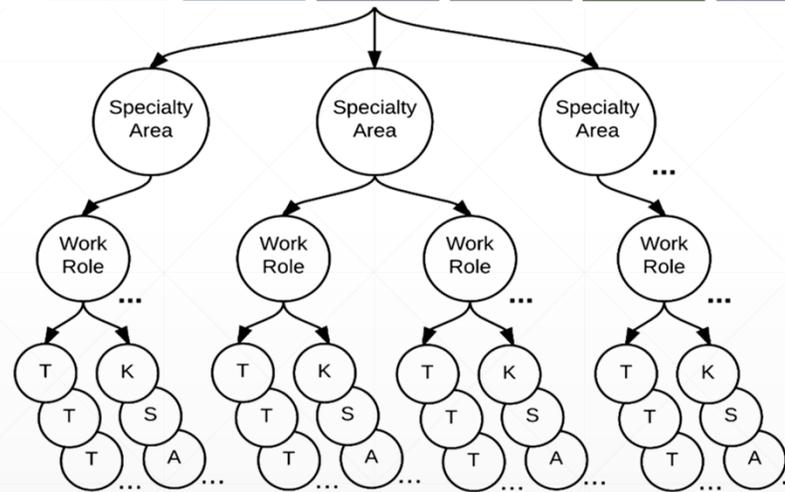
Nurture a Diverse Learning Community



Guide Career Development and Workforce Planning



7 Categories



33 Specialty Areas

52 Work Roles

~1000 Tasks

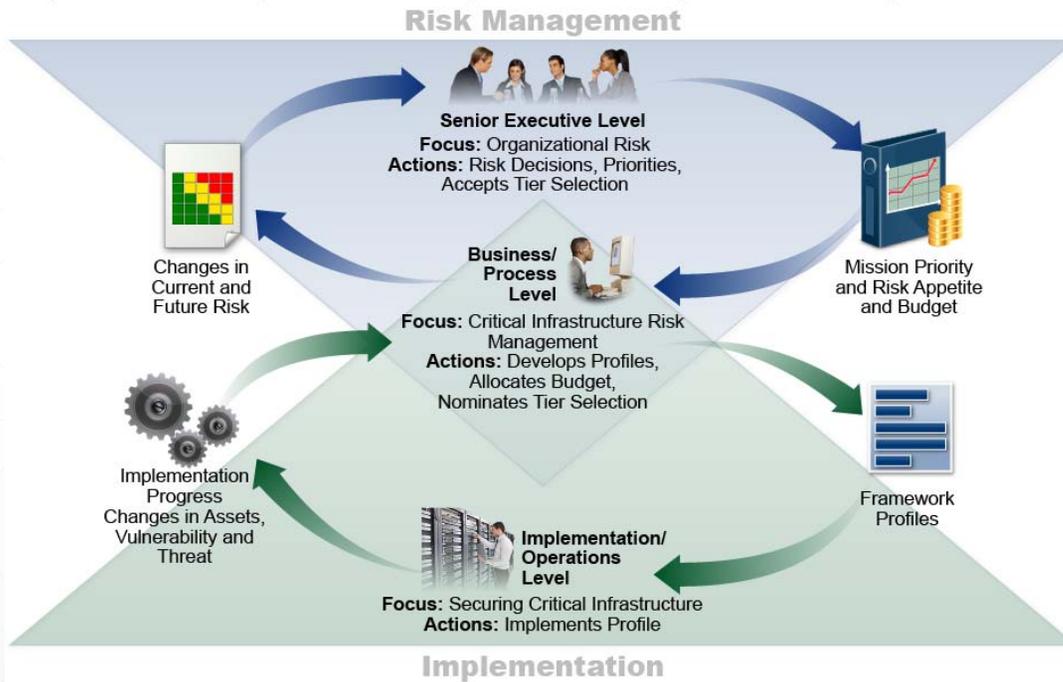
Knowledge, Skills, Abilities

Risk Management Framework

- Mandatory for Federal agencies but useful for all
- Works in tandem with Cyber Framework
- Being updated to better support evolving needs, integration with other frameworks, and system engineering approach
 - Draft NIST SP 800-160, Vol. 2, Systems Security Engineering: Considerations for Developing Cyber Resilient Systems,
 - Cyber resiliency goals, objectives, techniques, approaches, and design principles for system life cycle processes.
- Provides controls and enhancements for achieving CSF outcomes

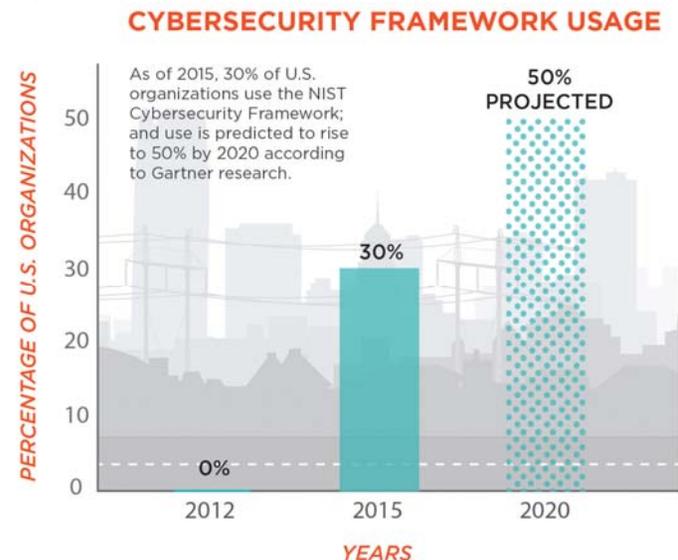


Cybersecurity Framework



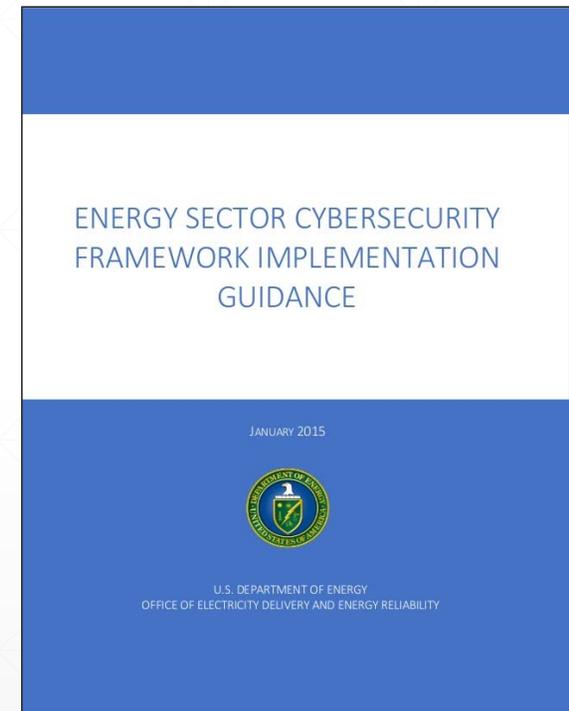
Cybersecurity Framework v1.1

- Released in April
- Clarifies use of Framework Components (i.e., Implementation Tiers and Profiles)
- Provides guidance on self assessment metrics and measurements
- Adds the concept of identity proofing and expands authorization
- Adds Supply Chain Category
- Now 23 Categories, 108 Subcategories
- Moving Informative References to an online database



Cybersecurity Framework and Regulation

- NIST's Frameworks complement, don't compete with most regulatory frameworks
- Some models are less prescriptive
- Others are quite specific but can align to the higher-level functions and categories



A Way of Seeing the Regulatory Environment

Regulator

- No surprises on rules or assessments
- Reduce engagement backlog
- Implementation of new rules by appropriate deadlines
- Fulfill government needs and satisfy citizens

***Clear
Communication***

***Efficient
Assessments***

***Efficient
Processing
of New Rules***

***Reduced
aggregate risk***

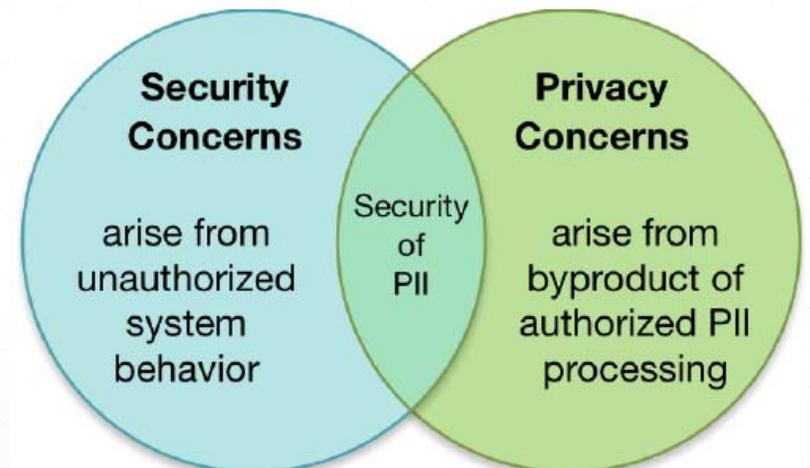
Regulated Entity

- Clearly understand rules and how to fulfill them
- Reduce compliance workload
- Quick integration of new rules into cybersecurity operation
- Achieve business objectives and gain customers



Privacy Framework

- Development of trustworthy information systems by –
 - applying measurement science and system engineering principles
- Kicked off on October 16th – lots of opportunity to participate in the one-year project
- Similar approach to NIST CSF



See: <https://www.nist.gov/privacy-framework>

Key Takeaways from Framework Implementation

- Go for the treat!
- Consider the goals of the organization, including those related to avoiding regulatory fines or contractual penalties
- Identify what's necessary and sufficient – across all areas – and make a plan to achieve and maintain that



Key Takeaways from Framework Implementation – Part II



- Beware a compliance-centric approach that may solve an immediate problem but doesn't really set one up for success in the long run
 - Work with managers, audit team, and implementers to understand how to comply through effective processes and practices
-

Great business results will be “in the bag”



- Cyber insurance providers tell us that organizations that improve their processes end up improving their bottom line as well by:
 - Avoiding risks the competitors don't
 - Avoiding compliance fines
 - Maintaining/Improving market share by protecting reputation and using cybersecurity as a differentiator

Thank you!

