



Keys to Operationalizing a Framework

About Us

Jeff Lemmermann	Bill Curtis	Paul Hender
CPA, CISA, CITP, CEH	CISSP, CISA, QSA, CCSP	CISSP, CISA, QSA
25+ Years IT/IS <ul style="list-style-type: none">• SynerComm• Precision Plus• CliftonLarsonAllen	30+ Years IT/IS <ul style="list-style-type: none">• SynerComm• CAT• Rockwell Automation	35+ Years IT 15+ Years Focused InfoSec <ul style="list-style-type: none">• SynerComm• ISO Federal level
Born and raised Wisconsinite	Midwestern (MI and WI)	Rolling Stone transplant

Agenda

- A Primer on Frameworks
- Framework Adoption
- Information Security Landscape

A PRIMER ON FRAMEWORKS

Why Adopt a Framework?

- Framework or Crash!

- Do you Fly?

- Pilot's pre-flight checklist
 - Plane mechanic repair and maintenance checklists



Are you checking your landing gear
AFTER you've taken off?

What will a Framework do?

For any organization:

- Ensure the process happens and is done the same way
 - Repetitive processes
 - Seldom occurring processes
- Adapts to changing environment
 - The most known are under constant development
- Thorough
 - Considers things you might miss if going at it alone...



What will a Framework do?

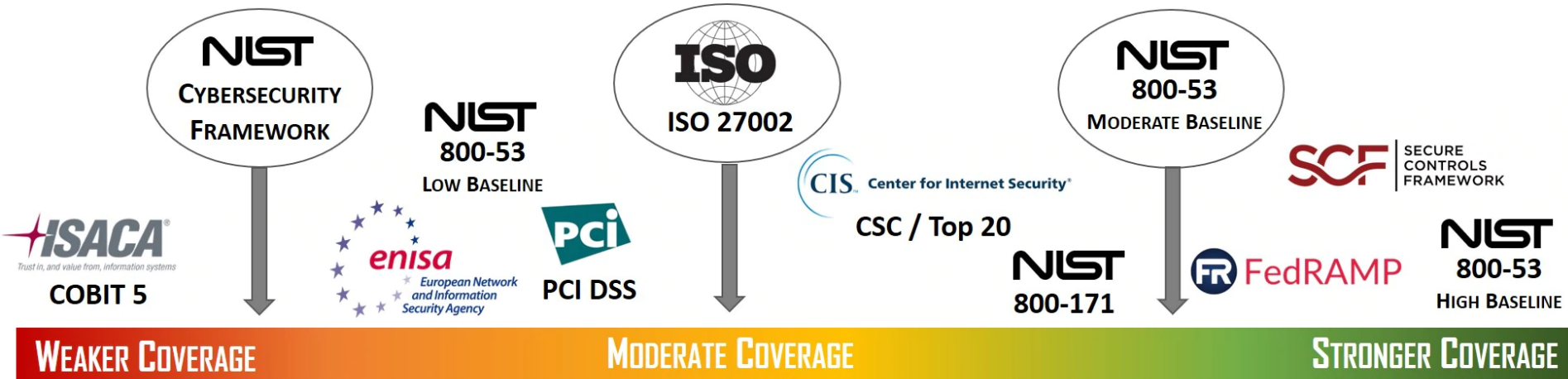
When properly implemented:

- Avoid or at the very least, minimize breaches
- Target 2013 Data Breach
 - 70 million customers affected
- NIST 800-53
 - AU-6: Audit Review, Analysis, and reporting
 - SE-1: Inventory of Personally Identifiable Information (PII)



Making it Relevant

- Guide to measure the organization's progress
- Standards for doing business and handling info



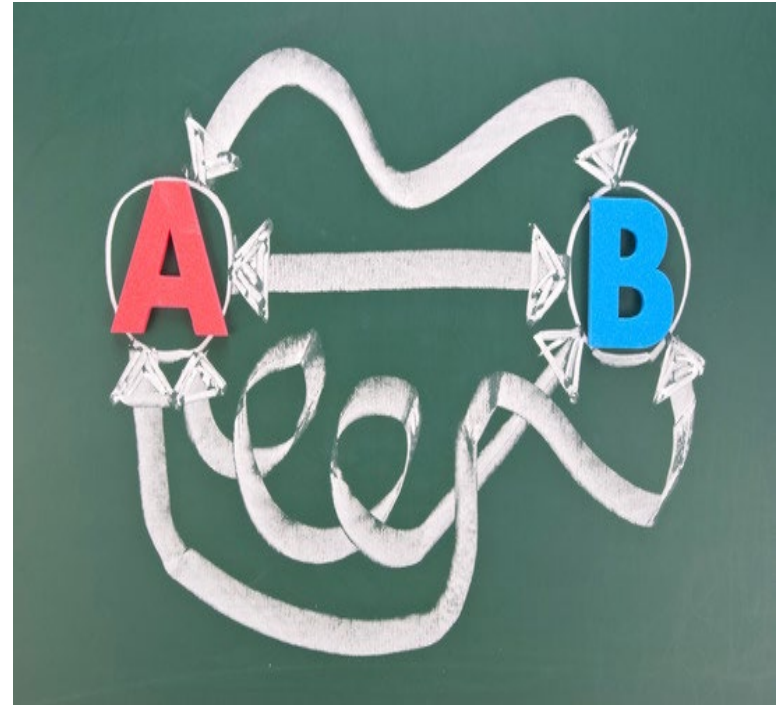
Effective today & in the future!

Technologies Change:

On Premise Servers moved to the cloud:

- User provisioning process
- Periodic review of accounts
- Monitoring privileged access

The map still works, just a different path to take



FRAMEWORK ADOPTION

Framework Adoption

- Q: Who is a framework for?
- A: Not just IT
 - Seek alignment with IT, IS, SDO (BU), and Leadership
 - Understand the total information systems picture
 - Support an effective communications strategy
 - Deliver meaningful outcomes

Framework Adoption

- Q: How can you overcome resistance?
- A: Market as 'business as usual'
 - Build on small victories (IT and strategic BU)
 - Workshop, lunch & learn, communications
 - Present relevant content to relevant groups

INFORMATION SECURITY LANDSCAPE

Where are We (thin ice)?




- Digital era – for a little while now
- Everyone wants to skate to where the puck will be... First - where are you, relevant to the puck?
 - Weekly, if not daily breaches
 - Climbing costs for breach fall-out, average 8.19M for each US breach (Yahoo – 117M, Equifax - ???)
 - Online customer experience: “That personal data you gave us? It’s been breached...”

Start Moving to That Point

- Standing still while the game is being lost around you – take action
- Get moving and take foundational actions
 - Document what you're doing (gives orientation relative to the puck)
- You will begin naturally drifting to that point on the ice where the puck is going to be



Where are We Going?

- Breach frequency and severity drivers 
 - Loss of 600+ GB of highly sensitive Military Data (one of many drivers for CMMC)
 - Loss of Electronic Library for Undersea Warfare
- HIPAA, FISMA, GDPR and now CMMC; NY and CA

Where are We Going?



- Looks like regulation is a safe bet
- Do Not Wait: Playing catch-up will cost more than just upgrades
- Select and adopt a NIST framework will aid in the coming compliance
- Holistic approach for success

THANK YOU
(questions)