CREATING A CLEAR 20/20 ERM VISION TO TAKE ON TOMORROW'S RISKS

AFERM
Association for Federal
Enterprise Risk Management

13TH ANNUAL ERM SUMMIT

AFERM
Association for Federal
Enterprise Risk Management

Integrating Cybersecurity & Enterprise Risk Management,

Breakout Session A-1
September 10, 2020; 1:00 PM - 2:00 PM EDT

Stephen Quinn, Computer Scientist at NIST
John Skober, NAVWAR Audit, Compliance and Controls Branch Head
Wm David Tillman, IT Security and Risk Executive at NCUA
Marshall Toburen, Risk Management Strategist, RSA (Moderator)

Panel: Self-Introductions

- Stephen Quinn, Computer Scientist at NIST
- John Skober, NAVWAR Audit, Compliance and Controls Branch Head
- Wm David Tillman, IT Security and Risk Executive at NCUA
- Marshall Toburen, Risk Management Strategist, RSA (Moderator)

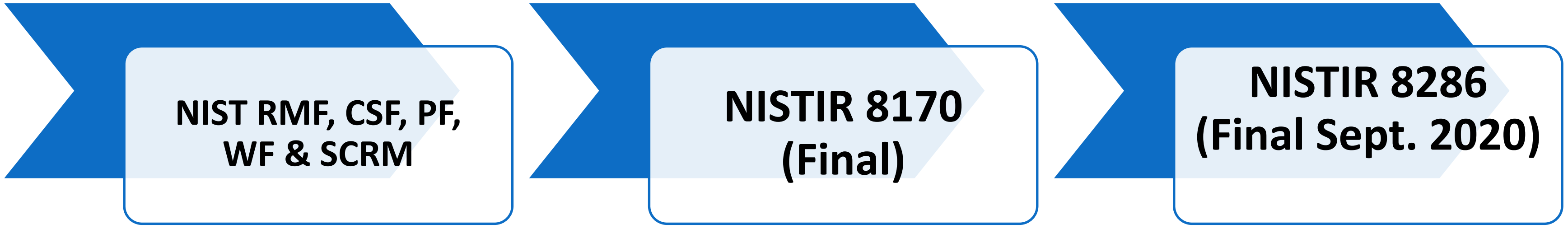
AFERM
Association for Federal
Enterprise Risk Management

NIST
CYBER

Anchoring NIST Risk Management Guidance in Enterprise Risk Management (ERM)

An overview of NISTIR 8170, NISTIR 8286 Series, and supporting tools

Integrating NIST RM with ERM Updates (slide 2)



NIST RMF, CSF, PF, WF & SCRM

NISTIR 8170 (Final)

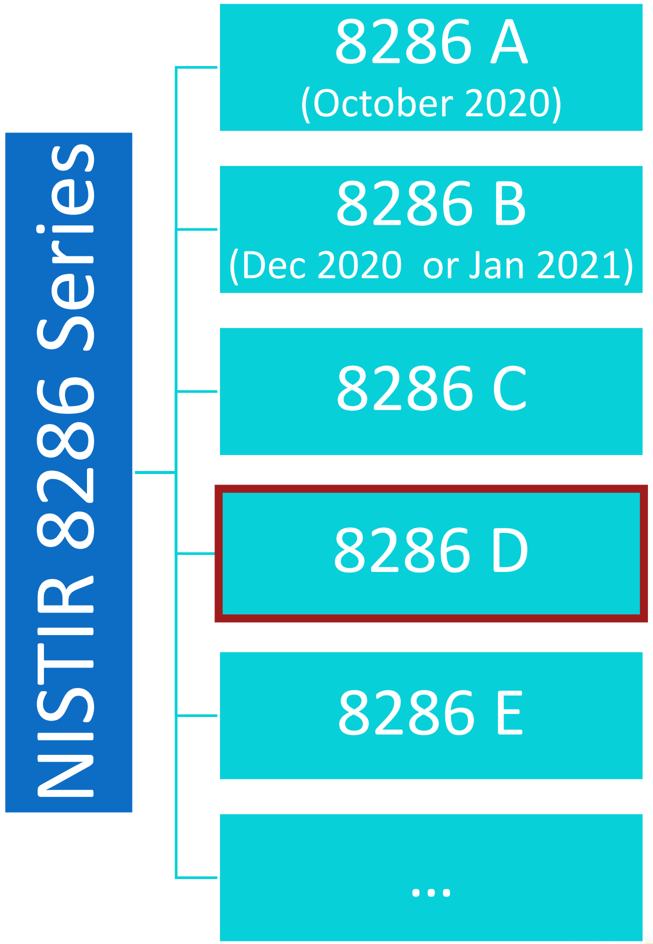
NISTIR 8286 (Final Sept. 2020)

Existing NIST documents and resources with different pedigrees, scopes, and audiences addressing individual disciplines of risk management.

A discussion of high-level ideas exploring touchpoints for integrating RMF, CSF, PF, and Workforce.

A specific discussion on using organizing constructs for integrating NIST Risk Management disciplines and ERM.

Holistic Risk Evaluation:



NISTIR 8286 Series

8286 A (October 2020)

8286 B (Dec 2020 or Jan 2021)

8286 C

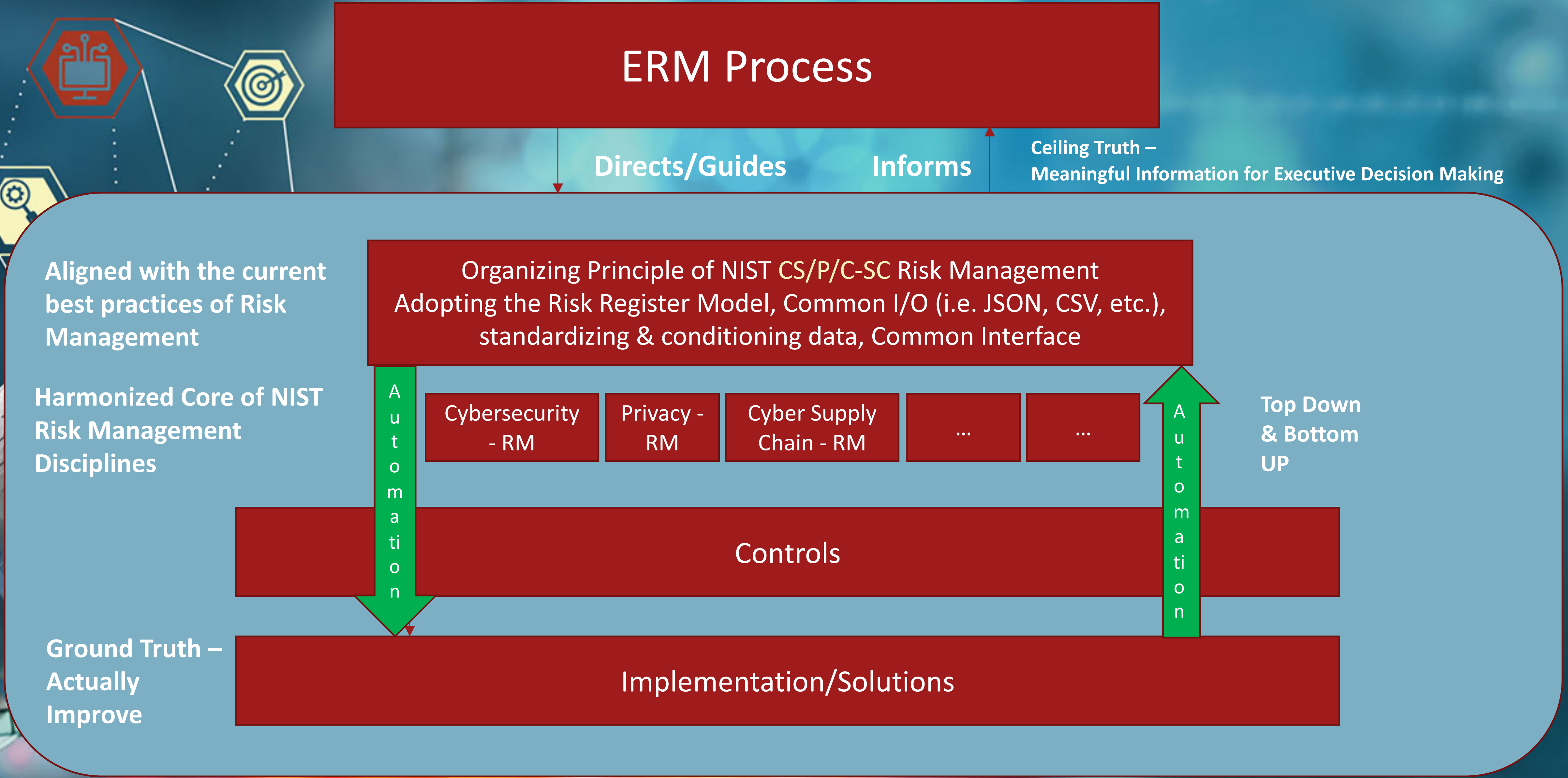
8286 D

8286 E

…

AFERM
Association for Federal
Enterprise Risk Management

NIST Risk Management Concept Model



ERM Process

Directs/Guides

Informs

Ceiling Truth –
Meaningful Information for Executive Decision Making

Aligned with the current best practices of Risk Management

Organizing Principle of NIST CS/P/C-SC Risk Management
Adopting the Risk Register Model, Common I/O (i.e. JSON, CSV, etc.), standardizing & conditioning data, Common Interface

Harmonized Core of NIST Risk Management Disciplines

Cybersecurity - RM	Privacy - RM	Cyber Supply Chain - RM	…	…

Top Down & Bottom UP

Controls

Ground Truth – Actually Improve

Implementation/Solutions

Polling Question

1. To What Degree is Cybersecurity Integrated with Your ERM Program?
    a. Don’t know / Not Applicable
    b. Not planning to integrate
    c. Just getting started with integration
    d. About half-way to integration
    e. Fully Integrated at this time

Panel Discussion: Considerations & Advice

- Audience Q&A
- What foundational issues should organizations address to begin the process of integrating cybersecurity and ERM?
  - *Taxonomy*
  - *Aligning Assessment Approaches (data security, privacy, etc.)*
  - *Risk Evaluation Consistency (risk appetite & tolerance decisions; and measurement metrics)*
  - *Prioritizing Risk Treatments*
  - *Unifying Reporting*
  - *Threat-sources vary (physical, electronic, errors, insider bad actors, third parties)*
- To fully integrate CS and ERM, should organizations take a phased approach? If so, what would phases look like?
- Any advice on breaking down CS silos, removing politics, and fostering collaboration?
- What if anything should organizations be able to demonstrate to evidence the design and effectiveness of their CS and ERM integration?

Polling Question

1. What is the biggest challenge to Integrating your Cybersecurity and ERM Program?
   a. Don’t know / Not Applicable
   b. Lack of commitment from Senior Management with broad enough domain of responsibility
   c. We can’t agree on risk management terminology
   d. We can’t find common risk assessment approach
   e. We can’t agree on standardized reporting
   f. Other (specify)

Final Comments

What is the most important piece of advice you can give the audience as they work toward integrating CS and ERM?

Q & A / Thank You!

Thank You!