TRUSTED CI

THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

trustedci.org

Trusted CI Framework

Bob Cowles

Virtual WISE Workshop

October 29, 2020

Trusted CI, the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Grant #1920430. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

What is a cybersecurity program?

A cybersecurity program is a group of related cybersecurity-focused projects and ongoing activities managed in a coordinated way **to obtain benefits not available from managing them individually**. Cybersecurity programs are an organ of the larger organization, living as part of that organization through its lifecycle.

→ Adapted in part from Schwalbe, Information Technology Project Management, 9th Edition.

A Program is more than a control set

- Controls are **specific administrative, technical, and physical safeguards and countermeasures**.
- A cybersecurity **control set** describes a group of controls that might be appropriate defaults for a given environment e.g., CIS Controls, NIST SP 800-53, NIST SP 800-171, ISO
- These are important, but there is more to a program.

Why approach cybersecurity programmatically?

Cybersecurity…

- is dynamic, complex, and multidisciplinary.
- is always relevant, no start and end

Supports…

- project management of projects and activities across time.
- clear roles, responsibilities, accountability, communication.
- resourcing and prioritization of efforts.

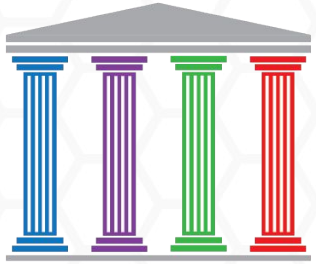
Motivations for Yet-Another-Framework

- Existing process frameworks tend to be expensive, incomplete, or impractical to implement effectively.
- Many policy-makers, leaders, and auditors confuse starting and maintaining a competent program with implementing a set of controls. You have to have the first to do the second.

Trusted CI Cybersecurity Program Framework for Open Science Projects and Facilities

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Pillars



Mission Alignment

- Mission focus, external obligations, asset inventory, information classification

Governance

- Roles and responsibilities, policies, program evaluation

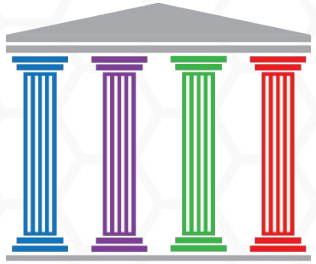
Resources

- People, budgets, services and tools

Controls

- Procedural, technical, administrative safeguards and countermeasures

Framework "Musts"



- Sixteen (16) concise, clear minimum requirements for cybersecurity programs.
- Based on cybersecurity best practices and evidence of what works.
- Emphasize programmatics that are too-often ignored or assumed.
- Infrequent updates.

Framework Musts (Mission Alignment)

1. Organizations must tailor their cybersecurity programs to the organization's **mission**.
2. Organizations must identify and account for cybersecurity **stakeholders and obligations**.
3. Organizations must establish and maintain **documentation** of information assets.
4. Organizations must establish and implement a **structure for classifying** information assets as it relates to the organization's mission.

Framework Musts (Governance)

5. Organizations must involve **leadership** in cybersecurity decision making.
6. Organizations must formalize roles and responsibilities for cybersecurity **risk acceptance**.
7. Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
8. Organizations must ensure the cybersecurity program **extends to all entities** with access to, control over, or authority over information assets.
9. Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policy**.
10. Organizations must **evaluate and refine** their cybersecurity programs.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Musts (Resources)

11. Organizations must devote **adequate resources** to mitigate cybersecurity risks deemed unacceptable by the organization.
12. Organizations must establish and maintain a cybersecurity **budget**.
13. Organizations must allocate **personnel** resources to cybersecurity.
14. Organizations must identify **external cybersecurity resources** to support the cybersecurity programs.

Framework Musts (Controls)

15. Organizations must adopt and use a **baseline control set**.
16. Organizations must select and deploy **additional and alternate controls** as warranted.

Framework Core

- Relatively stable, infrequent updates
- A statement of the Must and a paragraph that "unpacks" the language of the Must answering "What?"

Must 15:

Organizations must adopt and use a **baseline control set**.

Controls are specific administrative, technical, and physical safeguards and countermeasures applied to reduce cybersecurity risk. A baseline control set is a predetermined set of controls used as a default when selecting security controls for information assets. The baseline control set does not determine what security controls an organization must implement; rather, it provides a foundation from which an organization tailors control selection based on the needs of its mission. Baseline control sets vary in the number, specificity, and goals of the controls it describes. Baseline control sets may be legally imposed when handling specific types of data. In other cases, organizations can select a well-maintained control set that is based on evidence of what works to reduce cybersecurity risk.

Framework Implementation Guide (FIG)

- A FIG is an community-specific **roadmap** for how an organization could begin implementing the 16 Musts. A given community may have more than one good path, but almost certainly has a lot of bad ones.
- FIGs are expected to be updated much more frequently (at least annually).
- A diverse, representative Framework Advisory Board (FAB) of community experts helps ensure the FIG guidance is grounded and clear.

And the First FIG is for …. Research Cyberinfrastructure Operators (RCOs)

RCOs are organizations that operate on-premises, cloud-based, or hybrid computational and data/information management systems, scientific instruments, visualization environments, networks, and/or other technologies that enable knowledge breakthroughs and discoveries.

These organizations include, but are not limited to, major research facilities, research computing centers within research institutions, and major computational resources that support research computing.

FIG Development

- Parallel development, review, and revision efforts
- Feedback from the FAB has been very valuable
- Five groups of content

The Content Groups

CG1: Front material (Exec Summary, Introduction), Must 15 (Baseline)

CG2: Musts 3 (Inventory), 4 (Categorize), 16 (Additional Controls)

CG3: Musts 2 (Stakeholders), 12 (Budgets), 14 (Tools & Services)

CG4: Musts 1 (Mission), 5 (Leadership), 6 (Risk Acceptance), 7 (Lead)

CG5: Musts 8 (Extend), 9 (Policy), 10 (Evaluate), 11 (Adequate), 13 (Personnel)

FIG Development Status and Timeline

- Content Groups 1 and 2:Reviewed by the FAB and revised.
- Content Groups 3 and 4:Reviewed by the FAB and being revised
- Content Group 5 is being developed and to FAB on 11/11 for review
- Publication of FIG in late January 2021
- Trial implementation of Framework first half of 2021

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Thanks - Any questions?

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE