Outcomes of the Trusted CI Cybersecurity Framework HPC Cohort

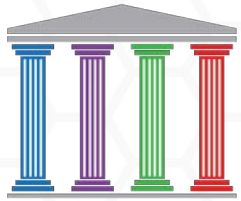
4th High-Performance Computing Security Workshop

Jim Basney
Principal Research Scientist, Cybersecurity, NCSA, UIUC
Director and PI, Trusted CI
jbasney@ncsa.illinois.edu

May 21, 2024

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Outline



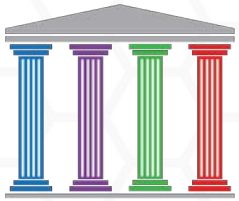
1. Trusted CI: Introduction
2. Trusted CI Framework for cybersecurity programs
3. Highlights of the Trusted CI Framework
4. Adopting the Trusted CI Framework
5. Trusted CI Framework HPC Cohort (Delta)

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI

An Introduction

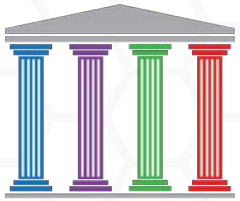
Trusted CI: An Introduction



1. Trusted CI is the NSF Cybersecurity Center of Excellence
   - Established in 2012
   - Collaboration between IU, UIUC, PSC, LBL, and UW:M.
   - Currently on a 5 year cooperative agreement with the NSF
   - We work with the NSF community to improve the cybersecurity of cyberinfrastructure
2. **Our goal**: Help NSF cyberinfrastructure operators build effective cybersecurity programs
   - Assessments, trainings, consultations, cohorts, recommendations, community events, etc.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Community Resources



Ransomware
https://www.trustedci.org/ransomware

Research Transition to Practice
https://www.trustedci.org/ttp

Identity and Access Management
https://www.trustedci.org/iam

Software Assurance
https://www.trustedci.org/software-assurance

Operational Technology
https://www.trustedci.org/operational-technology

Science DMZs
https://www.trustedci.org/science-dmz

Trustworthy Data
https://www.trustedci.org/trustworthy-data

Compliance Programs
https://www.trustedci.org/compliance-programs

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF Cybersecurity Summit

- October 7-10, 2024 at CMU in Pittsburgh, PA
- Program agenda is community-driven based on responses to community polling, session proposal submissions, and trending topics
- Summit format includes:
  - Plenary sessions
    - Presentations
    - Panel discussions
    - Lightning talks
  - Workshops and training
  - BoFs and “Community of Practice” meetings (TLP)
  - Student program and Poster session

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

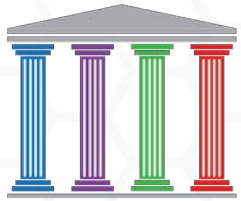
https://trustedci.org/summit

The Trusted CI Framework

An Overview

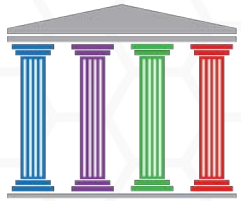
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity Programs



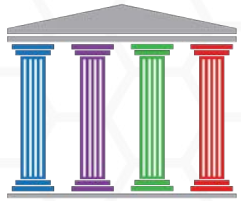
1. We regularly conduct assessments, trainings, consultations, and other types of engagements with a wide range of organizations.
2. The primary challenges organizations face with cybersecurity are not technical: They are on programmatic elements.
   a. Money
   b. Governance
   c. Leadership Involvement
   d. Mission Alignment
3. Organizations lack guidance on how to address these non-technical elements

Cybersecurity Programs



1. Many organizations anticipate incoming cybersecurity compliance
    a. Controlled Unclassified Information & NIST SP 800-171
    b. Cybersecurity Maturity Model Certification
    c. National Security Presidential Memorandum 33
    d. FISMA
2. These compliance control sets typically focus on technology, and don't address those key enablers of cybersecurity.
3. Without a cybersecurity program, organizations often don't even know where to begin when handed a cybersecurity control set.

The Trusted CI Framework



The Trusted CI Framework establishes a **minimum standard** for cybersecurity programs.

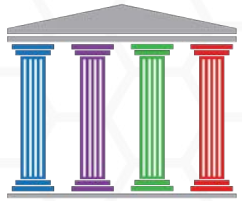
- 16 clear and concise requirements.
- Based on best practices and evidence of what works.
- Designed to be universal and timeless.

It focuses on cybersecurity programmatics: Mission Alignment, Governance, Resources, and Controls.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Highlights

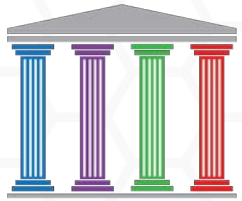
Framework Highlights: Must 5



Involve leadership in cybersecurity decision making

1. Responsibility. It is a basic principle (and often law) that these people are ultimately responsible for the organization. Some, but not all responsibility can be delegated.
2. Power. Senior leaders ultimately control the allocations of resources, budget, and personnel to support the cybersecurity program.
3. Perspective. Leaders in these roles are in the best position to adjudicate competing demands for resources across the organization, to include how much to prioritize cybersecurity.

Framework Highlights: Must 7



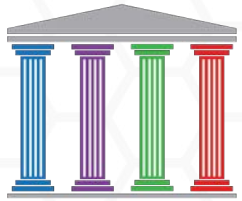
Establish a lead role with responsibility to advise and provide services to the organization on cybersecurity matters

Why is this a Must? For the same reasons you need health care providers to help you take care of your body.

1. Complexity. Cybersecurity is a complex, changing, and challenging function in any organization.
2. Impact. Cybersecurity incidents and issues can impact any part of an organization, and bring business to a halt.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Highlights: Must 12

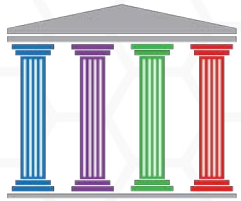


Establish and maintain a **cybersecurity budget**

Why is this a Must?

1. Informs Decision Making. Knowing how much you are spending helps evaluate the program's benefit to the mission.
2. Transparency & Rigor. Make explicit how much you are spending on cybersecurity, and have leadership approve it.
3. Organizational Commitment. A dedicated budget shows that leadership is committed to support the cybersecurity program.

Framework Highlights: Must 15



Adopt and use a **baseline control set**

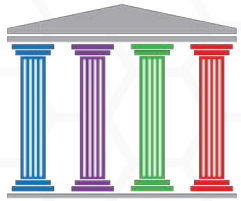
You need a well-rounded diet of known-good controls.

1. Rally! Common language and structure.
2. Save resources. It relieves the resource burden of ad hoc control selection and wasted effort "reinventing the wheel."
3. Avoid gaps. A major risk of ad hoc control selection is missing important, doable controls.
4. Good baseline protection. Will address the majority of attacks.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Adoption

Resources



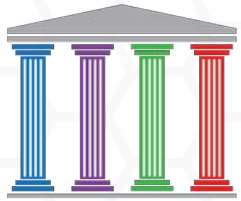
Framework Implementation Guide (FIG)

1. In-depth, audience specific guidance
2. Roadmaps, common challenges, and key resources
3. Available at: https://www.trustedci.org/framework/implementation

Templates and Tools:

1. Master Information Security Policy & Procedures
2. Incident Response Policy
3. Cybersecurity Program Strategic Plan
4. Available at: https://www.trustedci.org/framework/templates

Framework Cohorts



Overview:

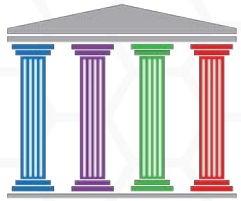
1. **Period**: 6 months
2. **Group engagement**: 4-6 organizations
3. **Goal**: Framework Adoption & Implementation

Strengths

1. Learn from/with fellow organizations
2. In-depth Trusted CI guidance
3. Lower time commitment than a full assessment

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Cohorts (cont.)



Outcomes:

1. **Framework Adoption:** Organizations will adopt the Framework.
2. **Program Evaluation**: Organizations will develop a validated self-assessment of their cybersecurity program.
3. **Strategic Plan**: Organizations will draft a Cybersecurity Program Strategic Plan that:
    i. Connects cybersecurity to the mission
    ii. Defines a cybersecurity strategy
    iii. Set out a timeline of milestones

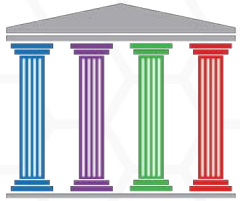
Participants

1. Cohort Alpha
   a. GAGE, LIGO, NOIRLab, NRAO, NSO, OOI
2. Cohort Bravo
   a. CENIC, FABRIC, NEON, SAGE
3. Cohort Charlie
   a. ARF, DSE, IceCube, GMTO, NAN, USAP
4. Cohort Delta
   a. NCSA, PSC, SDSC, TACC, UCAR
5. Cohort Echo
   a. CXFEL, ICPSR, MagLab, Simons Observatory, SPHERE, TMT

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Cohort Delta

About Cohort Delta



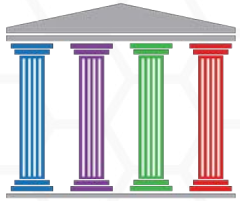
Participants: NCSA, PSC, SDSC, TACC, UCAR

Inspiration: Panel at 3rd HPC Security Workshop

Information Sharing: Chatham House Rule and Traffic Light Protocol

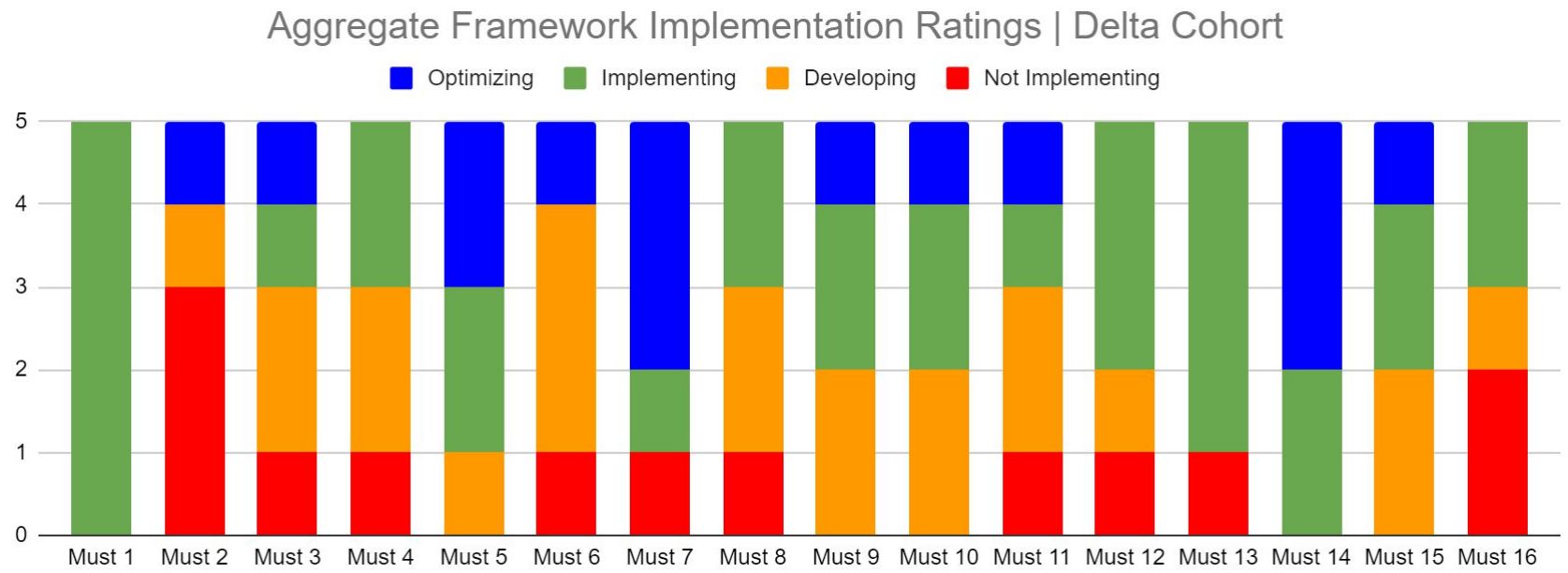
Dates: July 2023 - December 2023

Cohort Delta Takeaways



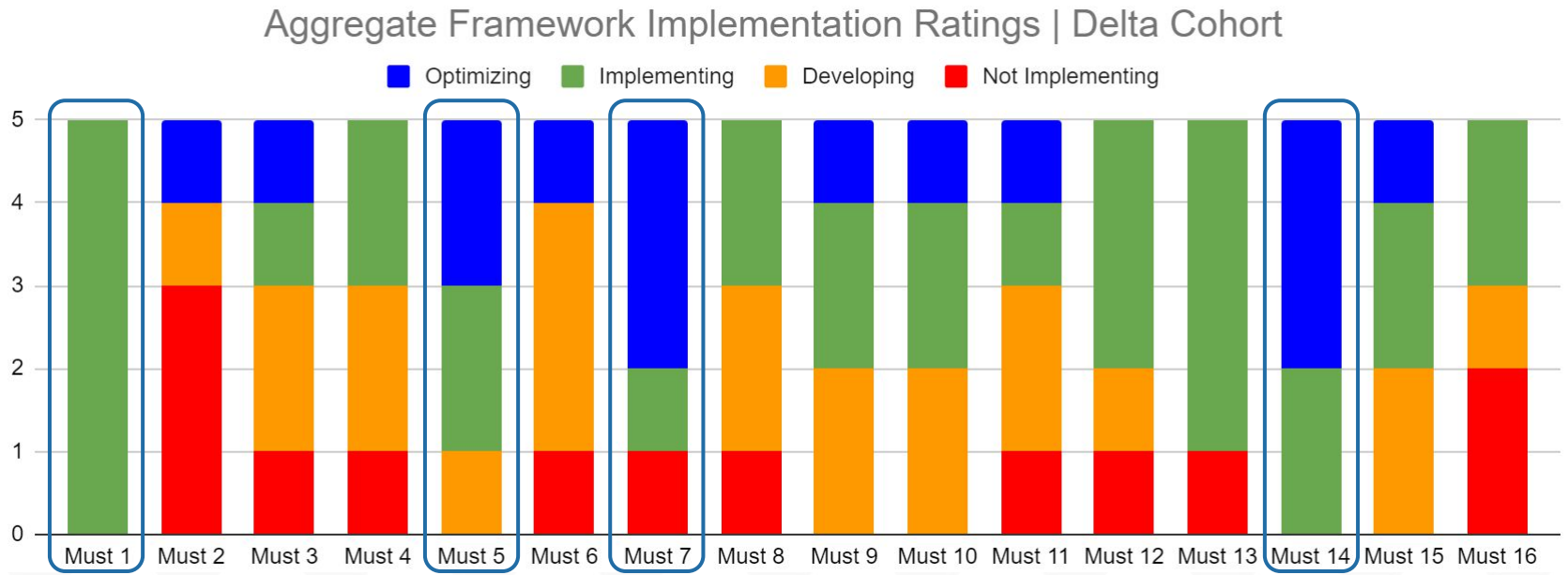
- Peer information sharing / peer assessments
- Understanding connections with parent organizations
- Comparing staffing levels and responsibilities
  - Dedicated cybersecurity staff
  - Sysadmins with cybersecurity responsibilities
  - Cybersecurity is a shared responsibility
- Baseline control sets: 800-53, 800-171, CIS
- Strategic priorities:
  - Baseline control set implementation
  - Managing stakeholders and obligations
  - Asset tracking

1: Mission Focus
2: Stakeholders & Obligations
3: Information Assets
4: Asset Classification
5: Leadership
6: Risk Acceptance
7: Cybersecurity Lead
8: Comprehensive Application
9: Policy
10: Evaluation & Refinement
11: Adequate Resources
12: Budget
13: Personnel
14: External Resources
15: Baseline Control Set
16: Add'l & Alternate Controls



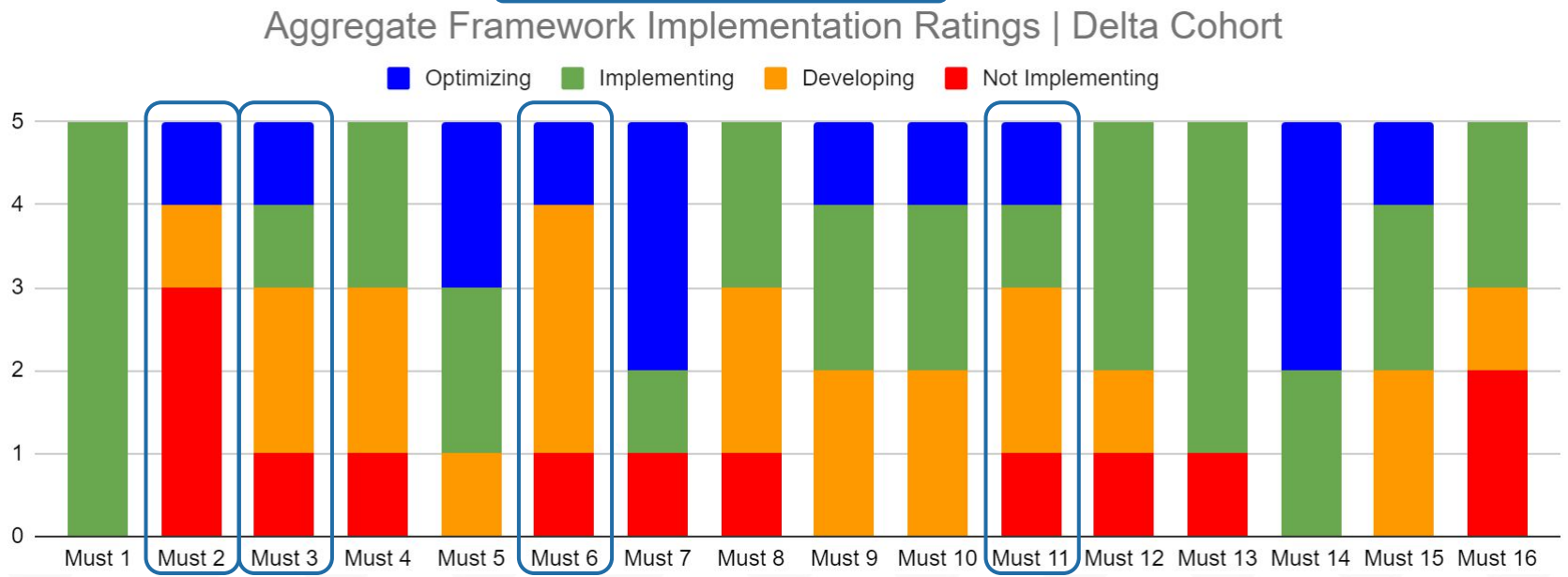
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

1: Mission Focus
2: Stakeholders & Obligations
3: Information Assets
4: Asset Classification
5: Leadership
6: Risk Acceptance
7: Cybersecurity Lead
8: Comprehensive Application
9: Policy
10: Evaluation & Refinement
11: Adequate Resources
12: Budget
13: Personnel
14: External Resources
15: Baseline Control Set
16: Add'l & Alternate Controls



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

1: Mission Focus
2: Stakeholders & Obligations
3: Information Assets
4: Asset Classification
5: Leadership
6: Risk Acceptance
7: Cybersecurity Lead
8: Comprehensive Application
9: Policy
10: Evaluation & Refinement
11: Adequate Resources
12: Budget
13: Personnel
14: External Resources
15: Baseline Control Set
16: Add'l & Alternate Controls

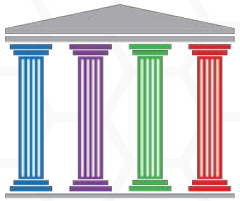


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Next Steps

- Re-engage to check and promote progress
- Share updates in implementations
- Research Infrastructure Security Community (RISC)
- NSF Research Infrastructure Workshop
- NSF Cybersecurity Summit

Thanks!



Thanks to the Cohort Participants and Trusted CI staff.

Trusted CI, the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Grant #2241313. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

https://trustedci.org/ info@trustedci.org jbasney@ncsa.illinois.edu

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE