Cybersecurity That Works

The Trusted CI Framework

Craig Jackson
Program Director, IU CACR
Senior Personnel, Trusted CI

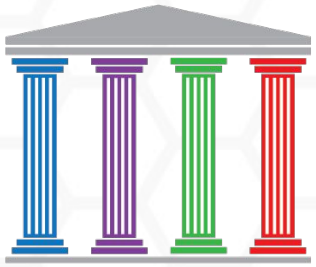
… with Leyna and Vesper

SIG-ISM - WISE Workshop
25 May 2021

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Trusted CI Framework

4 Pillars, 16 Musts



The Trusted CI Framework helps organizations establish and refine **cybersecurity programs** that work.

It focuses on often neglected programmatic fundamentals across 4 Pillars: **Mission Alignment**, **Governance**, **Resources**, and **Controls**.

This is not yet another long list of technical requirements.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Musts One-Pager

https://trustedci.org/framework/M1P

The Trusted CI Framework

Four Pillars. Sixteen Musts. An Architecture for Cybersecurity Programs

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 they relate to the organization's mission.

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.

Resources

11. Organizations must devote **adequate resources** to address unacceptable cybersecurity risk.
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.

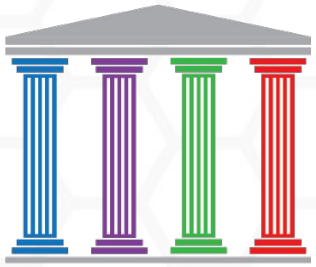
Controls

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

Visit www.trustedci.org/framework to learn more.

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.

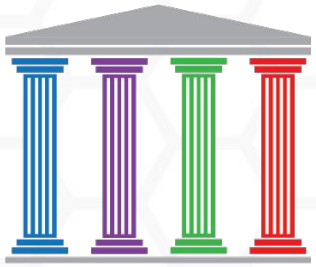
→ Adapted in part from Schwalbe, Information Technology Project Management, 9th Edition.

A cybersecurity program is not...

- A “plan”
- A “project”
- Doing a set of “controls” (like the CIS Controls, NIST CSF, NIST 800-53, NIST 800-171, ASD Essential Eight) you are supposed to implement

The Trusted CI Framework complements and puts all of these in context.

Framework Implementation Guide for Research Cyberinfrastructure Operators



Go to https://www.trustedci.org/framework and hit the **green button**. The guide gives research organizations a community-tailored head start on choosing among good paths and avoiding treacherous ones.

Includes:

- roadmaps for establishing mature cybersecurity programs
- tailored advice on overcoming common challenges
- pointers to resources, including our publicly available tools and templates

Built by Trusted CI's experienced multi-institutional team, and vetted by a Framework Advisory Board representing the diversity of our community.

Replaces 2014's Guide.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Framework Core

About

Framework Core

Implementation Guidance

Templates and Tools

Share Your Feedback

DOWNLOAD THE FRAMEWORK IMPLEMENTATION GUIDE

The Trusted CI Framework is structured around **4 Pillars** which make up the foundation of a competent cybersecurity program: **Mission Alignment, Governance, Resources, and Controls**. Composing these pillars are **16 Musts** that identify the concrete, critical requirements for establishing and running a competent cybersecurity program. The 4 Pillars and the 16 Musts make up the **Framework Core**, which is designed to be applicable in any environment and useful for any organization.

Mission Alignment

Must 1: Mission Focus

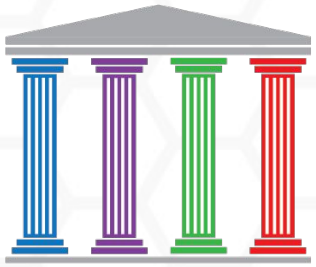
Organizations must tailor their cybersecurity program to the organization's mission.

Cybersecurity is not undertaken as an end unto itself: the ultimate goal of a cybersecurity program is to support the organization's mission. "The mission" is the foundational motivating force driving decision making: it is made up of the task(s), purpose(s), and related action(s) that the organization treats as most important or essential. The program's implementation must account for the positive and negative impacts security can have on the organization's mission.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

trustedci.org/framework/core

Getting Started



Check out trustedci.org/framework/core. This briefly explains the **16 Musts**. For each, ask yourself:

Have we addressed this?
If not, why not?
If so, how's it working out?

Hit the green button to grab the guide, and share with your team and leadership.

Check out FIG p.7 → One page start-up suggestions.

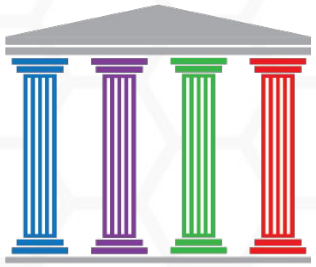
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Next Steps for Trusted CI

1) Working with NOIRLab on assessment and adoption right now. (First time using TCIF / FIG as the sole standard for an assessment.)
2) Looking for additional opportunities for assessments, consultations, training, feedback, collaboration.
3) We will revise the FIG regularly and expand/refresh the available tools.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Acknowledgments



Special thanks go to our Framework Advisory Board (FAB). The members are: Kay Avila (NCSA); Steve Barnet (IceCube); Tom Barton (University of Chicago); Jim Basney (NCSA); Jerry Brower (NOIRLab, Gemini Observatory); Jose Castilleja (NCAR/UCAR); Shafaq Chaudhry (UCF); Eric Cross (NSO); Carolyn Ellis (Purdue University); Terry Fleury (NCSA); Paul Howell (Internet2); Tim Hudson (NEON/Battelle/Arctic); David Kelsey (UKRI/WISE); Tolgay Kizilelma (UC Merced); Nick Multari (PNNL); Adam Slagell (ESnet); Susan Sons (IU CACR); Alex Withers (NCSA/XSEDE); Melissa Woo (Michigan State University). Thanks to our Framework Advisory Board Governance and Collaboration Leads: Andrew Adams and Von Welch.

Many thanks to current and past collaborators Kay Avila, Jim Marsteller, Kelli Shute, Susan Sons, Rebecca Yasky, John Zage, and the entire membership of the Large Facilities Security Team (https://www.trustedci.org/lfst). Their past work on this and related projects have had an important impact on the architecture and content of the Framework.

This presentation, the Trusted CI Framework, and the Framework Implementation Guide are products of Trusted CI, the NSF Cybersecurity Center for Excellence. Trusted CI is supported by the National Science Foundation under grants numbered OCI-1234408, ACI-1547272, and ACI-1920430. For more information about Trusted CI, please visit https://www.trustedci.org/. 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, the Framework Advisory Board members, or their respective organizations.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE


TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.org