
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.org

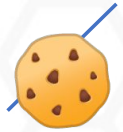
# The Policy Lifecycle
## More than Words


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

CACR Brown Bag
11 Sep 2020

CCoE Pilot IDM Working Group
14 Sep 2020

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



# Trusted CI:
# The NSF Cybersecurity Center of Excellence

Our mission: to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

INTERNET2

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

PITTSBURGH SUPERCOMPUTING CENTER

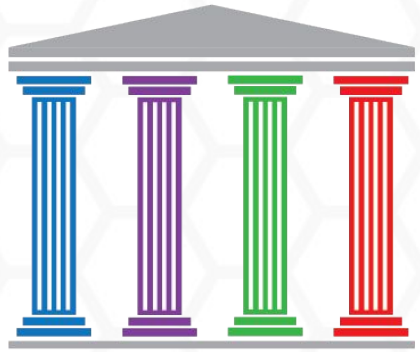
BERKELEY LAB

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/

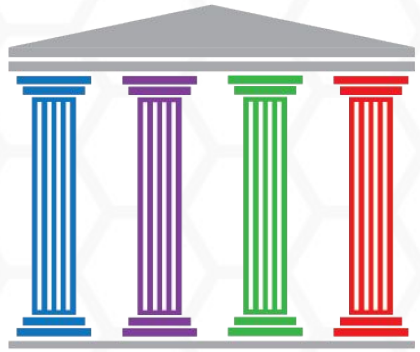
# The Trusted CI Framework

# Motivations



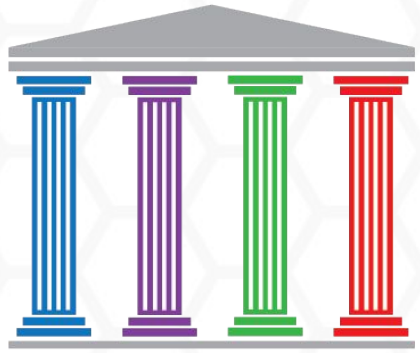
1. The cybersecurity community generally lacks a comprehensive, comprehensible minimum standard for cybersecurity **programs**.
2. Existing process frameworks tend to be expensive or impractical to implement effectively.
3. Many auditors, leaders, and policy-makers confuse implementing a bunch of controls with standing up and maintaining a competent program. You have to have the latter to do the former competently.

# Goals



1. Develop an initial **Framework Implementation Guide** oriented toward research cyberinfrastructure operators (RCOs).
2. Put other frameworks and controls sets in perspective. Arm the community with a minimum standard for a competent, mission-focused cybersecurity program.
3. Achieve early adoption by a diverse set of stakeholder institutions and facilities.
4. Achieve acceptance by NSF, project leads, CIOs, CISOs.

# Architecture



**The Musts**

- Sixteen (16) concise, clear minimum requirements for cybersecurity programs organized under the 4 Pillars: Mission Alignment, Governance, Resources, and Controls
- Based on cybersecurity best practices and evidence of what works.
- Emphasizes programmatics that are too-often ignored or assumed.
- Infrequent updates.

**Framework Implementation Guides (FIGs):**

- Guidance vetted by and tailored to a particular community.
- Curated pointers to the very best resources and tools.
- Frequent (at least yearly) updates.

# Governance:

**Must 9**. Organizations must develop, adopt, explain, follow, enforce, and revise **cybersecurity policy**.

How much policy is enough?
How much policy is known to cause cancer in lab rats?

# Policy Development

You may not need a ton of written policy, but you need some.

Results in:

- Reproducible, communicable, and enforceable policy and processes
- Artifacts that can be critiqued and evolved

# The Policy Lifecycle ©

(DAEFER?... Without "adopt" it's just DEFER.)

1. *Develop*
2. *Adopt*
3. *Educate*
4. *Follow*
5. *Enforce*
6. *Revise*

The policy valley of death

# Leading questions…

# Develop

Policies don't emerge magically from some event horizon. People develop them, even if that means slightly modifying a template.

1. Are their people in your organization who are experienced in developing policy? If so, are they involved in developing cybersecurity policies?
2. Are there templates or other guidance to help people develop adoptable, enforceable policies?
3. Are the stakeholders for a policy involved in its development? If so, how? If not, why not?
4. Are policies written in a way so that the people to whom they apply know who they are?
5. Are policies written such that people will understand the difference between suggestions and hard requirements?
6. Is it clear where to go to ask for exceptions?

# Adopt

If a policy is developed, but never adopted, is it a policy of the organization? No. Is it enforceable? Probably not. The policy valley of death starts here. Some organizations expend the effort to develop cybersecurity policies, and they never achieve adoption.

1. Is there a formalized process for adopting enforceable policies? If so, is it followed?
2. Have appropriate stakeholders (*e.g.*, HR professionals) reviewed enforcement provisions?
3. Is it clear to the people developing policy who has the power to adopt that policy?
4. Do policies have documented adoption dates?
5. Is there a history of success or failures to getting policies from development into actual adoption?

# Educate

Notice is a practical (and often ethical) requirement for any enforceable policy. Moreover, people are much more likely to follow policy if they understand not only where, but what that policy is.

1. Are policies readily available to the people to whom they apply? How and when is that availability and location communicated?
2. Do people have to acknowledge receipt or reading of any policies? If so, which policies and people?
3. Do people receive training on policies? If so, how, when, and how often? If not, why not?

# Follow

This is especially important and frequently an issue for people with power, control, or access.

1. Is there a history of people or roles (e.g., leadership) ignoring adopted policy? If so, which policies and which people?

# Enforce

Many organizations struggle with enforcement, but a policy that is never enforced is (at best) a suggestion, and (at worst) a serious liability.  Enforcement is about more than people getting in trouble; it includes simple reminders, education, limiting access or putting controls in place, and correcting honest mistakes.

1. Do adopted policies include (or include by reference) enforcement provisions?
2. Are policies actually enforced?
3. Are policies enforced consistently?
4. Do policies have explicit provisions regarding the who, what, when, how, and why of policy exceptions?

# Revise

Environments can change dynamically; policies cannot.  Revision is an opportunity to update, correct, and improve existing policies.

1. Are policies reviewed or opened for revisions with any regular frequency, as needed, or at all?  Is there a formal process?
2. Are superseded policies marked, archived, or otherwise handled in such a way as to communicate the valid, active version?
3. Are there any policies that are so far behind the times that they need to be deprecated or completely overhauled?

# **Policy Development & Revision:** Tips and Gotchas

## Please do:

1. Involve stakeholders (yes, even the relevant lawyers)
2. Prioritize
3. Use templates, examples
4. Ask for help
5. Share the resulting policies and train your personnel
6. Include instructions for requesting exemptions

## Please don't:

1. Fall into the policy valley of death
   a. Allow policies to be developed and filed away without a formal approval process
   b. Assume people will read them without training/education
   c. Develop policies no one can or will enforce
2. Be afraid to take this seriously
3. Underestimate the power of v2

# Templates!

Check out templates at:

https://trustedci.org/guide

(coming soon) https://trustedci.org/framework

Cautionary Note: You will *have to* make these your own.

# Discussion / Questions / Commiseration

# Thank you!

This training is a product of the Trusted CI, the NSF Cybersecurity Center of Excellence. Trusted CI is supported by the National Science Foundation under Grants Numbered OCI-1234408, ACI-1547272, and ACI-1920430. For more information about the Trusted CI, please visit https://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.

info@trustedci.org
scjackso@iu.edu

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE