PACT Assessments

Mission-focused, holistic, actionable cybersecurity assessments for decision makers

CENTER FOR APPLIED CYBERSECURITY RESEARCH

Innovation Center
2719 E. 10th Street, Suite 231
Bloomington, IN 47408
Phone: 812.856.0458
Fax: 812.856.7400

Cybersecurity is so much more than a technical problem. Cybersecurity assessments need to address the practical, organizational realities that are preventing our organizations from figuring out what, how, and how much to do.

PACT cybersecurity assessments focus on mission success, not checklist compliance. We look at your organization with the understanding that cybersecurity can be either a burden or an enabler. We then deliver actionable recommendations for operational personnel and lay out strategic priorities for leadership. Our partners use our assessment reports to guide their cybersecurity activities for years.

> *Based on your recommendations we have decided to revisit our cybersecurity strategy from the top down....Thanks for all your efforts—and in helping us take a different perspective.*
>
> **—Rich Ceci, senior vice president for technology and projects, Port of Virginia**

Methodology

The PACT methodology is collaborative and non-invasive. It was developed by CACR subject matter experts for the US Navy and has been successfully applied in diverse operational environments. The methodology is based heavily on assessments conducted in 13 prior engagements through the NSF Cybersecurity Center of Excellence and US Navy. It has been proven by two congressionally funded, DoD-sponsored pilots, most recently at the Port of Virginia in collaboration with the United States Coast Guard.

PACT assessments are:

- **Mission-focused:** We emphasize security's value to the mission, not just whether you've checked all the right boxes.
- **Practical:** We find a security path that makes sense given your organization's constraints.
- **Holistic:** We assess all aspects of cybersecurity, not narrowly focusing on technology.
- **Advisory:** We provide highly usable guidance, not just a description of the problem.
- **Understandable:** We write for non-technical decision makers, avoiding jargon and focusing on fundamentals.
- **Collaborative:** Our assessments are non-invasive. We don't "plug in" or try to "break into" your systems.

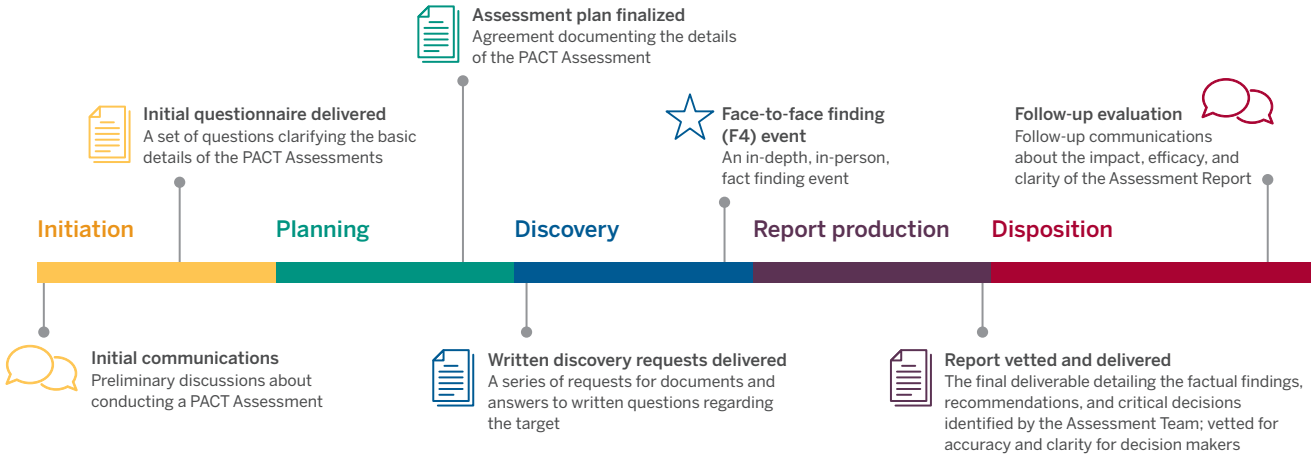
For more information, please contact **cacr@iu.edu** or visit **cacr.iu.edu/pact**

PACT Assessments

cacr.iu.edu/pact

Phases and milestones

PACT assessments follow the collaborative phases shown.



Assessment levels

Our assessments are scalable in terms of calendar time and overall effort. All PACT assessments take a broad, holistic view of the organization's cybersecurity strategy and operations. Larger assessments allow our teams to dive deeper into the complexities and details of mission alignment, governance, resourcing, threat identification, and security control selection and implementation. We consider three tiers as starting points to tailor PACT assessments to customer needs.

Assessment tier	Execution period*	Benefits	Deliverables	Best for
BASELINE *This is the annual exam with your internist.*	30 days	• An understanding of the maturity and major gaps in your cybersecurity program. • Actionable guidance on how to build an effective, efficient cybersecurity program.	• A well-written report with a programmatic maturity rating, strategic roadmap, 10–15 detailed recommendations, and a one-page executive summary. • A briefing for senior leadership.	Organizations with fledgling cybersecurity efforts, or for whom this is their first cybersecurity assessment.
FULL *This is the full physical exam.*	90 days	*Baseline assessment benefits, plus:* • More detailed analysis of strategic and tactical priorities, opportunities, and dangerous gaps.	• A well-written report with a programmatic maturity rating, strategic roadmap, 15–25 detailed recommendations, artifact inventory, and a one-page executive summary. • A briefing for senior leadership.	Most organizations, especially those established cybersecurity programs looking to identify blind spots, address challenge areas, and prioritize investments.
COMPREHENSIVE *This is the executive physical where you must go to Mayo Clinic for a week.*	135 days	*Baseline and full assessment benefits, plus:* • More detailed technical analysis and recommendations, including the results of non-invasive open source intelligence gathering. • Enhanced awareness on exactly how cybersecurity effort and gaps tie into organizational mission priorities.	• A well-written report with a mission decomposition, programmatic maturity rating, strategic roadmap, 25–60 detailed recommendations, open source intelligence summary, artifact inventory, and a multi-page executive summary. • A briefing for senior leadership.	Organizations that are high risk, technologically novel, or organizationally complex.

**Discovery and report production*