MITRE Adaptive Capabilities Testing (ACT) for Risk-Based Decision Making



MITRE ACT is a capabilities-focused assessment framework that encourages and drives risk-based decision making to improve cybersecurity planning, postures, and resource allocation.

Why use ACT?

Cyber risk mitigation is a fundamental part of modern acquisitions, Information Security Continuous Monitoring (ISCM), Authority to Operate (ATO), and Ongoing Authorization (OA) programs. To be effective, these programs require that systems implement context-appropriate security processes and comply with or justifiably deviate from various security standards and controls. Risk-based analysis must be performed to determine where to focus resources. Cybersecurity decisions should not be solely based on compliance with existing policies and procedures; cybersecurity planning must recognize and address the greatest risks to ensure acquisition efforts and follow-on cybersecurity programs are focused on the most important problems, and that limited resources are used with maximum effectiveness.

"Our ACT pilot program is reporting significantly reduced overall assessment costs (time, personnel, money); reduced need for frequent compliance audits; and faster access to 'so what' analyses of the risk postures of our systems."

Andrew Bennett, Centers for Medicare and Medicaid Services ACT Government Task Lead

MITRE

MITRE Adaptive Capabilities Testing (ACT) for Risk-Based Decision Making

MITRE ACT accelerations acquisition, ISCM, ATO, and OA decision processes by identifying which threats to mitigate with which defenses and which risks to accept as capabilities are satisfactorily provided (i.e., within risk tolerance). ACT can provide the primary input into the ATO process, superseding existing compliance-oriented decision-making frameworks.





ACT Uncovers Risks That Compliance Can't

Many acquisition, monitoring, and ATO efforts suffer from similar weaknesses. Low-level technical findings are often handed directly to less-technical decision makers without the appropriate framework for understanding the risk of findings. Without a risk context, closing all findings is the "safest" reaction. Decision makers are implicitly encouraged to blindly comply with standards rather than make risk-based decisions.

When decision makers implement technical changes to the system to close low-level findings without properly understanding the risk context and operational "ground truth," the system will cyclically deviate from compliance, resulting in repeat findings. This results in wasted resources, inappropriate compliance, implicit acceptance of unknown risk, and weaker security postures.

ACT Risk Assessment Workflow

ACT provides fast, efficient, flexible, ongoing risk assessment and facilitates risk-based decision making.

- *Manual* ACT risk assessment can be fully executed in approximately 20 business days.
- *Automated* ACT risk assessment can be configured for specific systems to be executable in minutes.

ACT supports ongoing authorization, ATO, continuous diagnostics and mitigation (CDM), and other risk-based decision-making processes.

For more information about MITRE's Adaptive Capabilities Testing expertise and capabilities, contact act@mitre.org. For more information about MITRE, visit mitre.org.

Want more information?

Contact act@mitre.org

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

© 2023 MITRE | #23-3222 9/28/23

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®