

ADAPTIVE CONTROL TESTING



The Centers for Medicare & Medicaid Services (CMS) is transitioning from the legacy security control assessment (SCA) model to an Adaptive Control Testing (ACT) team. The ACT model will help CMS to improve their security and privacy posture through more frequent, targeted testing by an Information Security and Privacy Group (ISPG) team familiar with the CMS mission and system operation. This new ACT approach also positions CMS to further support the flexible, dynamic DevOps|Agile development methodology, leverage Continuous Diagnostics and Mitigation (CDM) Program automation as part of continuous monitoring, prioritize mitigation of system risks, address evolving threats, and move toward ongoing authorization.

How will this new program change the security and privacy control testing process?

The ACT team will test all Acceptable Risk Safeguard (ARS) selected controls early and throughout the Expedited Life Cycle (XLC), support new system authorizations and conduct thorough, risk-based, efficient continuous security and privacy testing that will support DevOps|Agile development projects and expedite testing schedules.

The ACT Advantage

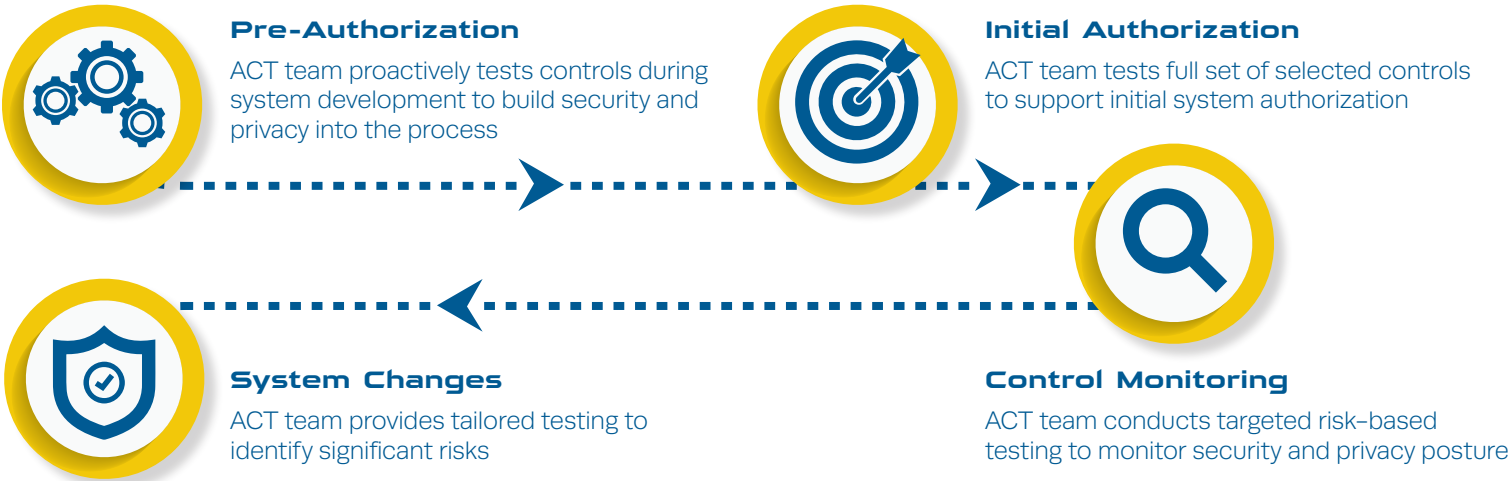
CMS and Cyber Smart. In-house CMS testing team with advanced knowledge of CMS business processes and environments.

Integrated. Leverages existing CMS enterprise tool sets as well as DHS and HHS tests such as Cyber Hygiene, Risk and Vulnerability Assessments, and Einstein.

Targeted. Implements risk- and threat-based approaches to prioritize higher-risk systems including High Value Assets and implement continuous security and privacy monitoring.

Efficient. Automates testing and artifact generation, creates reusable tests and scripts, and focuses on critical controls.

Intelligent. Mine and analyze data sets across CMS to drive business decisions through improved awareness of threats and vulnerabilities that pose security and privacy risks.



Risk-based, Efficient Continuous Security and Privacy Control Testing

Challenges with the SCA Process	Benefits of the Adaptive Control Testing Model
<p>"Point-in-Time" / Annual SCA (or at system change)</p> <p>Decentralized SCA funded by Business Owner with limited scheduling flexibility</p> <ul style="list-style-type: none">> Six-week lead time required for contract action for every test/SCA> Extensive coordination required between Business Owner, ISPG, and SCA Contractor> Not aligned to system risks, evolving threats, or contemporary development methodologies (DevOps Agile)	<p>"Continuous" active testing leverages automation, promotes ongoing authorization, and increases visibility into risks</p> <p>Direct funding model provides flexibility for changing schedules to support CMS mission</p> <ul style="list-style-type: none">✓ Creates a specialized ISPG testing team, builds CMS's cyber capacity, and fully integrates with existing DHS, HHS, and CMS continuous security testing✓ Streamlines testing process with automation to focus stakeholders on risk management✓ Encourages DevOps Agile development processes✓ Targets opportunities to bolster security and privacy posture and aligns testing of system risks to the evolving threat landscape