

Does Cyber Crucible have a change management process?

Short answer: Yes. Production changes follow a documented change-management process with review, testing, and approval. Because the product operates at the kernel level, change discipline is treated as a security control rather than merely an engineering practice.

What the process covers

Changes to application code, kernel drivers, server configurations, and supporting infrastructure move through defined lifecycle stages: security requirements are set at design; source is version-controlled and secrets are never embedded in cleartext; automated testing validates changes before promotion; and production changes receive formal review and approval. Segregation of duties is maintained, so the author of a change is not its sole approver. Server baselines follow approved configuration guides, and unused services are disabled where practical.

Emergency and driver changes

Emergency changes use an expedited path that still requires authorization, targeted testing, and a post-implementation review. Windows kernel drivers undergo internal quality assurance and are submitted for Microsoft's Windows Hardware Compatibility Program (WHCP) certification before release — an independent, external check of the most privileged component.

Framework alignment and the honest boundary

The process aligns to NIST SP 800-53 (CM family) and ISO/IEC 27001:2022 A.8.32. Cyber Crucible does not claim any certification. The detailed change-management procedure and supporting evidence are provided to reviewers under NDA.

Revision #1

Created 2026-07-24 23:08:40 UTC by Dennis Underwood

Updated 2026-07-24 23:08:40 UTC by Dennis Underwood