SmartSuite

Framework / Cybersecurity / Other

OCC Cybersecurity Supervision Work Program (CSW)

The OCC Cybersecurity Supervision Work Program (CSW) is the examiner work program, aligned with the NIST CSF, that OCC examiners use to assess cybersecurity preparedness at national banks.



What it is

The OCC Cybersecurity Supervision Work Program (CSW, earlier abbreviated CSWP) is the set of high-level examination objectives and procedures that Office of the Comptroller of the Currency (OCC) examiners use to assess cybersecurity preparedness at national banks, federal savings associations, and federal branches and agencies of foreign banking organizations. It is an examiner work program, not a rule for banks: OCC Bulletin 2026-48 of September 21, 2026 states that the CSW does not establish new regulatory expectations and that banks are not expected to use it to assess their own preparedness. The OCC first issued the program with Bulletin 2023-22 on June 26, 2023; the 2026 bulletin rescinds and replaces that issuance.

At a glance

PUBLISHER Office of the Comptroller of the Currency (OCC)	TYPE Guidance	VERSION OCC Bulletin 2026-48 (September 21, 2026), replacing Bulletin 2023-22
EFFECTIVE June 26, 2023	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Financial Services	ADOPTION MODEL Voluntary
IMPLEMENTATION COMPLEXITY Medium		

Source: occ.treas.gov/topics/supervision-and-examination/bank-operations/bit/cybersecurity-supervision-work-program-overview.html

Why it matters

- **One vocabulary with examiners** The OCC structured the CSW to align with the six NIST CSF 2.0 functions and their categories and subcategories so that examiners and bank management discuss cybersecurity in the same terms.
- **Published cross-references** The CSW References page maps the procedures to supervisory guidance, examiner guidance and industry frameworks, including the Comptroller's Handbooks, the FFIEC IT Examination Handbook, the CIS Critical Security Controls and the Cyber Risk Institute Profile.
- **Scaled to the bank** The bulletin's note for community banks says the CSW enables risk-based examination scoping and is scalable for banks of different sizes and complexity.
- **No new obligations** The CSW does not establish new regulatory expectations; the OCC encourages, but does not require, a standardized approach and leaves the choice of tool or framework to the bank.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OCC CSWP

Examiner Cross-Reference Map

Map each control in the bank's chosen framework to the CSW's Govern, Identify, Protect, Detect, Respond, and Recover functions and their categories, mirroring the OCC's own References page, so examiner requests are answered in the CSW's vocabulary.

Framework of Choice Register

Keep the standardized tool or framework the bank selected, such as the CIS Critical Security Controls or the Cyber Risk Institute Profile, as a control library in Compliance Management with owners, applicability and testing status.

Cyber Risk Register

Use Cyber & IT Risk to link cyber risks, vulnerabilities and security controls to the CSF functions the CSW follows, so risk-based scoping discussions with examiners start from the bank's own risk picture.

Examination Request Tracker

Log each BIT examination request, the control and evidence that answer it, the owner and the response date, so a community bank or a large bank can show its preparation against the CSW structure.

Incident and Resilience Records

Use Operational Resilience & Business Continuity to hold incident response and recovery plans, exercise results and lessons learned under the Respond and Recover functions.

Audit and Board Reporting

Use Internal Audit Management to plan audits of cybersecurity controls, record findings and track remediation to closure, reported by CSF function for the board and for the examination.

Common framework mappings

EU DORA | CRI Profile | FFIEC IT Handbook | GLBA Safeguards Rule (16 CFR Part 314) | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

OCC Cybersecurity Supervision Work Program Overview

Provides a detailed framework for assessing cybersecurity risk management in banks by the OCC.

occ.treas.gov/topics/supervision-and-examination/bank-operations/bit/cybersecurity-supervision-work-program-overview.html

Frequently asked questions

Does the OCC Cybersecurity Supervision Work Program impose requirements on banks?

No. OCC Bulletin 2026-48 states that the CSW does not establish new regulatory expectations and that banks are not expected to use the work program to assess cybersecurity preparedness. The OCC continues to encourage, but does not require, a standardized approach to assessing and improving preparedness, citing the FFIEC press release of August 28, 2019, and banks may choose from a variety of tools and frameworks.

What changed in OCC Bulletin 2026-48?

The structure and references of the CSW were updated to align with the updated NIST Cybersecurity Framework categories and subcategories. The bulletin's highlights say the procedures remain unchanged and no new procedures were added. Bulletin 2026-48, dated September 21, 2026, rescinds OCC Bulletin 2023-22 of June 26, 2023, which carried the same title.

How is the CSW organized?

The OCC's CSW Overview page says the program is structured to align with the six NIST CSF 2.0 functions, Govern, Identify, Protect, Detect, Respond, and Recover, and the related categories and subcategories. The OCC describes this alignment as giving examiners a common framework and terminology for discussions with bank management.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Which banks and examinations does the CSW cover?

The bulletin is addressed to all national banks, federal savings associations, and federal branches and agencies of foreign banking organizations, and to OCC examining personnel. The CSW is a component of the OCC's risk-based bank information technology supervision process and supplements the Community Bank Supervision, Large Bank Supervision, and Federal Branches and Agencies Supervision booklets of the Comptroller's Handbook and the FFIEC IT Examination Handbook booklets. The note for community banks says it enables risk-based scoping and is scalable to banks of different sizes and complexity.

What does the CSW References page map to?

The References page, linked from the CSW Overview page on www.occ.gov, provides cross-references that map the CSW procedures to existing supervisory guidance, examiner guidance and industry cybersecurity frameworks. Bulletin 2026-48 gives as examples the OCC Comptroller's Handbooks, the FFIEC IT Examination Handbook, the Center for Internet Security Critical Security Controls, and the Cyber Risk Institute Profile, and says future changes to the page will be made available through www.occ.gov.

License included / downloadable: Yes OCC Bulletin 2026-48, the CSW Overview page and the CSW References page are published free of charge by the Office of the Comptroller of the Currency on its website.

Full framework page and mappings: smartsuite.com/frameworks/occ-cybersecurity-supervision-work-program-cswp