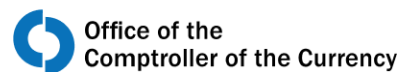


OCC Cybersecurity Supervision Work Program (CSWP)

The OCC Cybersecurity Supervision Work Program guides examiners in assessing banks' cybersecurity risk management, controls, and incident response.



What it is

The OCC Cybersecurity Supervision Work Program (CSWP) is a supervisory framework that guides the assessment of cybersecurity risk management and controls within financial institutions supervised by the Office of the Comptroller of the Currency (OCC). It establishes structured procedures for evaluating how banks safeguard information systems and protect sensitive data against evolving cyber threats.

Developed and maintained by the OCC, the CSWP is used by examiners to assess the effectiveness of a bank's cybersecurity strategies, risk management practices, incident response capabilities, and governance structures. The program covers areas such as access controls, vulnerability management, third-party risk, data protection, and compliance oversight, aligning its focus with regulatory expectations and industry standards.

At a glance

PUBLISHER Office of the Comptroller of the Currency (OCC)	TYPE Guidance	VERSION Current OCC Cybersecurity Supervision Work Program
EFFECTIVE 2022	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

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

Why it matters

- **Support effective cybersecurity oversight** Facilitates systematic assessment and monitoring of risk management practices across critical banking functions and infrastructure.
- **Enhance regulatory compliance** Aligns internal controls with OCC requirements, ensuring institutions are prepared for examinations and regulatory scrutiny.
- **Strengthen incident response readiness** Promotes development and validation of robust detection, response, and recovery capabilities against emerging threats.
- **Reduce third-party risk exposure** Requires evaluation of vendor management practices to mitigate vulnerabilities stemming from relationships with external service providers.

How SmartSuite supports OCC CSWP

Exam Expectation Mapping

Map CSWP focus areas to controls, owners, and evidence sources.

Risk Assessments and Governance Reporting

Track cyber risk assessments and maintain leadership reporting artifacts.

Vendor Inventory and Contingency Planning

Manage vendor inventories, monitoring, and contingency planning evidence.

Control Testing and Assurance Cadence

Schedule testing, capture results, and manage remediation through closure.

Incident and Resilience Workflows

Run incident response and resilience exercises with documented outcomes.

Posture and Remediation Reporting

Report posture, gaps, evidence coverage, and remediation status.

Common framework mappings

EU DORA

FFIEC CAT

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

What is the OCC Cybersecurity Supervision Work Program (CSWP) used for?

The CSWP is used by the Office of the Comptroller of the Currency (OCC) to assess how effectively financial institutions manage cybersecurity risks and protect information systems. It provides examiners with structured procedures to evaluate controls over sensitive data, system access, risk management, and incident response.

Is compliance with the CSWP mandatory for financial institutions?

Yes, for OCC-regulated financial institutions, adherence to the CSWP serves as a critical component of regulatory examinations. While not a certifiable standard, it is a supervisory expectation; failure to align with CSWP requirements may result in findings or regulatory action.

What is the scope of the CSWP and which institutions must comply?

The CSWP applies to national banks, federal savings associations, and federal branches regulated by the OCC. Its scope covers institution-wide cybersecurity governance, technology infrastructure, third-party risk, incident management, and ongoing resilience.

What key controls and documentation does the CSWP require?

The CSWP emphasizes access controls, vulnerability management, third-party risk procedures, incident response plans, and documented governance structures. Institutions are expected to maintain evidence of risk assessments, control testing, policy adherence, and remediation actions.

How should a financial institution implement the CSWP?

Implementation involves mapping existing controls to the CSWP's control areas, conducting periodic risk assessments, performing internal testing, and documenting findings. Institutions should integrate remediation efforts into governance reporting and update policies to address identified gaps.

How does the CSWP relate to other cybersecurity frameworks and standards?

The CSWP aligns with regulatory expectations and industry standards, including the FFIEC Cybersecurity Assessment Tool and NIST frameworks. Utilizing CSWP helps institutions demonstrate alignment with broader compliance requirements and recognized best practices.

What are the ongoing compliance requirements under the CSWP?

Ongoing compliance with the CSWP requires continuous control monitoring, timely remediation of identified weaknesses, regular risk reviews, and transparent reporting to senior management and examiners. Periodic updates to risk assessments and incident response capabilities are essential.

How would SmartSuite support OCC Cybersecurity Supervision Work Program (CSWP)?

SmartSuite enables financial institutions to manage CSWP requirements through centralized control libraries, risk registers, and policy governance. It facilitates automated evidence collection, configurable remediation workflows, and compliance tracking, supporting audit readiness and transparent reporting for OCC examinations.

License included / downloadable: Yes The OCC Cybersecurity Supervision Work Program is publicly available through the U.S. Office of the Comptroller of the Currency.

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