SWIFT CSCF v2026 · Control 7.3A

SWIFT CSCF v2026 Control 7.3A penetration-test readiness checklist

1. Scope by consequence

- ☐ The SWIFT estate is inventoried: secure zone, messaging interface, operator workstations, the connection to the network, and the back-office systems that feed it.
- ☐ Attack paths are ranked by the consequence of compromise, not by ease of testing.
- ☐ Scope is defined against the secure zone and its trust boundaries, so the test proves an attacker cannot pivot from the back office into the messaging layer.
- ☐ Testing is planned across the three-year scenario cycle, covering application, infrastructure and human paths.

2. Frame with threat intelligence

- ☐ Current intelligence on actors targeting financial messaging informs the test scenarios.
- ☐ Scenarios rehearse plausible, named intrusion paths rather than generic vulnerability classes.
- ☐ The intelligence basis is documented, so the test qualifies as threat-led under DORA and OSFI B-13.

3. Execute to the strongest standard

- ☐ The test runs from both inside and outside the systems' boundaries, meeting the NYDFS Part 500 expectation.
- ☐ The test is performed by a competent and sufficiently independent party.
- ☐ Rules of engagement, authorisation and safety controls for testing live systems are documented and approved.
- ☐ A defined cadence is set and recorded, satisfying the annual NYDFS minimum and the SWIFT cycle together.

4. Measure your own defences

- ☐ The exercise measures whether monitoring detected the simulated intrusion, not only what was found.
- ☐ Response and containment performance is recorded against the Detect and Respond functions.
- ☐ Detection gaps are logged as findings in their own right.

5. Close the loop and bank the evidence

- ☐ Findings enter a tracked remediation cycle with owners and dates.
- ☐ Remediation closure is evidenced, not merely asserted.
- ☐ The full record (scope, scenarios, attack narrative, findings, remediation, detection performance) is filed once against the NIST Cybersecurity Framework 2.0 spine.
- ☐ The single record is tagged to each regime: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.