NYDFS Part 500 — Tabletop Exercise Prep Checklist

Evidence requirements for incident response and BCDR testing under 23 NYCRR 500 § 500.16

WHY THIS MATTERS: NYDFS examiners expect evidence that IR plans were tested, decisions were intentional, lessons were captured, and governance improved. Annual certification (due April 15) requires documentation sufficient to demonstrate material compliance.

Key deadline: April 15 annual cybersecurity compliance certification — signed by a senior officer under personal accountability.

1. PRE-EXERCISE PLANNING

§ 500.16(a)(1), § 500.16(b)

- ☐ Define scenario scope: IR, BCDR, or integrated exercise
- ☐ Identify all critical staff required to participate
- ☐ Confirm exercise tests the actual IR plan (not a generic script)
- ☐ Include relevant threat type (ransomware, BEC, insider, etc.)
- ☐ Assign roles matching real organizational responsibilities
- ☐ Schedule pre-brief for participants on exercise objectives
- ☐ Prepare injects aligned to your environment and crown jewels
- ☐ Confirm documentation method before exercise begins

2. DURING THE EXERCISE — EVIDENCE CAPTURE

§ 500.16(a)(2), § 500.17(a)

- ☐ Log participant attendance with names, roles, timestamps
- ☐ Record each decision point and the rationale behind it
- ☐ Document escalation paths taken (or missed)
- ☐ Capture communication actions: who was notified, when, how
- ☐ Track actions against IR plan steps — note deviations
- ☐ Record containment, eradication, and recovery decisions
- ☐ Note BCDR activation triggers and recovery sequencing
- ☐ Flag gaps in real time: unclear roles, missing runbooks, delays

3. POST-EXERCISE — DOCUMENTATION & REPORTING

§ 500.16(a)(3), § 500.16(c)

- ☐ Produce structured after-action report (not narrative-only)
- ☐ Categorize all identified gaps by severity and domain
- ☐ Map findings to specific IR/BCDR plan sections for revision
- ☐ Assign remediation owners with target completion dates
- ☐ Generate executive summary for board / risk committee
- ☐ Document how findings will be incorporated into plan updates
- ☐ Archive all exercise artifacts in a centralized, auditable location
- ☐ Confirm 5-year retention for all compliance documentation

4. PLAN REVISION & IMPROVEMENT TRACKING

§ 500.16(a)(3), § 500.16(d)

- ☐ Update IR plan based on exercise findings (not just the report)
- ☐ Update BCDR plan with revised recovery procedures if tested
- ☐ Compare current exercise results against prior exercises
- ☐ Document what changed between exercises and why
- ☐ Track gap closure rate over time (year-over-year trend)
- ☐ Verify updated plans are redistributed to relevant staff

5. CERTIFICATION READINESS (APRIL 15 DEADLINE)

§ 500.17(b)

- ☐ Confirm all exercise evidence is accessible and organized
- ☐ Verify documentation chain: exercise → findings → plan revision
- ☐ Ensure signing officer can explain how testing improved readiness
- ☐ Validate evidence covers both IR and BCDR if applicable
- ☐ Confirm no open critical gaps from most recent exercise
- ☐ Brief certifying executive on evidence package before signature

THE EXAMINER QUESTION TO PREPARE FOR:

"How did this exercise improve your incident response and business continuity plans — and can you show me the evidence?"

This checklist reflects regulatory intent and examination practice under 23 NYCRR Part 500 (amended Nov 2023). It is not legal advice.
For questions on operationalizing these requirements, contact ChaosTrack | chaostrack.com
© 2026 ChaosTrack