FINANCIAL SERVICES

STIG

Examiner-Ready Cyber Checklist

A forward-facing checklist to strengthen cybersecurity programs, produce examiner-ready evidence, and reduce tool sprawl through a platform-first security operations model.

Version 1.0 | February 13, 2026

Built for community banks, credit unions, insurance carriers, brokers/MGAs, lending & mortgage organizations, and fintech teams.

Note: This checklist is a high-level reference and does not constitute legal advice. Your regulatory obligations vary by charter, footprint, products, and regulator expectations.

Purpose

Financial services cybersecurity programs are held to a higher standard: strong controls are table stakes, but the ability to demonstrate them—quickly, consistently, and with credible evidence—is what makes an organization examiner-ready.

This checklist is designed to help you: (1) identify practical control gaps, (2) build an evidence repository that holds up under NYDFS/GLBA/FFIEC scrutiny, and (3) modernize security operations while reducing operational overhead.

Aligned to Common Expectations

- NYDFS 23 NYCRR 500 (for covered entities)
- GLBA Safeguards expectations (and related state privacy expectations where applicable)
- FFIEC guidance and examination focus areas
- NIST Cybersecurity Framework (CSF) 2.0 outcomes and governance focus
- CISA Cross-Sector Cybersecurity Performance Goals (CPGs) as a practical baseline
- CIS Controls v8 as an actionable implementation guide

Top Risks We See

- Evidence gaps: policies exist, but controls aren’t consistently documented and repeatable.

- Identity risk: credential theft + privileged access sprawl create rapid compromise paths.
- Tool sprawl: disconnected tools drive alert fatigue and inconsistent response outcomes.
- Unrehearsed incident response: teams are unprepared for incident decisions and reporting timelines.

A Roadmap That Reduces Tool Sprawl and Improves Outcomes

- Phase 1 — Foundation: endpoint and identity hardening + baseline MDR.
- Phase 2 — Visibility: vulnerability/exposure management + cloud visibility.
- Phase 3 — Modernization: SIEM modernization + correlation + automation at scale.
- Phase 4 — Optimization: continuous improvement + executive reporting cadence.

How to Use This Checklist

- Assess: Mark each item as In Place, Partial, or Not In Place.
- Evidence: Attach proof (policy, screenshot, report, ticket, log sample) for items marked In Place.
- Plan: Convert gaps into a prioritized roadmap (people, process, technology) tied to risk reduction.
- Validate: Test with tabletop exercises, recovery drills, and penetration testing/validation.
- Maintain: Re-validate at least annually and after major changes, incidents, or material new threats.

Scope and Inputs

Before starting, confirm scope: business-critical services, supporting applications and infrastructure (on-prem, cloud, SaaS), external dependencies (core systems, telecom, payment processors, MSPs), and the regulatory/consumer impact of disruption or data exposure.

Examiner-Ready Evidence Pack

- Program governance: security charter, roles, board reporting, metrics, exception register.
- Risk and control mapping: risk assessment, asset/data inventory, control mapping and testing cadence.
- Identity & access: MFA coverage, privileged access reviews, joiner/mover/leaver evidence.
- Vulnerability & configuration: scan results, patch SLAs, secure baselines, change control.
- Monitoring & response: logging standards, alert triage SOPs, incident tickets, response timelines.
- Resilience: backup strategy, recovery test results, RTO/RPO, DR and crisis communications.
- Third-party: vendor inventory, due diligence, contract clauses, ongoing monitoring, offboarding.
- Training: security awareness metrics, phishing results, role-based training, exercise records.

FINANCIAL SERVICES

STIG

1. Governance, Risk, and Examiner Readiness

Checklist item	What good looks like	Status / notes
☐ Executive sponsor and security charter are established	Charter defines objectives, scope, decision rights, and lines of accountability.	In Place / Partial / Not In Place
☐ Cyber risk appetite and key risk indicators (KRIs) are documented	Defines tolerance thresholds and triggers for escalation and investment.	In Place / Partial / Not In Place
☐ Security program maps to baseline frameworks	Mapping supports consistent reporting (NYDFS/GLBA/FFIEC) and reduces audit churn.	In Place / Partial / Not In Place
☐ Formal risk assessment is performed and updated	Includes inherent risk, control effectiveness, and residual risk; updated after major changes.	In Place / Partial / Not In Place
☐ Policies and standards are current and enforced	Policies are approved, communicated, and tied to procedures and technical enforcement.	In Place / Partial / Not In Place
☐ Evidence repository exists for audits and examinations	Central store for policies, test results, tickets, and control evidence with ownership.	In Place / Partial / Not In Place
☐ Exception process exists with approvals and expirations	Risk-accepted exceptions have compensating controls, owners, and review dates.	In Place / Partial / Not In Place
☐ Metrics and reporting cadence are defined	Regular reporting on MTTD/MTTR, MFA, patch SLAs, vuln backlog, phishing, and incidents.	In Place / Partial / Not In Place

2. Asset, Data, and Architecture Visibility

Checklist item	What good looks like	Status / notes
☐ Enterprise asset inventory is maintained	Covers endpoints, servers, network, cloud, SaaS, and critical third-party connections.	In Place / Partial / Not In Place
☐ Data classification and handling standards exist	Identifies customer data, NPI/PII, payment data, and sensitive operational data.	In Place / Partial / Not In Place
☐ Crown jewels and critical services are identified	Defines high-value assets, business processes, and dependencies for resilience planning.	In Place / Partial / Not In Place
☐ Network and cloud diagrams are current	Documented trust boundaries, segmentation, and connectivity to core banking/fintech systems.	In Place / Partial / Not In Place
☐ Logging sources are prioritized	EDR + identity + email + network/cloud/app logs	In Place / Partial / Not

by risk	are prioritized and integrated.	In Place
☐ Shadow IT is controlled	Discovery and approval workflow for SaaS, remote access tools, and integrations.	In Place / Partial / Not In Place

3. Identity, Privileged Access, and Authentication

Checklist item	What good looks like	Status / notes
☐ MFA is enforced for all remote and privileged access	Phishing-resistant or stronger MFA is used for high-risk roles and systems.	In Place / Partial / Not In Place
☐ Privileged access is minimized and monitored	PAM or equivalent controls; admin accounts are separate, time-bound, and reviewed.	In Place / Partial / Not In Place
☐ Account lifecycle is governed	Joiner/mover/leaver process with timely disablement and periodic access recertification.	In Place / Partial / Not In Place
☐ Service accounts and API keys are inventoried	Secrets are vaulted, rotated, and scoped; usage is logged and reviewed.	In Place / Partial / Not In Place
☐ Conditional access policies are implemented	Device compliance, location/risk signals, and session controls reduce takeover risk.	In Place / Partial / Not In Place
☐ Identity logs are centralized	SSO/IdP logs are retained and monitored for anomalous behavior and privilege escalation.	In Place / Partial / Not In Place

4. Exposure, Vulnerability, and Secure Configuration

Checklist item	What good looks like	Status / notes
☐ Secure configuration baselines are defined	Hardened baselines for endpoints, servers, network, cloud, and SaaS configurations.	In Place / Partial / Not In Place
☐ Vulnerability scanning is comprehensive	Internal/external scanning with authenticated coverage and documented remediation SLAs.	In Place / Partial / Not In Place
☐ Patch management is risk-based and tracked	Critical patches and exploited vulns are prioritized; exceptions are documented.	In Place / Partial / Not In Place
☐ Penetration testing validates real-world exposure	Testing focuses on external perimeter, internal paths, and high-value applications.	In Place / Partial / Not In Place
☐ Configuration and change control are enforced	Change approvals, rollback plans, and segregation of duties are documented.	In Place / Partial / Not In Place

☐ Email and web protections are hardened	DMARC/SPF/DKIM, phishing protections, safe links/attachments, and user reporting.	In Place / Partial / Not In Place

5. Detection, Response, and Automation

Checklist item	What good looks like	Status / notes
☐ Endpoint detection and response (EDR) coverage is complete	All endpoints/servers are onboarded with consistent policy enforcement.	In Place / Partial / Not In Place
☐ Security monitoring has defined use-cases	Documented detections for credential abuse, ransomware behaviors, and data exfiltration.	In Place / Partial / Not In Place
☐ SIEM/log management supports investigation	Time sync, retention, and searchable logs enable efficient triage and forensics.	In Place / Partial / Not In Place
☐ SOC workflows and escalation paths are documented	Clear triage SOPs, severity definitions, and on-call/escalation expectations.	In Place / Partial / Not In Place
☐ Automated response is implemented safely	SOAR/workflows for enrichment, containment, and ticketing with guardrails and approvals.	In Place / Partial / Not In Place
☐ Threat intelligence is operationalized	IOCs/TTPs are integrated into detections and exposure reduction prioritization.	In Place / Partial / Not In Place

6. Incident Response, Reporting, and Communications

Checklist item	What good looks like	Status / notes
☐ Incident response plan (IRP) is current and exercised	IRP includes roles, escalation, evidence handling, and decision-making under pressure.	In Place / Partial / Not In Place
☐ Regulatory and contractual reporting timelines are documented	Playbooks include NYDFS/agency notice, customer notice, and insurer requirements.	In Place / Partial / Not In Place
☐ Ransomware and extortion playbooks exist	Covers containment, negotiation decision points, sanctions screening, and payment controls.	In Place / Partial / Not In Place
☐ Forensic readiness is established	Log retention, imaging procedures, and third-party IR support are pre-arranged.	In Place / Partial / Not In Place
☐ Crisis communications plan is	Internal/external comms templates,	In Place / Partial / Not

defined	spokespersons, and approval paths are established.	In Place
☐ Lessons learned drives improvements	Post-incident reviews produce tracked corrective actions and control updates.	In Place / Partial / Not In Place

7. Third-Party, Cloud, and Service Provider Oversight

Checklist item	What good looks like	Status / notes
☐ Third-party inventory is complete and risk-ranked	Vendors are categorized by data access, criticality, and connectivity.	In Place / Partial / Not In Place
☐ Due diligence is performed before onboarding	Security questionnaires, SOC reports, pen test summaries, and breach history reviewed.	In Place / Partial / Not In Place
☐ Contracts include enforceable security requirements	MFA, logging, patching, breach notification, audit rights, and support SLAs defined.	In Place / Partial / Not In Place
☐ Ongoing monitoring is performed	Periodic reassessment scaled to vendor criticality; issues are tracked to closure.	In Place / Partial / Not In Place
☐ Vendor offboarding is prompt and verifiable	Accounts, keys, and access paths are removed; data return/destruction is confirmed.	In Place / Partial / Not In Place
☐ Cloud and SaaS configurations are governed	Shared responsibility is documented; misconfiguration risk is continuously managed.	In Place / Partial / Not In Place

8. Resilience, Recovery, and Continuous Improvement

Checklist item	What good looks like	Status / notes
☐ BCP/DR plans include cyber scenarios	RTO/RPO targets are defined and validated for critical services and dependencies.	In Place / Partial / Not In Place
☐ Backups are resilient to ransomware	Immutable/offline backups, protected credentials, and regular restore testing.	In Place / Partial / Not In Place
☐ Recovery testing is performed and documented	Includes tabletop + technical recovery drills with measurable outcomes.	In Place / Partial / Not In Place
☐ Operational resilience supports customer trust	Plans address prolonged outages, degraded operations, and manual fallback procedures.	In Place / Partial / Not In Place
☐ Training is role-based and	Security awareness + privileged user training;	In Place / Partial / Not

measured	phishing simulations and metrics.	In Place
☐ Continuous improvement cadence is defined	Roadmap is updated quarterly; metrics drive investment and control tuning.	In Place / Partial / Not In Place

References

- Federal Financial Institutions Examination Council CAT sunset statement
- National Institute of Standards and Technology CSF 2.0
- Cybersecurity and Infrastructure Security Agency Cross-Sector CPGs
- Office of the Comptroller of the Currency + Federal Register references for the 36-hour incident notification rule
- New York State Department of Financial Services Part 500 resource hub (for the NYDFS track)
- Federal Trade Commission Safeguards Rule overview
- Securities and Exchange Commission incident disclosure timing reference (public-company context)

How STIG Can Help

- Financial Services Cyber Readiness Assessment (NYDFS/GLBA/FFIEC mapped gap assessment + evidence package)
- Penetration testing and exposure validation to prioritize real-world risk
- Incident Response tabletop exercises to rehearse decisions and reporting timelines
- CrowdStrike-native security operations (STIG MDR + automation) for 24×7 detection and response
- Security awareness and managed phishing to reduce social engineering risk

Next Step

If you want help operationalizing this checklist—closing gaps, consolidating tools, and building an examiner-ready evidence repository—STIG can guide the program end-to-end. Contact: info@stig.net | 201-431-2678