BROTHERLY TECHNOLOGY

FINANCIAL SECURITY CHECKLIST

The Financial Services IT Security Checklist

Security and documentation requirements mapped to the controls examiners actually ask to see.

01	**Access, encryption and retention requirements**
02	**Incident response documentation you need on file**
03	**Vendor due-diligence questions worth asking**

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology
Owner-led IT, security, and compliance support.

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

[ ] A written information security program has a qualified owner and leadership oversight.	[ ] Yes [ ] Partial [ ] No
[ ] Risk assessments identify customer information, threats, controls, and residual risk.	[ ] Yes [ ] Partial [ ] No
[ ] Access is least-privilege, MFA-protected, reviewed, and removed promptly.	[ ] Yes [ ] Partial [ ] No
[ ] Customer information is encrypted in transit and at rest or an approved alternative is documented.	[ ] Yes [ ] Partial [ ] No
[ ] Systems, applications, and vendors are inventoried with data classification and owners.	[ ] Yes [ ] Partial [ ] No
[ ] Secure development, change, vulnerability, patch, and configuration processes are documented.	[ ] Yes [ ] Partial [ ] No
[ ] Logs and alerts support timely detection, investigation, and evidence preservation.	[ ] Yes [ ] Partial [ ] No
[ ] Backups are isolated, monitored, and tested against approved recovery targets.	[ ] Yes [ ] Partial [ ] No
[ ] Incident response includes defined roles, external contacts, notification decisions, and exercises.	[ ] Yes [ ] Partial [ ] No
[ ] Service providers receive risk-based due diligence, contract controls, and ongoing monitoring.	[ ] Yes [ ] Partial [ ] No
[ ] Retention and disposal rules are applied to records, backups, exports, email, and devices.	[ ] Yes [ ] Partial [ ] No
[ ] Control testing and program reporting produce corrective actions with owners and dates.	[ ] Yes [ ] Partial [ ] No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

CONTROL MAP

Make access, encryption, and retention defensible

Tie each requirement to an owner, technical setting, operating record, and review date.

Area	Minimum decision	Evidence
Access	Unique IDs, MFA, least privilege, privileged separation, timely offboarding	Coverage, access reviews, tickets, logs
Encryption	Approved protection for stored data, endpoints, backups, and transmission	Configuration, key ownership, exception record
Retention	Schedule by record and obligation; defensible disposal	Policy, system rules, legal holds, deletion record
Monitoring	Relevant identity, endpoint, email, network, cloud, and application events	Log sources, alerts, investigations, tests
Recovery	Protected copies and tested RTO/RPO	Job reports, immutability settings, exercise results
Governance	Qualified owner, board/senior reporting, risk acceptance	Approvals, reports, minutes, corrective plan

Requirements vary by institution, charter, regulator, state, services, and data. Map this worksheet to the obligations your counsel and regulators identify.

INCIDENT AND VENDOR FILES

Keep the documentation ready before the request arrives

A plan is useful only when contacts, systems, responsibilities, decision criteria, and exercise results are current.

1	Maintain an incident plan with severity, authority, evidence handling, communications, legal, insurer, regulator, and customer-notification decision paths.
2	Keep offline contact details, system diagrams, logging sources, critical vendors, data locations, and recovery priorities.
3	Exercise ransomware, customer-data exposure, wire fraud, vendor compromise, and extended service outage scenarios.
4	For vendors, record service, data, access, criticality, security evidence, contract terms, subcontractors, incidents, and exit plan.
5	Track every exercise and vendor finding to a named owner, due date, risk decision, and closure evidence.

What to watch for

WATCH: The incident plan is a generic template with no authority or notification decision path.

WATCH: A critical vendor cannot provide security evidence or a timely incident-notification commitment.

WATCH: Retention is configured in one system but not exports, backups, or employee archives.

WATCH: Privileged access is reviewed only during annual audit preparation.

WATCH: Corrective actions have no due dates or closure evidence.

MAKE IT ACTIONABLE

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	_____
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	_____
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	_____
NEXT QUARTER	Test the process, document results, and assign improvements.	_____

Notes / decisions / questions for your provider

_____

_____

_____

_____

_____

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.

Reference points: FTC Safeguards Rule: ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act | FFIEC IT Examination Handbook: ffiec.gov/it-booklets