SAMPLE REPORT — ILLUSTRATIVE DATA, NOT A REAL ASSESSMENT

Sample Organization (illustrative)

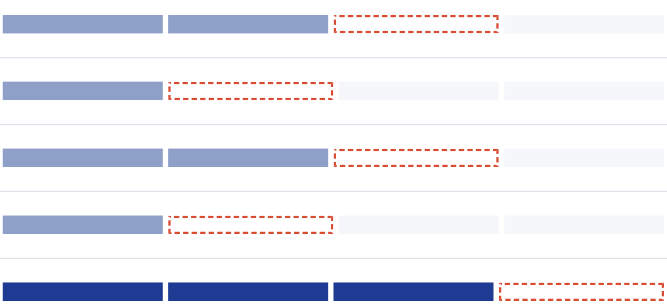
Financial Services · Assessed January 15, 2026 · Prepared by Sample data — not a real assessment · Next reassessment April 15, 2026

EXECUTIVE SUMMARY

OVERALL MATURITY	PRIORITY GAPS	PLANNED ACTIONS
L2 Orchestrated Average 1.80 of 4	**4** Dimensions at Level 1–2	**5** 4 high priority

Overall maturity band is an application convention applied to the average score (1.00–1.49 Manual, 1.50–2.49 Orchestrated, 2.50–3.49 Proactive, 3.50–4.00 Adaptive). The source maturity model defines levels per dimension only; each dimension progresses independently.

MATURITY BY DIMENSION



Incident Execution & Accountability	L2 Orchestrated ’ L3
Cross-Functional Coordination	L1 Manual ’ L2
Regulatory & Legal Readiness	L2 Orchestrated ’ L3
Documentation & Continuous Improvement	L1 Manual ’ L2
Training & Operational Readiness	L3 Proactive ’ L4

EXECUTIVE ASKS

- Require each function to name primary and backup responders.
- Designate the authoritative incident system of record.
- Agree escalation SLAs and the leadership audience for each severity.
- Approve notification templates and the sign-off chain for disclosures.

FINDINGS — WEAKEST FIRST

DIMENSION	LEVEL	RISK	NEXT STEP
Cross-Functional Coordination	L1 Manual	Coordinating through meetings, email, and disconnected channels slows approvals and leaves functions unsure what is expected of them.	Write playbooks that assign repeatable actions to security, IT, legal, privacy, communications, and executives.
Documentation & Continuous Improvement	L1 Manual	Incomplete records and after-the-fact timeline reconstruction leave gaps when decisions must be explained to regulators, auditors, or the board.	Centralize incident records so facts, evidence, actions, and decisions are captured in one place.
Incident Execution & Accountability	L2 Orchestrated	Without defined owners and severity tiers, decisions depend on whoever is available and escalations happen late or not at all.	Introduce context-based rules so ownership and escalation adjust automatically with incident type, data involved, and impact.
Regulatory & Legal Readiness	L2 Orchestrated	Manual legal interpretation can miss thresholds or deadlines, increasing regulatory and contractual exposure.	Trigger draft notices automatically from incident facts and the applicable regulatory requirements.
Training & Operational Readiness	L3 Proactive	Static, security-only playbooks that are rarely exercised fail in ways that only surface during a real incident.	Run realistic, on-demand exercise scenarios, including AI-generated scenarios, so teams build muscle memory.

90-DAY PLAN · DAYS 1–30

Establish incident ownership, severity, and cross-functional responsibilities; set owners and measures.

High Write playbooks that assign repeatable actions to security, IT, legal, privacy, communications, and executives.
Cross-Functional Coordination ’ L2 · Owner: Incident Response Lead · Due: 2026-02-14 · Done when: Each function has reviewed and accepted its responsibilities in the playbooks.

High Centralize incident records so facts, evidence, actions, and decisions are captured in one place.
Documentation & Continuous Improvement ’ L2 · Owner: Incident Response Lead with Legal · Due: 2026-02-14 · Done when: All incidents in the review period have records in the central repository.

High Introduce context-based rules so ownership and escalation adjust automatically with incident type, data involved, and impact.
Incident Execution & Accountability ’ L3 · Owner: CISO / Incident Response Lead · Due: 2026-02-14 · Done when: Escalations in an exercise or live incident follow the rule set within the SLA.

90-DAY PLAN · DAYS 31–60

Map regulatory obligations and stand up a single system of record for the response.

High Trigger draft notices automatically from incident facts and the applicable regulatory requirements.
Regulatory & Legal Readiness ’ L3 · Owner: General Counsel / Privacy Counsel · Due: 2026-03-16 · Done when: In an exercise, applicable obligations and draft notices are produced from incident facts.

90-DAY PLAN · DAYS 61–90

Run a cross-functional exercise, measure outcomes, and feed findings back into playbooks.

Medium Run realistic, on-demand exercise scenarios, including AI-generated scenarios, so teams build muscle memory.

Training & Operational Readiness ' L4 · Owner: Incident Response Lead / Exercise Coordinator · Due: 2026-04-15 · Done when: Exercises per quarter and playbook update rate are tracked and reviewed by leadership.

MEASURES OF SUCCESS

Incident Execution & Accountability: % of incidents opened with an owner and severity assigned; escalation SLA adherence.

Cross-Functional Coordination: % of incidents with documented cross-functional tasks and approvals; stakeholder response time.

Regulatory & Legal Readiness: % of incidents with obligations mapped; time to produce a notification timeline.

Documentation & Continuous Improvement: % of incidents with a complete timeline and evidence package; time to generate a final report.

Training & Operational Readiness: # of exercises per quarter; % of playbooks updated after incidents and exercises.

This report reflects self-reported answers against the BreachRx Cyber Incident Response Management (CIRM) Maturity Model. Recommendations are planning guidance, not legal advice, and do not guarantee incident outcomes, privilege, or regulatory compliance.

Optional BreachRx capabilities are shown for reference only and are separate from the neutral recommendations. They do not assure legal privilege, regulatory compliance, or incident preparedness. Confirm current feature availability before relying on it.