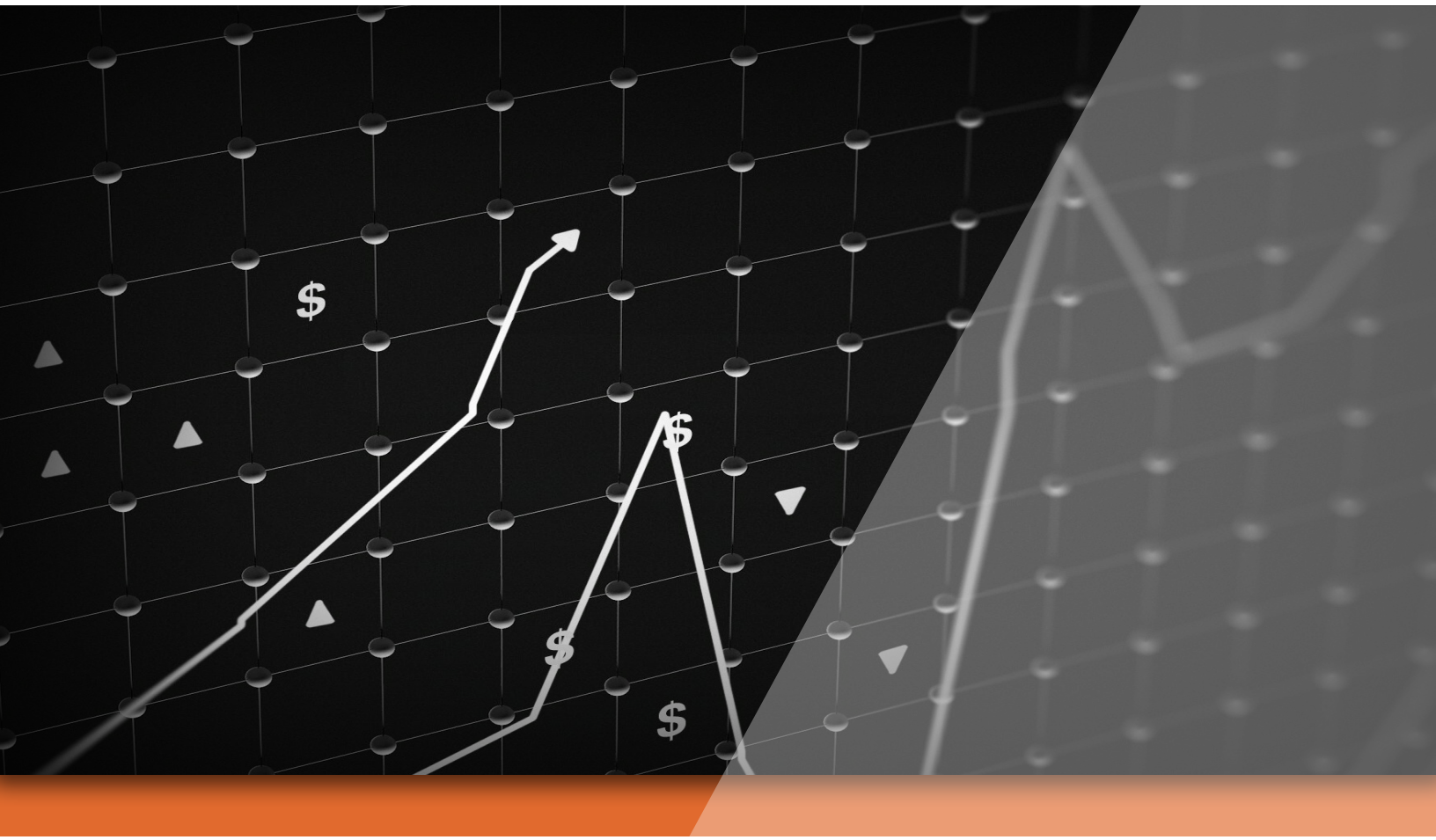


MALA TECHNOLOGY ADVISORS

EXECUTIVE BRIEF · CONFIDENTIAL

BEFORE THE CALL COMES

IT Operational Risk and Executive Accountability in Banking

US Banking Edition

What US banking executives need to understand about IT operational risk — and the decisions that cannot wait for a crisis to force them.

TABLE OF CONTENTS

FOREWORD | WHY THIS GUIDE EXISTS

THE CALL WILL COME.

A system alert that looks like a hardware failure. An employee who clicked a link three months ago. A ransomware group that has been reading your network since February. The question that determines everything — how long this lasts, how much it costs, whether it ends careers — was answered months or years before anyone picked up the phone.

In late May 2024, an IT team at Evolve Bank & Trust in Arkansas noticed something wrong with their systems. What initially looked like a hardware failure was not. LockBit ransomware had been moving through Evolve's network since February — nearly four months undetected. The entry point was a single phishing link, clicked by one employee. By the time the attack was identified and stopped, data belonging to approximately 18 million people had been exfiltrated.

Evolve refused to pay the ransom. LockBit published the stolen data — names, Social Security numbers, bank account numbers, dates of birth — on its dark web leak site. Fifteen fintech partners, including companies processing payments for millions of Americans, were forced to notify their own customers of a breach they had no direct role in causing. The regulatory and legal fallout cost Evolve $11.85 million in settlements. The reputational damage to its Banking-as-a-Service business was harder to quantify.

Evolve is not an outlier. It is a template. The same criminal organization that hit Evolve — LockBit — disrupted derivatives clearing across dozens of institutions the year before by ransoming a single shared vendor, ION Trading UK, forcing banks including Citigroup, Bank of America, and Morgan Stanley to manually review trades. A different group used the same pattern of patient, undetected access to steal $101 million from Bangladesh Bank's SWIFT system in a single weekend. Ransomware attacks on US banking infrastructure are accelerating — FinCEN reported more than 1,500 incidents in 2023 alone, totaling over $1.1 billion in payments. The question facing every US banking executive is not whether an event of this kind could happen at their institution. It is whether their institution has made the decisions that determine whether they recover in four hours or four weeks.

Those decisions are not technical. They are governance, investment, and accountability decisions that belong in this room — not in the IT department. **This brief exists to give you the information you need to make them, and the questions to ask to confirm they have been made correctly.**

$6.08M
Average Data Breach Cost
Financial services, IBM 2024

>$1B
Largest BSA/AML Penalty
Single US enforcement action

This document is intended for informational purposes only and should not be used for legal advice. Examples, thresholds, and maturity targets are illustrative unless explicitly sourced.

SECTION 01

WHAT CAN ACTUALLY HAPPEN

> **FIVE SCENARIOS** can end a banking career, close a business line, or bring regulators into the boardroom for years. Each has happened. The numbers below are not projections — they are documented losses at real institutions.

Risk briefings often fail executives because they describe threats without consequences, or consequences without context. The table below does neither. It describes what actually happens — operationally, financially, and from a regulatory standpoint — when each scenario materializes. Read it as a contingency plan stress test: for each row, ask whether your institution's current preparations would produce an outcome you could defend to your Board, your regulator, and your customers.

Scenario 1: Ransomware — Core Banking and Payments

FINANCIAL EXPOSURE: $50M-$500M+

Everything stops at once. Online banking goes dark. Branch tellers cannot access accounts. ATMs go offline. Payment processing halts. The CEO learns about it from the COO, who learned about it from an alert at 3 AM. If backup systems share credentials with the encrypted network — which they do at most institutions — there is nothing to restore from. Recovery takes 2–4 weeks. The regulatory investigation opens within 36 hours. Customer attrition begins immediately and lasts 18 months.

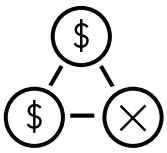
Scenario 2: Regulatory Consent Order — IT Governance Failure

$100M-$1B+, PLUS GROWTH CAP

Consent orders do not primarily follow dramatic security breaches. They follow governance failures: no Board-approved risk appetite, IT security oversight that lacks structural independence from IT operations, Internal Audit that is not genuinely independent, IT risk reporting that does not reach the Board in meaningful terms. The financial penalty is severe. The growth cap — which can restrict asset acquisition for years — is often worse. The CEO and Board are named. The remediation program is run by the regulator, not management.

Scenario 3: Payment Network Compromise

$50M–$1B+



Attackers gain access to the systems that authorize wire transfers and submit fraudulent instructions in the bank's name. Funds move across multiple correspondent accounts within hours. After 24 hours, recovery becomes near-impossible — the correspondent chain has cleared. The 2016 Bangladesh Bank SWIFT heist was $101 million over one weekend — $81 million routed through the Federal Reserve to the Philippines, and $20 million to Sri Lanka. The same criminal methods are in active use against US institutions today. The defense window is narrow: the first four hours are the only ones that matter.

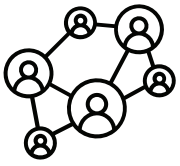
Scenario 4: Third-Party and Vendor Breach

$15M–$200M

A software provider, cloud platform, or technology partner that has access to the bank's systems is compromised through no failure of the bank's own controls. The bank's customers, data, or operations are affected anyway. Regulatory and industry data consistently show that a significant share of banking operational losses involve a third party. Because many banks share the same core vendors, a single supply-chain attack can affect dozens of institutions simultaneously — and each one faces the same regulatory obligations, the same customer notifications, the same reputational exposure.

Scenario 5: Customer Data Mass Breach

$50M–$500M



Millions of account records — transaction histories, personal identifiers, account numbers — are stolen and sold. Federal banking regulators require notification within 36 hours. The FTC Safeguards Rule triggers a 30-day FTC notification obligation. State attorneys general — led by New York and California — open parallel investigations. Class action litigation follows within weeks. The institution's name appears in every news cycle for months. Deposit outflows are measurable and prolonged. Financial services consistently ranks among the highest per-record breach costs of any industry. There is no such thing as a contained mass breach.

TWO RISKS ARE EARLIER IN THEIR DEVELOPMENT **BUT REQUIRE EXECUTIVE ATTENTION NOW.**

1. Artificial intelligence is generating US regulatory findings today — credit models discriminating against protected classes under the Equal Credit Opportunity Act, staff feeding customer financial data into external AI tools in violation of GLBA — and the enforcement posture of the CFPB, OCC, and Federal Reserve on AI model governance is hardening rapidly. The OCC, Federal Reserve, and FDIC have each confirmed that SR 11-7 model risk management requirements apply to AI systems, and it is an active examination standard.

2. Post-quantum computing will, within the next decade, break the encryption protecting every wire transfer, every stored record, and every regulatory communication the institution has ever sent. NIST finalized the first post-quantum cryptography standards in 2024 (FIPS 203, 204, 205). Adversaries are already collecting encrypted data today, waiting for the capability to decrypt it.

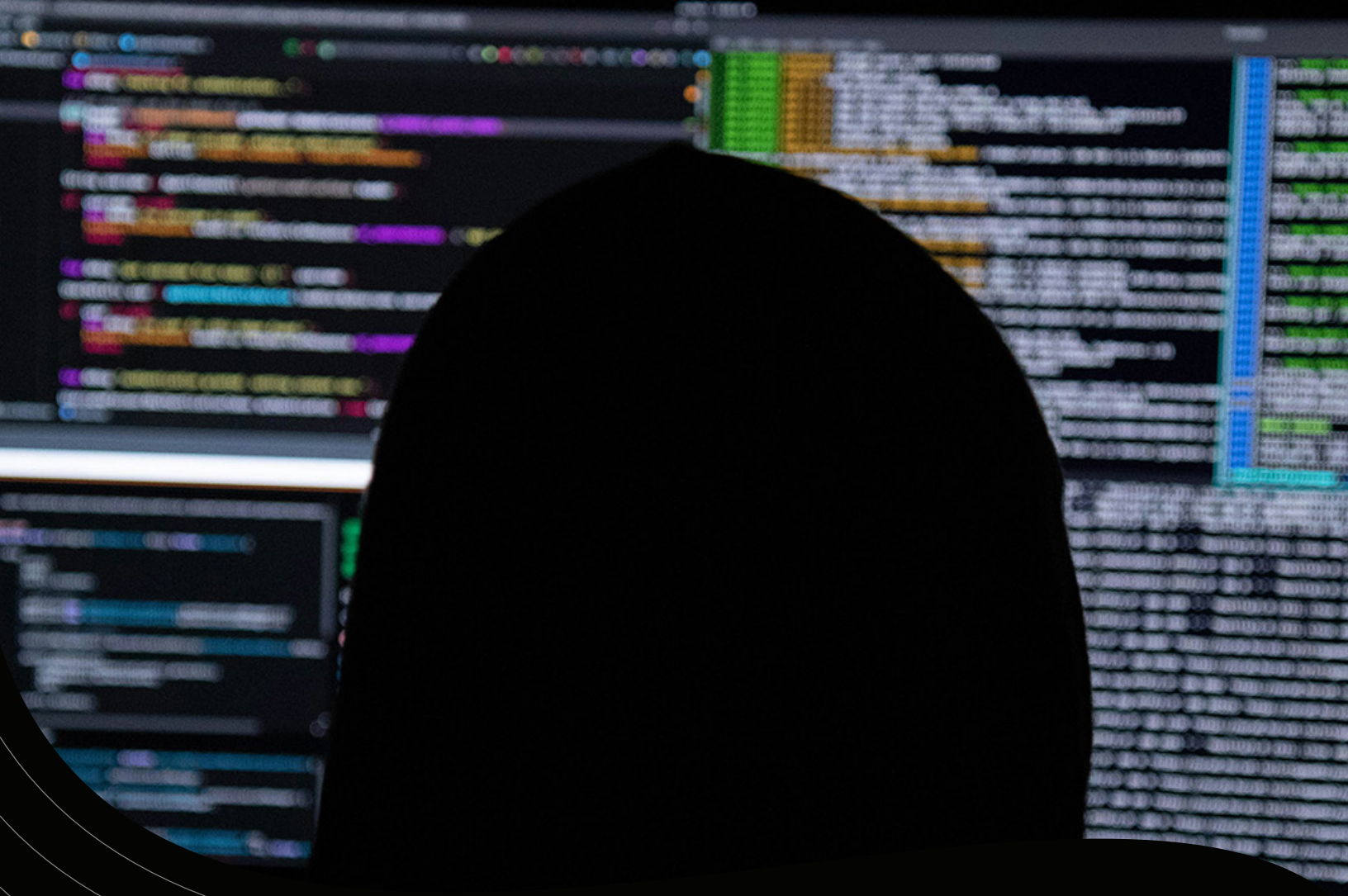
Both risks require funded program decisions now, not monitoring.

One Question. Answer It Now.

If your core banking systems were encrypted by attackers at 3 AM tonight — customers locked out, payments stopped, settlements at risk — what would happen next?

Who makes the decision to halt payment processing? How quickly can you restore from backup — and when was that last tested? What do you tell customers, and who authorizes that message? Does a regulatory notification go out tonight, and to whom?

If those answers require research, the gap they reveal is more consequential than anything else in this document. The answers must exist before the call comes — because during the call, there is no time to find them.



SECTION 02

WHO IS RESPONSIBLE FOR MAKING IT HAPPEN

> **THE ORGANIZATIONS ATTACKING BANKING INFRASTRUCTURE ARE NOT TEENAGERS WITH LAPTOPS.** Two categories account for most of the risk: criminal ransomware groups that have industrialized financial extortion, and nation-state actors with patience, resources, and strategic objectives that go beyond any single institution. Understanding the difference matters — they require different responses.

The Ransomware Economy

Ransomware has been industrialized. Criminal groups operate with specialist divisions — intrusion teams, access brokers, ransomware developers, negotiators, money launderers — with the operational structure of a mid-size company. Banking is a premium target category. They know that a bank whose systems are down faces a regulatory investigation within 36 hours, customer attrition beginning immediately, and operational costs that are multiples of any ransom demand. The leverage is not just technical. It is the regulatory and reputational clock that starts ticking the moment systems go dark.

The entry point, in most cases, is not a sophisticated attack on the bank's perimeter. It is a phishing email to an employee, or compromised credentials at a technology vendor with access to the bank's network. The bank's most expensive security investments are often irrelevant if an attacker can simply log in as a legitimate user or vendor. That is the conversation worth having with the CISO: not what technical defenses exist, but how an attacker would most likely bypass them — and whether that specific pathway has been addressed.

Ransomware groups now operate like companies, with specialized teams for intrusion, development, negotiation, and money laundering.

The State-Sponsored Threat

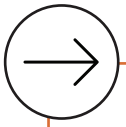
North Korea runs a cyber program that is, in effect, one of the world's most successful financial crime operations. Since 2017, Lazarus Group — the operational unit responsible — has stolen more than $3 billion from financial institutions. It is the primary hard-currency earner for a sanctioned regime. They do not improvise. A Lazarus operation follows a consistent pattern: months of open-source research on the target, phishing emails to payment operations staff, patient lateral movement through the network, and final execution during a weekend or public holiday — when the fewest people are watching and response is slowest.

Russia and China take a different approach. Their interest is less about immediate theft and more about long-term access — collecting intelligence on sanctions enforcement, M&A flows, and trading positions. They pre-position for potential disruption when geopolitical conditions warrant it. They may have been inside a network for a year before the organization knows it. The risk is not just what they do today. It is what they could do the moment doing it becomes useful to them.

The Human Dimension

The fastest-growing fraud category in banking today uses artificial intelligence to generate convincing real-time voice and video impersonation of executives and clients. A treasury manager joins what appears to be a video conference with the CFO and several colleagues — all deepfake recreations — with a credible business context and a sense of urgency, requesting an immediate wire transfer.

Individual incidents using this technique have reached $25 million in at least one documented case. The defense is not a technology purchase. It is a process: a pre-agreed, mandatory callback on an independent number for any transfer above threshold, regardless of how credible the request appears. That process must exist before the call comes.



The Questions That Reveal Whether You Are Actually Protected

On entry points: "How would an attacker most likely gain initial access to our systems today — phishing, vendor credentials, or something else — and have we specifically addressed that pathway?"

On detection speed: "If someone compromised a payment operations employee's credentials right now and started moving through our network, how long before anyone noticed?"

On vendor exposure: "Which of our technology vendors has direct access to our core banking or payment systems — and what do we actually know about their security posture?"

SECTION 03

THE REGULATORY STAKES

THE OCC, FEDERAL RESERVE, FDIC, AND NYDFS have each intensified enforcement on IT risk governance in the past three years. IT failures that once produced recommendations now produce consent orders. And the US enforcement structure is uniquely severe: financial penalties, asset growth restrictions, and personal accountability for named executives — simultaneously.

How a Finding Becomes a Consent Order

When federal examiners — OCC, Federal Reserve, or FDIC — find IT risk management deficiencies during an examination, they issue a Matter Requiring Attention. This sounds administrative. It is not. An MRA is a regulatory directive with a fixed deadline and a formal escalation path. Miss that deadline — or remediate inadequately — and it becomes a formal enforcement action. The enforcement action becomes the basis for a consent order. A consent order is a public, legally binding agreement that specifies penalty payments, asset growth restrictions, mandatory governance changes, and named executive accountability.

The largest US banking enforcement actions — BSA/AML consent orders exceeding $1 billion against major institutions — have consistently cited inadequate transaction monitoring systems and IT control failures as primary root causes. The CEO cannot acquire another bank. The Board cannot approve new business lines. The remediation program is supervised by the regulator, not management.

A Matter Requiring Attention is not a recommendation. It is the first step in the enforcement process that can end in a public consent order.

What executives consistently underestimate is that governance failures are as actionable as control failures. A Board that has not formally approved an IT risk appetite. An IT security function without a structurally independent reporting line to the CRO or CEO. Internal Audit that is not demonstrably independent. IT risk reporting that reaches the Board in technical metrics rather than financial terms. These structural deficiencies produce MRAs on their own, independent of whether any technical control has failed.

The examiner is not just asking whether the bank has strong IT security. They are asking whether the Board is genuinely overseeing it — and whether that oversight is documented in a form they can review.

The Notification Problem: Multiple Clocks, Running Simultaneously

When a significant IT incident occurs, several regulatory clocks start at once — and their deadlines are shorter than most institutions' legal review processes. Federal banking regulators — the OCC, Federal Reserve, and FDIC — require notification within 36 hours of a significant IT security incident. The SEC requires public disclosure of a material cybersecurity incident within 4 business days of a materiality determination. Under the updated FTC Safeguards Rule, financial institutions must notify the FTC within 30 days of a breach affecting 500 or more customers.

Customer notification obligations are governed separately by applicable state breach notification laws — the most stringent require notification as expeditiously as possible. For institutions licensed under the NYDFS Cybersecurity Regulation (23 NYCRR 500), a reportable cybersecurity event requires notification to the Department of Financial Services within 72 hours.

The practical implication is sharp: during an active incident, the CEO and General Counsel will be asked to make notification decisions within hours based on incomplete information. Institutions that handle this well have pre-structured those decisions — the criteria, the templates, the decision authority — before any incident occurs. Institutions that leave it to real-time legal deliberation routinely miss deadlines and convert a reportable incident into a separate regulatory violation.

SIX US FRAMEWORKS EVERY EXECUTIVE SHOULD RECOGNIZE

Framework 1: OCC Heightened Standards (12 CFR 30, App. D)

What it Governs:
Board approval of IT risk appetite; executive accountability; independent IT security oversight; three-tier governance structure

Maximum Consequence:
Consent order; asset growth cap; named executive liability

The Examiner Questions You Will Be Asked:

1. "Show us the Board minutes where IT risk appetite was approved."
2. "Show us the CISO's reporting line."
3. "How often does the Board discuss IT risk in financial terms?"

Framework 2: BSA / AML (Bank Secrecy Act)

What it Governs:
Systems that monitor transactions for money laundering, terrorist financing, and sanctions violations; SAR filing obligations

Maximum Consequence:
$1M per day in civil penalties; criminal referral; consent order exceeding $1B

The Examiner Questions You Will Be Asked:

1. "What happened to your transaction monitoring during last quarter's system outage?"
2. "How many SARs were filed late, and what caused the delay?"

Framework 3: FFIEC IT Examination Handbook

What it Governs:
IT risk management across all federally supervised institutions; examiner standards for governance, resilience, incident response, and vendor management

Maximum Consequence:
MRAs, MRIAs, and formal enforcement escalation across OCC, Federal Reserve, FDIC, and NCUA

The Examiner Questions You Will Be Asked:

1. "Show us your board-approved IT risk appetite."
2. "Show us your last business continuity test results and recovery time outcomes."

Framework 4: NYDFS Cybersecurity Regulation (23 NYCRR 500)

What it Governs:
Cybersecurity governance, controls, and incident reporting for all DFS-licensed entities; CISO appointment; 72-hour incident notification

Maximum Consequence:
Civil penalties; license suspension; named senior officer accountability

The Examiner Questions You Will Be Asked:

1. "Show us your most recent CISO report to the Board."
2. "When did you notify DFS after the incident, and what was your basis for that timeline?"

Framework 2: GLBA Safeguards Rule (FTC / CFPB)

What it Governs:
Protection of customer financial information; FTC notification within 30 days of a breach affecting 500+ customers; customer notification obligations governed by applicable state law

Maximum Consequence:
FTC enforcement; state AG enforcement; civil litigation

The Examiner Questions You Will Be Asked:

1. "When did you notify the FTC, and what triggered the 30-day clock?"
2. "What state notification obligations applied, and were all deadlines met?"

Framework 6: SEC Cyber Disclosure Rule

What it Governs:
Public disclosure of material cybersecurity incidents within 4 business days; annual disclosure of cybersecurity governance and risk management

Maximum Consequence:
SEC enforcement action; securities class action litigation

The Examiner Questions You Will Be Asked:

1. "Who made the materiality determination?"
2. "What criteria did you apply?"
3. "Why did disclosure take longer than 4 business days?"

The examiner questions in the right-hand column are not hypothetical. They appear in examination workpapers and enforcement documents. Any executive who cannot answer them confidently — without preparation — has identified the gap that the next section addresses.

SECTION 04

WHAT DETERMINES OUTCOMES

THE QUESTION POSED AT THE END OF THE PREVIOUS SECTION — what happens if your core systems are encrypted at 3 AM tonight — has a direct answer. It depends on three decisions made before that night. To illustrate: two institutions face the same ransomware attack. One is back online in four hours. The other is still recovering four weeks later, under active regulatory investigation, with $150 million in costs and growing. The difference was not the attack. It was three decisions made before it.

DECISION ONE: Where Are the Backups, and Can They Actually Be Used?

Ransomware groups encrypt backup systems alongside primary systems. They do this deliberately — it eliminates the recovery option and maximizes ransom leverage. The groups that hit banks specifically look for backup servers connected to the same network, using the same administrative credentials. At most legacy banking environments, they find them. The architectural decision — storing backups in isolated systems with completely separate credentials, tested weekly with a documented restore — is the single most consequential IT risk investment a bank can make. An institution that has made this decision recovers in hours. One that has not recovers in weeks, if at all.

THE CEO'S QUESTION: "When did we last successfully restore our core banking system from backup, and how long did it take? Is that answer documented and current?"

DECISION TWO: Can an Attack in One System Spread to All of Them?

The reason a single ransomware infection can take down an entire bank's operations is that most banking networks were designed for maximum connectivity — systems that need to communicate can reach each other directly. Separating payment systems, core banking, trading platforms, and corporate IT into isolated zones means that a compromise in one area stays in that area. It does not automatically reach payment infrastructure. It does not reach the backup servers. It does not reach the SWIFT terminal. This is an infrastructure project, not a technology purchase. It takes 6–12 months to implement correctly. Done well, it is the difference between a contained incident and a catastrophic one.

THE CEO'S QUESTION: "If an attacker compromised one of our branch IT systems tonight, could they reach our payment processing systems from there?"

DECISION THREE: Who Can Act Without Waiting for a Call?

In a major IT incident, the costliest delays are not technical. They are governance delays — the time spent seeking authorization for decisions that had not been pre-approved. Who can halt payment processing? Who authorizes the regulatory notification? Who calls the external crisis firm? Who approves the customer communication? In an active incident, each of these waits multiplies exposure. The institutions that manage major incidents well have documented, pre-authorized decision frameworks that can be executed immediately, without a 45-minute management call at 3 AM.

THE CEO'S QUESTION: "Does our incident response plan include pre-authorized decisions for the scenarios we are most likely to face — and has a realistic exercise confirmed that those decisions can actually be executed under pressure?"

Why IT Security Investment Is a Business Decision, Not a Technology Budget

As a representative example: a $5 million program to build genuinely isolated backup systems can reduce the direct cost of a ransomware recovery from an estimated $150 million to $5 million. That is a 30-to-1 return before accounting for avoided regulatory penalties and reputational damage. Network segmentation costing approximately $8 million materially reduces the probability that a compromised branch system ever reaches payment infrastructure. These are not technology expenses. They are the most straightforward expected-value calculations in the risk function.

The framing that changes budget conversations: do not ask how much a security investment costs. Ask what the institution retains in expected loss if it chooses not to make it. An institution that decides not to build isolated backup infrastructure is not saving $5 million. It is accepting a probability-weighted expected loss that independent industry analysis places above $40 million annually for a mid-size institution, plus the tail risk of a catastrophic event. That is a risk transfer decision, not a budget decision — and it belongs at the executive level.

A ransomware incident rarely becomes catastrophic in the moment. It becomes catastrophic months earlier when backup isolation, network segmentation, and incident authority were deferred as "next year's projects."

How to Translate Technical Briefings Into Business Decisions

When Your CISO says: “We have 847 unpatched vulnerabilities.”

The useful question: “How many of those could give an attacker access to our payment systems or customer data — and when will those specific ones be fixed?”

Technical metrics are inputs, not outputs. The output is a financial exposure and a timeline. If the CISO cannot convert a technical metric into a dollar consequence and a remediation date, the reporting process needs to change — not the executive’s willingness to engage with technical detail.

These three decisions — backup isolation, network segmentation, and pre-authorized response — are among the nine governance decisions in Section 07. They are the three where the engineering choices made by the CIO most directly determine outcomes. The remaining six address governance structure, regulatory compliance, reporting, vendor risk, and emerging technology — all of which are equally non-optional.

SECTION 05

THE CIO'S ACCOUNTABILITY

> SECTION 04 IDENTIFIED THE THREE DECISIONS that determine whether a major incident is a four-hour recovery or a four-week one. This section names who owns them. The CIO is the delivery owner for everything this document recommends. The threat is real, the regulatory requirements are clear, and the controls are well understood — but none of them exist without someone who builds and operates the infrastructure they run on. That is the CIO's role, and it is the most consequential one in the institution's IT risk program.

The tension the CIO carries is real and worth naming. Banking IT must simultaneously maximize availability — customers and regulators demand near-perfect uptime — and implement security controls that, done correctly, add friction and reduce connectivity. Network segmentation slows some workflows. Privileged access management adds steps to administrative tasks that previously took seconds. Immutable backup architectures require investment that competes with capability budgets. These are the genuine delivery challenges the CIO must solve. Solving them well is the difference between security that works and security that gets worked around. The CIO's most important contribution to IT risk management is not any single control — it is architecture.

Three decisions determine whether an institution recovers from a major incident in hours or weeks.

FIRST: Whether backup storage is genuinely isolated and uses credentials completely separate from production systems.

SECOND: Whether critical systems are segmented so that a compromise in one area cannot propagate to all others.

THIRD: Whether the engineering organization has built infrastructure that supports pre-authorized response decisions under pressure.

Each is a CIO delivery responsibility. Each requires sustained investment, careful planning, and organizational authority to implement over the resistance of short-term operational priorities.

The CIO's Specific Accountability Domain

BACKUP ARCHITECTURE AND RECOVERY READINESS.

The CIO owns the infrastructure that determines recovery time. Isolated backup storage with authentication credentials independent of production systems, tested weekly with a documented restore and a verified recovery time — this is engineering delivery, not policy. The CIO should be able to state, without looking anything up, when the last successful restore test was, how long it took, and whether that result meets the institution's regulatory commitment.

NETWORK SEGMENTATION AND BLAST RADIUS CONTROL.

Separating core banking, payment systems, trading platforms, and corporate IT into isolated zones is a major network architecture project — typically 6–12 months to complete. It requires the CIO to manage real operational disruption along the way. The CIO who has completed this has materially reduced the institution's worst-case ransomware scenario. The CIO who has not has accepted a risk that no detection capability compensates for.

THIRD-PARTY ACCESS GOVERNANCE.

Every technology vendor with direct access to production systems is a potential entry point for attackers. Routing all vendor remote access through a managed gateway — with session recording, time-limited credentials, and audit trails — is an infrastructure decision the CIO owns. Undocumented vendor access pathways are among the most common root causes of banking security incidents, and they are invisible to every control downstream of the access point.

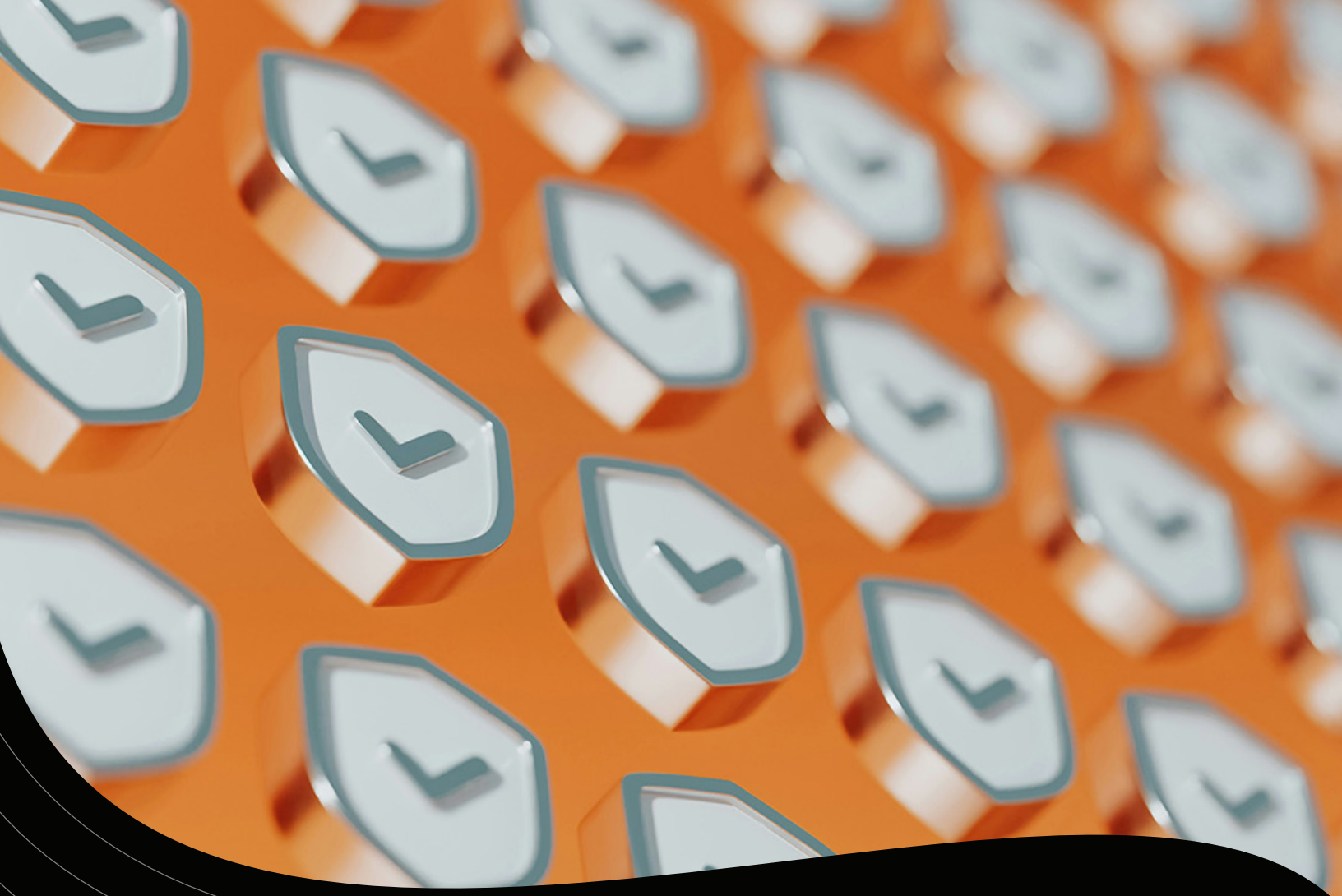
INCIDENT RESPONSE INFRASTRUCTURE.

When a major incident occurs, the CIO's team will be executing the recovery. The decisions made before the incident determine whether the plan on paper can be executed under pressure. Can systems be isolated cleanly? Can network zones be sealed without taking down unaffected services? Is backup restoration automated or manual? A response plan that depends on manual steps, undocumented system dependencies, or unavailable credentials will fail when it is needed most.

The Question the CIO Should Be Able to Answer Without Looking It Up

"If ransomware encrypted our core banking environment at 3 AM tonight, what is our recovery time to restore payments — and what are the three things most likely to prevent us from hitting it?"

The answer to that question — specific, honest, and based on the last actual restore test — is the most useful single input the CIO can give to a Board Risk Committee. It tells the Board what the institution's real resilience position is, what the current gaps are, and what investment is needed to close them. It is also the conversation that turns IT risk from an abstract governance topic into a concrete operational one.



SECTION 06

GOVERNANCE

> **THE BANKS THAT MANAGE IT RISK BEST DO NOT NECESSARILY HAVE THE BEST TECHNOLOGY.** They have governance structures that ensure the right information reaches the right people with enough time to act — and accountability structures that mean someone's career depends on whether those decisions were made correctly.

The Structure That Matters

Good IT risk governance has three observable characteristics, all of which regulators assess directly during examinations. The Board receives IT risk reporting in financial terms — not a technology update, but a clear assessment of the institution's exposure, whether it is moving in the right direction, and what management is doing about the most material gaps.

The CISO has a structurally independent reporting line to the CRO or CEO, ensuring security assessments reach executive leadership without filtering through the function whose infrastructure is being assessed. And the institution has a formally documented, Board-approved IT risk appetite that specifies — in numbers, not narrative — the financial exposures and operational conditions the institution will and will not accept.

The CIO and CISO relationship is worth addressing directly, because it is frequently misunderstood as a conflict. It is not. The CIO owns delivery: the infrastructure, the platforms, the uptime, and the engineering teams that build and operate the controls the CISO defines. The CISO owns independent assessment: setting security standards, measuring control effectiveness, and reporting the institution's risk position to the CRO and Board. That independence requires not assessing systems you also own. When both roles are working correctly, the CIO is the institution's most important implementation partner — and the CISO is the independent voice that confirms it is working.

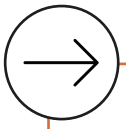
The governance structure that supports both gives the CIO full operational authority over IT delivery, and the CISO full independence over risk assessment and escalation. Neither role is diminished by that structure. Both are protected by it.

Effective IT risk governance requires three things: Board reporting in financial risk terms, an independent CISO reporting to the CRO or CEO, and a Board approved IT risk appetite with measurable limits that align CIO delivery with independent CISO oversight.

What the Board Needs to Receive — and What It Means to Actually Read It

A quarterly IT Risk Report to the Board Risk Committee serves two masters simultaneously: it is a governance document, and it is an examiner exhibit. Regulators review Board minutes to assess whether executives engaged substantively with IT risk — challenged assumptions, asked for more information, made documented decisions. A Board that approves an IT risk update without asking a question is not governing. It is witnessing.

The report should contain the top five risks expressed in dollar terms — not vulnerability counts, not security ratings, but financial exposure ranges tied to documented scenarios. It should show trend lines for each — is the exposure growing or shrinking? It should include every open regulatory finding with its owner, its deadline, and the evidence of progress. It should summarize every serious incident from the quarter with what caused it and what has changed as a result. And any budget requests should be framed as expected loss reduction — the CFO and the Board should be able to see the return on the investment, not just the cost of it.



The Governance Failure That US Examiners Find Most Often

The single most commonly cited IT governance deficiency across OCC, Federal Reserve, FDIC, and NYDFS examinations is the absence of a Board-approved, quantified IT risk appetite.

Not a narrative description of values. Not a list of control objectives. A document that specifies the financial loss thresholds, system availability standards, and operational conditions the Board has formally approved as the institution's risk tolerance — reviewed against actual conditions within the past 12 months.

If this document does not exist, it is an MRA waiting to be written. It takes weeks to develop and a Board meeting to approve. The cost of not having it dwarfs the cost of creating it.

SECTION 07

THE NINE DECISIONS

NINE DECISIONS. SHARED ACROSS THE C-SUITE. **NONE OF THEM OPTIONAL.**

Three of these — backup isolation, network segmentation, and pre-authorized response — were developed in Section 04 as the architectural decisions that determine recovery outcomes. They appear here because they require formal Board or executive ownership, not just CIO execution. The remaining six address governance structure, regulatory posture, reporting, vendor risk, and emerging technology obligations. Together, these nine are the complete governance checklist for IT operational risk in US banking.

These are not requests for IT approval or endorsements of a security strategy. They are governance obligations — the specific choices that determine whether the institution is prepared, whether regulatory obligations are met, and whether the right people have the authority to act when it matters. Each is assigned to the role that owns it. Each one either exists and is current, or it represents a gap with a measurable consequence attached.

1

Owner: Board • CRO

Formally approve an IT risk appetite with quantified thresholds — not a narrative, a document with numbers. This is the most common IT governance MRA across US banking examinations. Examiners will ask for it by name on day one. Its absence is an enforcement finding independent of how strong the underlying controls are.

Ask: Does a Board-approved IT risk appetite document exist? Has it been reviewed against actual conditions in the last 12 months?

2

Owner: CEO • CRO

Establish a governance structure in which the CISO has an independent reporting line to the CRO or CEO — and in which the CIO has unambiguous delivery authority over IT infrastructure and operations. The CISO needs independence to report security failures honestly, without the conflict of assessing systems they also own. The CIO needs clarity that they own delivery — architecture, uptime, engineering — not security oversight. Blurring these roles creates the structural ambiguity that produces regulatory findings. Separating them cleanly protects both.

Ask: Is the CIO's delivery authority formally documented? Does the CISO have a direct, independent escalation path to the Board? Are both roles clear on where their accountability begins and ends?

3

Owner: CIO

Confirm the CIO can demonstrate that backup systems are isolated, independently credentialed, and have been successfully restored within the institution's committed recovery timeframe — tested within the last 30 days. This is the single architectural decision that determines whether a ransomware event is a 4-hour recovery or a 4-week one. It is an engineering delivery responsibility, not a policy. If the answer requires research, the gap is already present.

Ask: When did we last successfully restore core banking from backup? How long did it take? Is that result documented and does it meet our regulatory commitment?

4

Owner: CIO

Confirm network segmentation isolates payment systems, core banking, and corporate IT so that a compromise in one zone cannot propagate to others. The reason ransomware can take down an entire institution rather than a single system is uncontrolled network connectivity. Segmentation is the architectural control that limits blast radius. Without it, no detection or response capability compensates.

Ask: If an attacker compromised one of our branch systems tonight, could they reach our payment processing infrastructure from there? When was this last tested?

5

Owner: CRO • CISO • CIO

Establish quarterly IT risk reporting to the Board Risk Committee in financial terms — dollar exposure, trend direction, open regulatory findings. Boards that cannot demonstrate substantive engagement with IT risk in financial terms receive governance enforcement actions independent of technical control quality. The report is an examiner exhibit.

Ask: Does the Board currently receive IT risk reporting that quantifies financial exposure — not just security metrics? Does it include the status of every open regulatory finding?

6

Owner: CRO • CISO • CIO

Review every open regulatory finding with its owner and remediation deadline. Confirm the Board has visibility on all of them. Every MRA past its deadline compounds. There is no risk management priority that outranks an open regulatory finding with a missed deadline. Not a security investment. Not a technology project. The MRA comes first.

Ask: How many open MRAs and MRIAs does the institution currently have? How many are past their remediation deadline?

7

Owner: CEO • CIO • CISO

Pre-authorize the decisions that cannot wait for a management call during an active incident. The costliest delays in major IT incidents are governance delays — time spent seeking approval for decisions that should have been pre-approved. Every 30 minutes of authorization delay during a payment infrastructure incident multiplies financial and regulatory exposure.

Ask: Does our incident response plan include pre-authorized decisions for payment system isolation, regulatory notification, and customer communication? When was this last tested under realistic conditions?

8

Owner: CIO • CRO

Confirm every critical technology vendor has a documented, tested plan for replacement if they fail or are compromised. Regulatory and industry data consistently show that a significant share of banking operational losses involve a third party. Concentration in core vendors without tested exit plans is a regulatory deficiency and a risk that internal controls cannot compensate for.

Ask: Which vendors, if compromised or unavailable tomorrow, would immediately stop our core operations — and do we have plans that have actually been tested?

9

Owner: CEO • CIO • CRO • CISO

Approve an AI governance policy aligned with SR 11-7 and ECOA/CFPB fair lending requirements — and fund a multi-year post-quantum cryptography migration plan against NIST FIPS 203/204/205. AI credit models are under active CFPB and OCC scrutiny for discriminatory outcomes. Regulators have confirmed that SR 11-7 model risk management requirements apply to AI systems, and it is examined today. NIST's 2024 post-quantum standards set the migration target; institutions that begin planning now will face significantly lower cost and disruption than those that wait.

Ask: Have our AI credit models been validated for fair lending compliance under SR 11-7? Has the Board approved a funded roadmap to migrate critical systems to post-quantum cryptography?

SECTION 08

WHAT LEADERSHIP SHOULD TRACK

ONCE THE NINE DECISIONS HAVE BEEN MADE, six metrics tell leadership whether they are holding. Each maps directly to one or more of the decisions above — and each one, if it moves into the critical range, signals that a decision has either not been made or has not been properly executed.

Six Numbers

If any one of them is in the red column, something material is wrong — and management should be able to say exactly what it is and when it will be fixed.

WHAT TO TRACK	HEALTHY	WARNING	CRITICAL	WHY IT MATTERS AT THE EXECUTIVE LEVEL
Core banking system availability	Above 99.99%	99.95–99.99%	Below 99.95%	Below 99.99% means the bank is already spending its annual allowance of system downtime. A second incident in the same year may breach customer and regulatory commitments.
Time to detect a security incident	Under 2 hours	2–8 hours	Over 8 hours	Every hour an attacker is inside the bank's systems undetected is an hour they can move toward payment systems or customer data. An 8-hour detection gap is near-total adversary freedom of movement.
Regulatory findings open past their deadline	None	1–2 findings	More than 2	Overdue findings are the direct precursor to enforcement action. More than 2 open past deadline is a material governance risk requiring CEO attention.
Backup restore test — last successful result	Passed within 30 days	Passed 30–90 days ago	Not tested or failed	This single indicator determines whether the institution can recover from ransomware in hours or weeks. If the answer is not immediately available, the gap is the answer.
Transaction monitoring system availability	Above 99.9%	99.5–99.9%	Below 99.5%	Downtime in the system that monitors transactions for money laundering creates regulatory filing obligation gaps that carry the same consequences as deliberate non-compliance — regardless of whether any actual financial crime occurred.
Critical vendor annual assessment completion	Above 90%	75–90%	Below 75%	The percentage of the bank's critical technology vendors that have completed an independent security assessment within the last 12 months with no critical findings outstanding. Each vendor below this standard is a potential uncontrolled entry point into the bank's systems.

CONCLUSION

The six metrics in the previous section are the ongoing signal. The nine decisions are the foundation. What follows is the reason both matter.

> **The institutions that handle major IT events well are not the ones with the most sophisticated technology. They are the ones where the right decisions were made before the crisis — and where governance structures ensured those decisions were actually executed.**

Nothing in this brief describes an unsolvable problem. The threat environment is severe. The regulatory burden is real. The financial exposures are large. But every risk covered here has a known response, a documented framework, and a body of industry experience behind it. What separates institutions that manage IT operational risk from those that are managed by it is not capability. It is whether the decisions that belong at the executive level have actually been made.

Those decisions are not about technology. They are about governance, accountability, and investment sequencing. They are about whether the CISO has genuine independence and the CIO has the authority and resources to deliver. Whether the Board receives information it can act on. Whether backup systems have been tested this month. Whether a realistic exercise has confirmed that the response plan works. Whether the nine decisions in this brief have been made, documented, and reviewed.

Three questions. They cut across all nine decisions above and compress the governance question to its essence. If the answers are immediate, confident, and specific, the governance is working. If any of them requires research, the gap it reveals should move to the top of the agenda.

- → “What is our largest single IT operational risk, in dollar terms — and is our exposure to it growing or shrinking?”
- → “How many open regulatory findings do we have, and which ones are at risk of missing their deadline?”
- → “If our core banking systems went down tonight, what happens — and when was that scenario last rehearsed?”

The answers to those questions already exist somewhere in the institution. The governance question is whether they reach this room before the call does.

ABOUT MALA TECHNOLOGY ADVISORS

TECHNOLOGY INNOVATION STARTS HERE

MALA Technology Advisors is a leading technology advisory firm helping businesses modernize, adapt, and grow through smart, strategic use of technology. MALA stands for Modernization, Agility, Leadership, and Advancement—the values that guide everything we do. As a vendor-neutral strategic partner, we work with forward-thinking organizations to align business and information technology goals. Using our 4-Pillar approach, we help clients reimagine, restructure, and renew business IT initiatives to create agile and resilient organizations.

Our Services

Managed Cybersecurity · Cloud Services · Network and SD-WAN · Managed IT · Communications as a Service · IoT and Wireless · Professional Services · Devices

How We Work

Our expert team of technology and business professionals works side-by-side with your organization across a proven engagement model: IT Strategy development, Environment Assessment, Vendor Identification and Selection, Proposed Solution design, and ongoing Account Management. We don't just consult—we partner to simplify complexity, accelerate progress, and unlock new opportunities for growth.

What Sets Us Apart

Our team is a diverse network of consultants and industry professionals with a global mindset and a collaborative culture. We focus on Workplace Technology Innovation, Flexibility in Integration and Implementation, Perpetual Enablement, and Human Connection. The speed of change in technology today is driving a matched evolution of the IT landscape—and more than ever, IT departments rely on MALA Technology Advisors to help them innovate and plan for the future.

GET IN TOUCH

500 Commercial Street, Suite 502, Manchester, NH 03101

(603) 802-2469 · info@malatechadvisors.com

malatechadvisors.com

MALA
TECHNOLOGY
ADVISORS