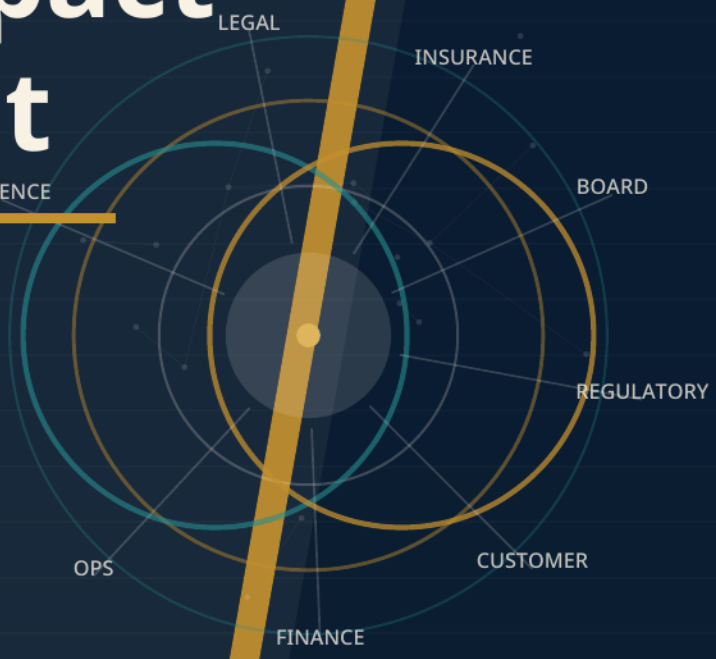
CYBANTAGE®

SECURITY INCIDENT IMPACT ADVISORY

Guide to Business Impact Management

When the Security Event Becomes a Business Event



Security response addresses the threat.

BIM addresses what the threat becomes.

An executive operating model for legal, insurance, regulatory, board, customer, operational, financial, and evidence pressure during serious cyber incidents.

Rod Andes
Executive Security Impact Advisor
Cybantage Press | 2026

EXECUTIVE CYBER INCIDENT READINESS

Cybantage Guide to Business Impact Management

When the Security Event Becomes a Business Event

Published by Cybantage Press

This guide is a framework, not an organization-specific plan. The BIM framework is common. The BIM plan is specific. No organization should treat this guide as a ready-to-execute incident response plan. The framework must be translated into an organization-specific plan that reflects the organization's actual industry, regulatory obligations, insurance policies, leadership authority, vendor ecosystem, and business model.

For permissions requests or licensing inquiries, contact:

Rod Andes | randes@cybantage.com | (629) 275-2770 | www.cybantage.com

Cybantage helps leadership teams prepare for the business pressures that follow a security incident — before those decisions have to be made under pressure.

Table of Contents

Foreword

What This Guide Is For

Most organizations know what to do when a system goes down. Very few know what to do when the business comes under pressure because of it.

That gap is what this guide addresses.

This is not a technical manual. It does not describe how to detect an intrusion, how to run a forensic investigation, or how to rebuild a compromised network. Those resources exist, and the teams who use them are skilled at what they do.

This guide addresses what happens after security teams begin their work — the second event that starts while the first is still unfolding. The insurance notice that must go out within hours. The legal privilege question that governs every communication made from that moment forward. The board that expects to hear something before it reads about it in the news. The customers waiting for a statement. The regulator who will want a timeline. The CFO trying to understand what this event is going to cost.

Those are not technical problems. They are business problems. And they require a business response model.

Business Impact Management is that model.

I have spent years working with leadership teams in the hours and days that follow serious incidents. The organizations that manage those events best are not the ones with the most security tools. They are the ones where leadership already knows what to do. Where decision authority is clear. Where the insurer has already been identified and the notice criteria have already been documented. Where legal counsel is already engaged under a structure designed to support privilege where available. Where the board knows what it will receive and when.

The organizations that struggle most are not poorly secured. They are unprepared for the business consequences of what their security team discovers.

This guide is designed to close that gap.

Every chapter in this guide reflects something I have seen fail in a real incident. Every framework reflects something that worked. I am not writing as an academic. I am writing as a practitioner who has sat with leadership teams at the worst possible moment and watched them discover that their business had no plan for the business event.

This guide provides the framework for building a cyber Business Impact Management plan. It does not prescribe a universal plan. A BIM plan cannot be copied from one organization to another because the business consequences of a cyber incident depend on the organization’s actual industry, revenue model, systems, customers, contracts, insurance policies, regulatory obligations, vendors, leadership authority, and board expectations.

The framework is common. The plan is specific. This guide explains what must be designed. The BIM plan documents what the organization decided. A BIM plan is not ready because the organization owns a template. It is ready when named leaders have made, documented, acknowledged, tested, and accepted the decisions required to manage the business consequences of a cyber incident.

This guide gives you that framework.

Rod Andes

Executive Security Impact Advisor

Cybantage

Why BIM Is an Executive Alignment Process, Not a Writing Project

A Business Impact Management plan cannot be created by one department in isolation.

The legal team cannot define technical containment authority alone. The CISO cannot define insurer notice obligations alone. The CFO cannot define evidence preservation requirements alone. The communications team cannot define customer messaging authority alone. The board cannot govern an incident response model it has never reviewed. The executive team cannot rely on vendors, counsel, insurance policies, authority structures, or decision paths that have not been validated before the incident.

BIM requires cross-functional decisions that most organizations have never made together.

The value of the BIM framework is that it identifies the decisions. The value of BIM implementation is that it forces the organization to make those decisions, document them, assign them to named leaders, test them under pressure, and maintain them as the organization changes.

A completed BIM plan should not be treated as a writing project. It is an executive alignment process.

Templates can organize information. They cannot resolve authority conflicts. They cannot validate insurance requirements. They cannot confirm whether outside counsel is conflict-cleared. They cannot determine whether the preferred forensic firm is approved by the cyber insurer. They cannot decide who may authorize emergency spending. They cannot make the board accept a reporting threshold. They cannot make named leaders acknowledge the responsibilities assigned to them.

Those decisions require facilitated leadership engagement.

BIM is not implemented by completing a document. It is implemented by forcing the organization to make, acknowledge, test, and maintain the decisions it would otherwise discover during the incident.

The guide explains the framework. The organization-specific BIM plan documents the decisions. The facilitation process helps leadership make those decisions before the incident makes them unavoidable.

HOW TO USE THIS GUIDE

From Framework to Organization-Specific BIM Plan

How to read and apply this guide to build an executable Business Impact Management plan.

> *This guide is not a ready-to-execute incident response plan. It is a framework for building an organization-specific Business Impact Management Plan — the executive operating model for managing the business consequences of a cyber incident.*

A cyber incident may begin as a technical event, but it can quickly become a legal, insurance, regulatory, operational, financial, contractual, customer, vendor, communications, board, law enforcement, and leadership accountability event.

This guide helps leadership identify the decisions that must be made before that happens.

The BIM Development Path

1. Understand the Second Event

Start with the core premise:

> *Security response addresses the threat. BIM addresses what the threat becomes.*

Use Part One to understand why cyber incidents create a parallel business event and why that event requires executive ownership.

Output: *Leadership understands that BIM is not a technical incident response plan. It is the business-response operating model.*

2. Identify the Required Business Decisions

Use Part Two to define how BIM activates, who owns each workstream, and who has authority to make decisions. The organization must determine:

- who can activate BIM
- who owns Executive Command
- who owns each workstream

- who can authorize containment with business consequences
- who can spend
- who can engage vendors
- who can notify the insurer
- who can contact law enforcement
- who can brief the board
- who can approve external communications

Output: *Draft activation criteria, workstream ownership, decision authority, and escalation structure.*

3. Map the Business Pressure Domains

Use Part Three to evaluate the business consequences that may activate during a cyber incident. Each organization must determine how a cyber incident could affect:

- Legal and Privilege
- Insurance and Claims
- Regulatory and Compliance
- Board and Governance
- Customer and Stakeholder Trust
- Operations and Continuity
- Finance and Revenue
- Contracts and Third Parties
- Communications
- HR and Workforce
- Evidence and Defensibility

Output: *A business-impact map showing which domains apply, who owns them, what evidence is required, and what decisions must be pre-approved.*

4. Validate the Assumptions the Plan Depends On

A BIM plan cannot rely on assumptions that have not been checked. The organization must validate:

- cyber insurance notice requirements
- approved vendor panels
- breach counsel readiness
- DFIR and recovery vendor status
- non-panel vendor coverage-risk process
- emergency spending authority

- board notification thresholds
- contract notice obligations
- critical third-party dependencies
- business-critical systems and data
- evidence and logging availability
- communication approval paths
- law enforcement and government coordination rules

Output: *Verified inputs for the organization-specific BIM Plan.*

5. Build the Organization-Specific BIM Plan

> *The framework is common. The plan is specific.*

The organization-specific BIM Plan should include the actual:

- named executives and alternates
- activation triggers
- decision authority matrix
- emergency spending limits
- law firms and outside advisors
- pre-approved vendors and retainers
- insurance contacts and claim requirements
- board thresholds
- contract notification obligations
- communication approval process
- evidence preservation locations
- situation report cadence
- open action register
- stand-down process
- corrective action governance
- leadership acknowledgment requirements

Output: *A complete organization-specific BIM Plan.*

6. Obtain Leadership Acknowledgment

> *A role is not assigned until it is acknowledged.*

Every named executive, workstream owner, alternate, emergency spending approver, board liaison, communications approver, insurance contact, legal contact, and escalation owner must confirm that they understand their role, authority, limits, dependencies, and documentation obligations.

Output: *BIM Leadership Acknowledgment and Attestation Register.*

7. Exercise the Business Event

Do not test only the technical incident. Test whether leadership can manage what the incident becomes. The exercise should test:

- BIM activation
- Executive Command
- decision authority
- emergency spending
- insurer notice
- vendor activation
- board briefing
- communications approval
- evidence preservation
- open action tracking
- stand-down readiness

Output: *Exercise findings, corrective actions, and updated BIM Plan.*

8. Maintain the Plan

A BIM Plan expires as the organization changes. The plan must be reviewed and updated when there are changes to:

- leadership
- board structure
- insurance policies
- vendors
- contracts
- business model

- systems
- regulators
- critical data
- incident response partners
- emergency spending authority

At minimum, BIM should be validated annually.

Output: *Current, tested, acknowledged, and maintained BIM operating model.*

The BIM Framework Map

Framework → Decisions → Plan → Attestation → Exercise → Maintenance

Step	What Happens	Result
1. Framework	Leadership understands BIM and the second event	Shared executive understanding
2. Decisions	The organization defines authority, ownership, spending, vendors, communications, insurance, board, and evidence rules	Required decisions are made before the incident
3. Plan	Decisions are converted into an organization-specific BIM Plan	Executable business-response operating model
4. Attestation	Named leaders acknowledge their roles and responsibilities	Accountability is confirmed
5. Exercise	Leadership tests the business event under pressure	Gaps are exposed before a real incident
6. Maintenance	The plan is updated, re-attested, and re-tested	BIM remains operational over time

PART ONE

Foundation

What Business Impact Management Is, Why It Exists, and Why Most Organizations Need It

CHAPTER 1

The Second Event

Why the Business Consequence Is the One You Are Least Prepared For

A security incident rarely stays technical. That is the central problem this guide is designed to solve.

When a security team detects a compromise, a standard set of actions begins. Alerts fire. Analysts engage. Containment protocols activate. Forensic investigation starts. The technical machinery moves.

What most organizations do not anticipate is that a second set of events begins at the same moment — events that have nothing to do with the technical response and everything to do with the business.

A compromised account does not stay a compromised account. It becomes a fraud question. It becomes an insurance notice question. It becomes a question about whether customers whose data was accessible need to be told. It becomes a board question. It may become a regulatory question. In a matter of hours, the technical event has become a business event, and the security team is not equipped — and should not be expected — to manage it alone.

What Creates the Second Event

The second event is not caused by the technical failure. It is caused by the absence of a business response model.

Consider what typically happens in the first hours of a serious incident. The security team is working. The technical facts are incomplete. The full scope is unknown. And leadership is being asked questions it cannot yet answer:

- Is this a security event or a business incident?
- Who do we notify?
- When do we notify them?
- Who is authorized to make these decisions?
- What evidence are we preserving?
- What can we say internally, and what should we not put in writing?
- Do we have any notification obligations, and if so, how long do we have?
- What does our insurance require from us right now?

These questions are not technical. They do not require a security analyst. They require a leadership team that has already worked through these decisions and knows exactly what to do.

Most leadership teams have not done that work.

That is the second event. It is the cascade of business pressures — legal, insurance, regulatory, board, customer, operational, financial, contractual, reputational — that activates when a security event crosses the threshold from technical problem to business problem.

The Gap Is Not Technical

Every year, organizations spend significant resources on security tools, compliance programs, cyber insurance, and incident response retainers. And every year, leadership teams discover during an incident that none of those investments prepared them for the business decisions they are now being asked to make.

The gap is not in security capability. It is in business response readiness.

A well-resourced SOC will detect and contain the threat. A skilled forensics team will identify the scope. But neither of them will tell leadership when to notify the insurer, how to structure communications to avoid waiving privilege, what evidence the carrier will require to support a business interruption claim, or how to document the decision record in a way that will survive a regulatory examination six months later.

Those are business decisions. They belong to a business response model.

The Two Events Running in Parallel

In every serious incident, two parallel tracks are running from the moment the event is detected.

The first track is the technical response. Security teams, IT, forensics, and incident response partners are managing detection, containment, eradication, and recovery. Their job is to stop the threat, understand what happened, and restore systems.

The second track is the business response. Legal, insurance, regulatory, board, customer, operational, financial, and communications decisions are being made — or not being made — in parallel. This track has no named owner in most organizations. It has no activation criteria. It has no decision authority matrix. It has no evidence preservation protocol.

Business Impact Management creates the second track.

BIM is a decision system, not a document set. Its purpose is to ensure that business-critical decisions are made by the right people, at the right time, with the right facts, within the right authority, using the right evidence, under the right legal and insurance constraints, and with the right documentation. BIM does not manage the technical event. BIM governs the business consequences that activate in parallel with the technical response.

> *Security response addresses the threat. Business Impact Management addresses what the threat becomes.*

Who Owns the Business Response?

That is the governing question of Business Impact Management.

It is a deceptively simple question. In most organizations, no single answer exists. The CEO assumes the CISO is handling it. The CISO assumes legal is handling it. Legal assumes the CFO has notified the insurer. The CFO assumes someone has briefed the board. Nobody has done the thing everyone assumed someone else was handling.

This is not a failure of leadership. It is a failure of pre-incident design. Organizations that perform well under business pressure during a security incident are not more talented than those that struggle. They are better prepared. They have built the response model before the incident began.

Every chapter in this guide contributes to that response model.

CHAPTER 2

Defining Business Impact Management

The Executive Operating Model for What Cyber Becomes

Business Impact Management is the executive operating model that governs the business consequences of a cyber incident.

That definition requires no technical translation. It is not a security framework. It is not a compliance program. It is not an IT governance structure. It is an executive decision-making model for the business pressures that follow a serious security event.

Security response addresses the threat. BIM addresses what the threat becomes.

What Business Impact Management Is

BIM defines six things before the incident begins:

- Who owns the business response
- When the business response activates
- Which leaders must be involved and under what authority
- What decisions must be made and in what sequence
- What evidence must be preserved and how
- What communications must be controlled, approved, and documented

Beyond those six definitions, BIM maps the specific domains that activate during a serious incident — legal, insurance, regulatory, board, customer, operational, financial, contractual, communications, workforce, and evidence — and assigns named owners and decision authority to each.

The output is not a document that sits in a policy library. It is a functional leadership infrastructure that activates when the event occurs.

What Business Impact Management Is Not

BIM is not another name for incident response. Incident response is the technical model for stopping the threat and restoring systems. BIM is the executive model for managing what the threat does to the business.

BIM is not a crisis communications plan. A communications plan defines what to say. BIM defines who has authority to approve what is said, under what legal constraints, through what approval process, and to which audiences.

BIM is not a business continuity plan. Business continuity focuses on operational resilience. BIM focuses on executive decision authority during business consequence activation.

BIM is not a compliance framework. Compliance frameworks define what controls must exist. BIM defines who owns the decision about what actions to take when those controls have failed or when regulatory notification may be required.

BIM is the coordination layer above all of them.

> *BIM does not prevent every incident. It prevents leadership from discovering its business response model during the incident.*

The One-Sentence Definition

Business Impact Management prepares leadership for the business event that follows the security event.

Every word in that sentence is doing work.

Prepares. This is pre-incident work. BIM built after the event has started is BIM built too late. The decisions that matter most in the first hours of a serious incident — who to call, what to document, when to notify, how to preserve privilege — have to be made before there is time to figure them out.

Leadership. Not security teams. Not IT. Leadership. The CEO, CFO, COO, General Counsel, Chief Risk Officer, board chair. The people who will be accountable for the business consequences long after the technical event is over.

The business event. Not the security event. The security event is what the attackers did. The business event is what it costs — in legal exposure, insurance recovery, regulatory scrutiny, customer trust, operational disruption, financial loss, and board accountability.

That follows the security event. The business event does not replace the security event. It follows it — often immediately, and often before the technical scope is fully understood.

The Framework Is Universal. The Plan Is Organizational.

Every BIM plan must be built from the organization's actual business model, industry obligations, insurance policies, contracts, revenue dependencies, operational realities, leadership authority, vendor ecosystem, and board governance structure.

A generic BIM plan creates the same false confidence BIM is designed to eliminate. The guide explains what must be designed. The BIM plan documents what the organization decided.

This distinction is not administrative. It is the difference between a plan that works and a plan that looks like it might work until it is needed. Organizations in healthcare face different notification obligations than organizations in financial services. Organizations with enterprise customer contracts face different notice requirements than those serving individual consumers.

Organizations with active government contracts face different disclosure obligations than private commercial firms.

The framework is the architecture. The plan is the building. This guide provides the architecture.

The Governing Question

> **Governing Question:** *Who owns the business response — and are they ready to act?*

That question should sit at the center of every BIM conversation. It is more useful than asking whether the organization has an incident response plan, because most organizations do. The question is whether the organization has a business response plan — and whether the people who own it are prepared to use it.

Every BIM engagement at Cybantage begins with that question. The answer shapes everything that follows.

CHAPTER 3

The Two-Event Model

Security Response and Business Response Are Not the Same Thing

Every serious cyber incident creates two events. Most organizations prepare for one. BIM prepares leadership for both.

Event One: The Security Event

The security event is the technical problem:

- A compromised credential or account
- Ransomware deployment
- Exposed or exfiltrated data
- A phishing campaign that succeeded
- Malicious actor access to systems or networks
- A third-party compromise that affects your environment
- A vulnerable system being exploited
- An outage caused by a security event
- Fraudulent activity using compromised systems or identities
- Unauthorized use of systems, accounts, or data

Security, IT, SOC, MSP, MSSP, forensics, and incident response teams lead this event. Their job is to detect what happened, contain the damage, eradicate the threat, and restore systems. They are good at this.

Event Two: The Business Event

The business event is what the technical problem causes:

- Customer impact, notification obligations, and trust erosion
- Legal exposure and privilege considerations
- Insurance claim risk and carrier notice requirements
- Regulatory review and notification deadlines
- Board scrutiny and governance documentation requirements
- Operational disruption and business continuity decisions
- Contract exposure, SLA breaches, and third-party obligations
- Revenue loss and financial impact
- Public trust damage and reputational exposure
- Executive accountability and decision record requirements
- Long-tail remediation costs and insurance recovery disputes

Leadership owns this event. Not the security team. Not IT. The CEO, CFO, General Counsel, COO, and board.

Why Organizations Prepare for One and Improvise the Other

The security event has a well-developed ecosystem of tools, frameworks, and playbooks. NIST. CISA. IR retainers. SOC procedures. Tabletop exercises. Security teams train for this. They practice it. They have runbooks.

The business event has no equivalent ecosystem. There is no standard executive playbook for the business consequences of a serious incident. There are legal guidelines, insurance policy provisions, regulatory frameworks, and board governance standards — but they exist in separate domains, owned by separate advisors, with no single operating model that connects them under a unified leadership structure.

Business Impact Management is that operating model.

> *BIM exists because most organizations prepare for Event One and improvise Event Two.*

The Consequences of Improvising Event Two

Improvising the business event is not merely uncomfortable. It is costly.

Insurance claims get disputed because notice did not go out within the required window. Regulatory penalties increase because the notification timeline was not properly documented. Legal exposure expands because communications were made before privilege was established. The board loses confidence because it was notified after the story appeared publicly. Customers leave because the communication was late, inconsistent, or incomplete. Contracts are invoked because no one was monitoring SLA obligations during the outage.

None of those outcomes are caused by the security failure alone. They are caused by the absence of a business response model.

That is what BIM prevents.

CHAPTER 4

The Eleven Business Pressure Domains

What Activates When the Incident Begins

A serious incident does not activate one business problem. It activates eleven simultaneously. Most organizations are prepared for none of them.

The following domains define the full scope of business consequence in a serious cyber incident. Each domain has its own owners, its own timeline, its own evidence requirements, and its own standards for what reasonable leadership looks like. BIM addresses all eleven before the first alert fires.

#	Domain	What It Governs
1	Legal and Privilege	Counsel engagement, privilege structure, legal exposure, evidence handling, and communication controls
2	Insurance and Claims	Carrier notice, broker coordination, claim evidence, business interruption documentation, and coverage conditions
3	Regulatory and Compliance	Notification analysis, regulatory deadlines, examination readiness, privacy review, and sector obligations
4	Board and Governance	Board reporting thresholds, oversight record, decision documentation, and executive accountability
5	Customer and Stakeholder Trust	Customer communication, retention, notification, reassurance, and account management
6	Operations and Continuity	Service delivery, production, clinical continuity, downtime decisions, and restoration priorities
7	Finance and Revenue	Cash impact, revenue disruption, fraud losses, recovery costs, and financial exposure
8	Contracts and Third Parties	Vendor obligations, customer commitments, SLAs, indemnity, and contractual notice
9	Communications	Internal messaging, external statements, media response, employee guidance, and spokesperson control
10	HR and Workforce	Employee data exposure, workforce instructions, credential resets, and insider concerns
11	Evidence and Defensibility	Decision logs, timelines, preserved artifacts, approvals, rationale, and post-incident review records

Why All Eleven Matter

Every organization will not face all eleven domains in every incident. But most organizations cannot predict which domains will activate until the incident is underway.

A phishing event looks like a security problem until it is discovered that the attacker accessed a patient database. Then it is a HIPAA notification problem. Then it is a regulatory enforcement problem. Then it is a board governance problem. Then it is an insurance problem. Then it is a customer trust problem.

The domains activate in sequence, but the preparation must happen in advance of all of them.

BIM defines ownership, decision authority, activation criteria, and evidence requirements for each domain before the incident begins. That is the difference between a leadership team that responds and a leadership team that improvises.

> *BIM prevents leadership from improvising across eleven business pressure domains at the worst possible moment.*

Cross-Domain Governance Mechanisms

Some BIM requirements cut across multiple domains. Emergency spending, law enforcement coordination, materiality review, executive attestation, and stand-down authority are not separate pressure domains. They are cross-domain governance mechanisms that must be embedded into the BIM operating model.

These mechanisms are addressed throughout this guide and formalized in the Addenda. They appear where the domains they govern require them, not as isolated constructs but as integrated features of a functional leadership response infrastructure.

The Domain Most Organizations Miss

Of the eleven domains, the one most consistently underprepared is Evidence and Defensibility.

In the heat of an incident, leadership focuses on stopping the damage and communicating with affected parties. Documentation feels secondary. Decision records feel bureaucratic. Evidence preservation feels like something that can wait.

It cannot wait.

Every decision made during the incident — every action taken, every communication sent, every authorization given, every notification made or delayed — will be subject to review by insurers, regulators, plaintiffs' attorneys, and board members. The organizations that survive that scrutiny are the ones that documented why their decisions were reasonable, what they knew when they made them, and what they did as a result.

The organizations that do not survive that scrutiny are not necessarily the ones that made worse decisions. They are the ones that cannot prove the decisions they made were reasonable.

Evidence and Defensibility is not a legal formality. It is a business survival requirement.

PART TWO

The Operating Model

How BIM Is Structured, Who Owns What, and When It Activates

CHAPTER 5

The Nine Executive Workstreams

Building the Leadership Infrastructure for Business Response

BIM is not a plan that one person owns. It is a leadership infrastructure with nine defined workstreams, each with a named owner, defined authority, and clear activation criteria.

The reason most organizations struggle with the business event is not that leadership lacks the competence to manage it. It is that the structure has not been built before the event. Who calls whom? Who can approve what? Who owns which domain? Without pre-built structure, those questions consume time and create conflict in the first hours — exactly when clarity is most critical.

The nine BIM workstreams eliminate that uncertainty.

Workstream	Owns	Typical Leader
Executive Command	Activation, business priorities, executive coordination, and final escalation	CEO, COO, or designated incident executive
Security and Technical Response	Technical investigation, containment, eradication, recovery, and technical evidence	CISO, CIO, SOC, MSP, or forensic partner
Legal and Privilege	Counsel direction, privilege, legal review, evidence protection, and notification analysis	General Counsel, outside counsel, or breach counsel
Insurance and Claims	Carrier notice, broker coordination, claim evidence, and coverage conditions	CFO, risk manager, or coverage counsel
Regulatory and Compliance	Reporting obligations, regulatory communication, and compliance evidence	Compliance officer, privacy officer, or legal
Operations and Continuity	Business continuity, service delivery, production decisions, and operational recovery	COO, operations leader, or clinical leader
Customer, Partner, and Vendor Management	Customer impact, account communication, supplier coordination, and retention actions	CRO, customer success, or vendor management
Communications	Internal messaging, external statements, media response, and stakeholder communications	Communications, PR, or legal-approved spokesperson
Board and Governance	Board notification, oversight record, governance documentation, and executive accountability	CEO, board chair, GC, or corporate secretary

How the Workstreams Function Together

The nine workstreams do not operate sequentially. They activate in parallel and must be coordinated through the Executive Command workstream.

Executive Command is the integration point. The CEO or designated incident executive does not manage every workstream directly. They manage the coordination between workstreams —

ensuring that the legal team knows what communications is planning to say, that insurance knows what claims evidence operations is collecting, that the board is receiving appropriate updates from governance, and that technical findings are being translated into business decisions at the right escalation thresholds.

Each workstream has a named owner and a named alternate. During a serious incident, individuals may be unavailable. The alternate structure is not optional. It is a required component of every BIM deployment.

Naming the Owners Before the Incident

One of the most important BIM design decisions is naming workstream owners in advance.

This sounds obvious. In practice, it does not happen in most organizations. General statements about roles — “the CFO owns insurance” or “legal handles notifications” — are not the same as a named owner with documented authority, defined activation criteria, and a confirmed understanding of their responsibilities under BIM.

Every BIM implementation should produce a Workstream Ownership Document that identifies the primary owner, the alternate, the activation trigger for that workstream, and the specific decisions that workstream owner is authorized to make without escalation to Executive Command.

That document is tested before it is needed. Not in a tabletop exercise that simulates the technical event, but in a leadership exercise that simulates the business event — where workstream owners are given scenarios and asked to demonstrate that they know what to do.

A Role Is Not Assigned Until It Is Acknowledged

A BIM plan should not assign responsibility silently. Every named executive, workstream owner, alternate, emergency spending approver, board liaison, communications approver, insurance contact, legal contact, and incident escalation owner should acknowledge their role in writing.

The acknowledgment confirms that the individual has reviewed the plan, understands their responsibility, understands their authority and its limits, knows when their role activates, knows what must be escalated, understands documentation and evidence obligations, and has identified any gaps, conflicts, or resource constraints that would prevent execution.

Role acknowledgment is not a formality. It is the moment at which the BIM framework becomes an organizational commitment. See Addendum A for the Leadership Acknowledgment and Attestation format.

The CISO’s Role in BIM

BIM gives the CISO something they rarely have during a serious incident: a clear escalation path into the business.

In most organizations, the CISO is managing the technical response while simultaneously being asked to answer business questions they are not equipped to answer. When do we notify the

board? What do we tell customers? Does this require regulatory notification? Can we say this in an email or does privilege apply?

Those are not security questions. They are business questions. And the CISO should not be the one answering them.

BIM removes that burden. It creates a defined handoff from the Security and Technical Response workstream to the other eight workstreams — a clear moment where technical facts become business inputs, and the business response takes ownership of what happens next.

The CISO's job in BIM is to provide accurate, current technical intelligence to Executive Command. Not to manage insurance. Not to brief the board directly. Not to approve customer communications. Not to own the regulatory notification analysis. BIM returns the CISO to their lane while ensuring that the information they provide is immediately actionable by the right business leaders.

CHAPTER 6

When BIM Activates

The Criteria That Trigger Business Response

Not every security alert requires a business response. BIM activates when a security event has credible business consequence potential.

That distinction matters. If BIM activates for every minor event, it loses its authority. Leaders stop treating it seriously. Workstreams become fatigued. The structure atrophies.

BIM activates when the business is at risk — not merely when the security systems are responding.

The Activation Test

> **Governing Question:** *Could this security event create a legal, insurance, regulatory, customer, operational, financial, contractual, board, or reputational consequence?*

If the answer is yes, BIM activates.

The activation test is deliberately broad. That is intentional. The cost of failing to activate BIM when a business consequence emerges is far higher than the cost of activating BIM for an event that turns out not to require a full business response. Workstream owners can stand down. They cannot un-miss a 72-hour regulatory notification window.

Activation Does Not Require Certainty

BIM activates on credible business consequence potential. Waiting for complete certainty can cause the organization to miss insurance notice windows, regulatory analysis deadlines, evidence preservation requirements, board reporting expectations, or customer communication obligations.

The organizations that manage incidents best are the ones that activate early and stand down if not needed. The organizations that suffer the worst business outcomes are the ones that waited for certainty before activating — and discovered they had already missed the decisions that mattered most.

Specific Activation Criteria

BIM should activate when any of the following conditions appear credible:

- Customers, patients, members, employees, or partners may have had their data accessed or exfiltrated

- Regulated data — PHI, PII, financial data, or sector-specific categories — may be involved
- Production, clinical operations, transaction processing, or service delivery is or may be affected
- Revenue, cash flow, or financial systems may be impacted
- Contractual commitments, SLAs, or vendor obligations may be triggered
- Insurance notice obligations may be in effect
- Regulatory notification analysis may be required
- Board reporting thresholds may be met
- Public trust, media exposure, or reputational risk may emerge
- Critical vendors, suppliers, or third-party systems may be affected or compromised
- Executive decision authority may be required for containment actions
- Evidence preservation obligations may be activated

The word “may” is doing important work in every one of those criteria. BIM does not wait for certainty. It activates on credible potential. By the time certainty arrives, the first-hour decisions have already been made — and made without the structure that BIM provides.

Activation Brief Requirement

When BIM is activated, the Security and Technical Response workstream must provide an initial Security-to-Business Activation Brief to Executive Command. This brief translates available technical facts into business consequence terms: what is known, what is unknown, what systems are affected, what data may be involved, what business consequences are possible, and what decisions Executive Command needs to make in the next 30, 60, and 120 minutes.

The Activation Brief does not require complete information. It requires organized information. Executive Command cannot manage the business event without a structured briefing from the technical team. See Addendum B for the Activation Brief format.

The Severity Classification

Every BIM implementation should include a Business Incident Classification Model that separates technical severity from business consequence severity.

A technically minor event — a compromised low-privilege account, for example — can have significant business consequences if it turns out to belong to someone with access to regulated data, or if it is used to send fraudulent communications to customers, or if it triggers a contractual notification obligation with a key partner.

Conversely, a technically severe event — a significant infrastructure compromise — may have limited business consequence activation if it affects only internal systems that do not interact with regulated data, customers, or key operational processes.

Technical severity and business consequence severity are not the same scale. BIM uses its own classification model, distinct from the security team's incident severity ratings, to determine which workstreams activate and at what level.

Who Activates BIM?

The BIM activation authority should be defined in advance.

In most organizations, the person with the most current information in the first hours is the CISO or security lead. They should have explicit authority to activate BIM. Not to manage it — that belongs to Executive Command — but to trigger its activation when the technical event meets the activation criteria.

The activation trigger should be documented. It should be understood by every workstream owner. And it should be practiced, so that when the CISO calls, the workstream owners know what that call means and what they are expected to do within the next thirty minutes.

CHAPTER 7

The Decision Authority Matrix

Who Can Authorize What, Under What Conditions

Decision authority is the most critical and most overlooked component of business response readiness. Organizations that cannot make decisions quickly in the first hours of an incident pay for that delay for months.

The Decision Authority Matrix (DAM) defines, in advance, who is authorized to make each category of business decision during an incident — without escalation, without committee approval, without waiting for someone to be located.

What the Matrix Defines

The Decision Authority Matrix should define authorized decision-makers for the following categories:

- Containment actions that affect operations or production
- System isolation or shutdown decisions
- Insurer notice — who can initiate and what triggers it
- Legal counsel engagement and privilege establishment
- Regulatory notification initiation
- Board notification — who initiates, with what information, under what threshold
- Customer or patient communication — who approves and through what process
- External statement approval — media, public, or partner communications
- Transaction suspension or financial system isolation
- Vendor notification or contract invocation
- Evidence preservation authority — who directs and what is preserved
- Business continuity activation — who triggers and what it covers

Each category should have a primary decision-maker, an alternate in case the primary is unavailable, and a defined threshold that determines when escalation to the next level is required.

Why Pre-Built Authority Matters

In a serious incident, the pressure to act is constant and the information available is incomplete. Leaders are making decisions before the full picture is clear. That is not a failure. It is the nature of incident response.

What turns incomplete information into dangerous improvisation is the absence of pre-defined authority. When nobody knows who can approve the containment action that will halt production, the decision gets delayed. When nobody knows who can authorize the customer

notification, the message goes out without proper legal review. When nobody knows who can initiate the insurance notice, the window closes.

Pre-built authority does not mean pre-made decisions. It means that the people who need to make decisions know they are authorized to make them, know what they need to make them well, and do not have to locate a committee or a chain of approval before acting.

Decision Authority Without Spending Authority Is Incomplete

During a cyber business incident, leadership must be able to authorize the resources required to protect customers, patients, employees, operations, evidence, insurance recovery, and the organization's legal position. BIM therefore defines not only who may decide, but who may spend, how much they may authorize, when insurer consent must be checked, and how emergency spending must be documented.

Spending authority and decision authority are not the same thing. An executive may have the decision authority to engage a forensic vendor, a ransomware negotiator, or outside counsel — and have no defined authority to approve the invoice. BIM closes that gap before it becomes a problem in the middle of the incident. See Addendum C for the Emergency Spending Authority format.

Law Enforcement and Government Coordination Authority

Government coordination is a business decision, not an ad hoc technical contact. Law enforcement and federal authority engagement can support investigation, recovery, fraud response, public safety, ransom decision-making, and regulatory posture. But it also affects legal strategy, insurance recovery, communications, evidence handling, and board oversight.

BIM defines who may contact authorities, which agencies apply, what may be shared, and how the contact is documented. That authority belongs to Executive Command and the Legal and Privilege workstream — not to the security team acting independently. See Addendum D for the Law Enforcement and Government Coordination Protocol.

Emergency Identity and Access Authority

Cyber containment may require disabling accounts, terminating sessions, forcing credential resets, suspending vendor access, revoking tokens, disabling APIs, or restricting privileged access. These are not purely technical decisions. They create business consequences — for employees, customers, vendors, and operations.

The BIM plan must define who can authorize these actions when they create business consequences. That authority must be defined in advance. The security team cannot act alone on decisions that affect customer access, employee access, or vendor relationships without knowing who in the business has the authority to accept those consequences. See Addendum E for the Emergency Identity and Access Authority format.

Conflict Resolution Rule

When workstreams disagree, Executive Command resolves the conflict after receiving input from the relevant workstream owners. If the issue involves legal, regulatory, privilege, sanctions, law enforcement, notification, or insurance exposure, General Counsel must be consulted before the final decision is made. If the issue affects patient safety, employee safety, physical safety, or operational safety, the relevant safety or operations owner's recommendation must be formally considered and documented.

Conflict between workstreams is not a failure of BIM. It is a predictable feature of managing competing obligations simultaneously. BIM resolves those conflicts through structure, not improvisation. The conflict resolution rule ensures that the right inputs reach the right decision-maker in time to matter. See Addendum F for the Conflict Resolution Protocol.

Vendor Activation Authority

Vendor engagement is a decision-authority issue, a spending-authority issue, a legal issue, and an insurance issue.

The Decision Authority Matrix must define who may activate outside incident vendors during a BIM activation. This includes breach counsel, coverage counsel, DFIR providers, recovery and restoration providers, ransomware or extortion advisors, crisis communications firms, notification vendors, call center providers, eDiscovery providers, identity recovery providers, backup recovery vendors, OT recovery specialists, cloud recovery specialists, and payment fraud recovery support.

Vendor activation authority should specify:

1. who can activate each vendor;
2. whether Legal must approve activation;
3. whether insurer consent is required;
4. whether broker or carrier notice is required;
5. what spending limit applies;
6. whether emergency exception authority exists;
7. how the activation is documented;
8. whether the vendor is approved, panel-approved, non-panel, pending, or emergency-only.

This cannot be assumed during the incident.

A vendor listed in the plan is not necessarily ready to use. The BIM plan must connect each vendor to authority, contract status, insurer status, emergency spending authority, and activation process.

See Addendum Y for the Pre-Approved Incident Vendor and Retainer Register.

The Containment Authorization Problem

One of the most consequential decisions in a serious incident is containment. Technical containment — isolating a system, cutting a network segment, taking down a service — often has immediate business consequences.

If the system being isolated is a clinical system in a hospital, patient care is affected. If it is a payment processing system, transactions cannot be completed. If it is a production control system in a manufacturing plant, the line stops. If it is a trading platform in a financial institution, market exposure changes with every second of downtime.

The security team cannot be expected to authorize those containment decisions alone. They have the technical authority to act. They do not have the business authority to accept the operational consequences.

The Decision Authority Matrix defines who has that business authority. It names the person who can tell the security team “yes, take it down” and accept the operational consequences of that decision. Without that person identified in advance, the security team either acts without business authorization — potentially causing unacceptable business disruption — or waits for authorization that is not coming fast enough.

BIM solves that problem before the incident begins.

PART THREE

The Critical Domains

Insurance, Legal, Regulatory, Board, and Operational Response in Depth

CHAPTER 8

Insurance and Financial Recovery

Why the Policy You Bought Must Become an Executable Incident Requirement

Cyber insurance is not self-executing. The coverage you purchased requires specific actions at specific times. BIM ensures those actions happen.

Most executives believe that cyber insurance is a safety net — something that catches the organization when a serious incident occurs. That belief is accurate in principle. It is not always accurate in practice.

Insurance policies contain conditions. Those conditions define not only what is covered but what the insured organization must do to preserve coverage. Notice requirements. Evidence preservation obligations. Proof of loss documentation. Cooperation clauses. Policy exclusions that activate based on specific behaviors during the incident.

Organizations that handle those conditions well recover their covered losses. Organizations that handle them poorly find themselves in coverage disputes — arguing with their insurer about whether the claim is valid, whether notice was timely, whether the evidence supports the claimed loss, and whether a policy exclusion applies.

Most coverage disputes do not arise because the organization had bad insurance. They arise because the organization did not manage the insurance process correctly during the incident.

The Notice Requirement

Every cyber insurance policy contains a notice requirement. It defines the window within which the insurer must be notified of a potential claim. That window varies by policy — some require notice as soon as practicable, some specify defined timeframes, some require notice within a specific number of hours or days of the organization learning of a potential claim.

Notice must go to the right parties through the right channels. Most policies require notice to the carrier, the broker, or both. Some require notice to a specific claims contact or portal.

BIM defines the notice trigger, the notice process, the notice recipients, and the person responsible for ensuring notice is given. That person has confirmed authority, confirmed contact information, and confirmed understanding of what constitutes adequate notice under the policy.

Cyber Insurance Readiness Review

The Cyber Insurance Readiness Review tells the organization what the policy demands. BIM assigns the people, evidence, authority, timing, and documentation needed to meet those demands. Every BIM implementation should confirm the following elements from the active cyber policy:

- Policy notice requirements and deadlines
- Broker and carrier contacts for claims initiation

- Approved vendor panel requirements
- Panel counsel requirements
- Forensic vendor requirements
- Insurer consent requirements for significant expenditures
- Sublimits applicable to specific loss categories
- Retentions and co-insurance obligations
- Policy exclusions and how they activate
- Business interruption evidence requirements
- Proof-of-loss requirements and deadlines
- Cooperation obligations during investigation
- Application representation evidence that may be relevant to coverage
- Claim communication protocol and approval requirements

See Addendum G for the Cyber Insurance Readiness Review format.

Evidence That Supports the Claim

A business interruption claim requires documented proof of loss. The insurer will want to see what systems were affected, when they were affected, what the impact on operations and revenue was, and how long the disruption lasted.

That documentation must be contemporaneous. Reconstructed records prepared weeks after the event carry less weight than records created during the event. BIM establishes evidence preservation protocols that ensure the documentation needed for insurance recovery is being collected from the first hours of the incident.

The insurance workstream owner — typically the CFO or risk manager — is responsible for ensuring that financial impact tracking begins at incident activation, not at claim submission. See Addendum H for the Insurance Notice and Claim Evidence Tracker.

Insurance Portfolio Review

The Insurance and Recovery workstream must determine whether the incident may implicate policies beyond cyber insurance. A single incident can trigger multiple coverage areas simultaneously.

Crime policies may respond to business email compromise or financial fraud. Technology errors and omissions coverage may apply to service failures. Directors and officers coverage may be relevant if executive decisions are scrutinized. Property and business interruption coverage may apply if physical operations are affected. Professional liability, general liability, and product liability coverage may also be implicated depending on the nature of the incident and the organization’s sector.

Every relevant policy must be identified at activation. Notice requirements and cooperation obligations under each policy must be tracked separately. The assumption that only the cyber

policy is relevant is one of the most common and costly errors in post-incident insurance management.

Coverage Counsel and Breach Counsel

In a significant incident, the organization will typically have both breach counsel (managing the legal response to the incident itself) and coverage counsel (managing the insurance claim process). These are often different attorneys. Their work is related but distinct.

BIM defines the relationship between these two counsel roles in advance, so that there is no ambiguity during the incident about which attorney is responsible for which communications, which decisions, and which documentation requirements.

Approved Vendor and Panel Counsel Verification

The Insurance and Financial Recovery workstream must verify which vendors are approved by the cyber insurer before the incident.

This includes breach counsel, DFIR providers, ransomware or extortion advisors, notification vendors, crisis communications firms, credit monitoring providers, recovery vendors, and any other service providers whose costs may be submitted as part of the claim.

The organization must not assume that a preferred vendor is reimbursable. The BIM plan must document whether each vendor is:

1. approved by the carrier;
2. approved only with prior consent;
3. not on the panel but accepted by the organization;
4. pending confirmation;
5. not expected to be claim-relevant;
6. available only through emergency exception.

The insurer’s vendor requirements should be reviewed at each policy renewal and whenever the organization changes breach counsel, DFIR providers, recovery partners, notification vendors, or other material incident vendors.

If the organization chooses to use a non-panel vendor, the coverage risk must be documented. The decision record should identify the business reason for the selection, whether carrier consent was requested, whether broker input was obtained, who approved the decision, and what reimbursement risk the organization accepted.

Vendor panel verification is not an administrative detail. It is a claim-readiness requirement.

See Addendum Y for the Pre-Approved Incident Vendor and Retainer Register.

CHAPTER 9

Legal, Privilege, and Internal Investigation

Protecting the Organization's Right to Confidential Counsel

Privilege is not automatic. It must be established, structured, and maintained from the first moments of the incident. Mistakes made in the first hours can compromise the organization's ability to protect its most sensitive communications.

Attorney-client privilege protects communications between an attorney and their client for the purpose of obtaining legal advice. Work product protection protects materials prepared by attorneys in anticipation of litigation.

In a serious cyber incident, the organization will generate enormous volumes of communications, documents, and analysis. Some of those materials will be discoverable in litigation. Some will be protected by privilege. Which category a given document falls into depends on how the legal engagement was structured and how communications were managed from the beginning of the incident.

BIM helps leadership pre-plan counsel engagement and communication protocols that qualified counsel may use to establish and maintain privilege where available.

Engaging Counsel at Activation

The most important legal decision in a serious incident is when and how to engage outside counsel.

Counsel should be engaged at or near BIM activation — not after the organization has already generated days of potentially discoverable internal communications about the incident. Early engagement creates the opportunity to structure subsequent communications and analysis under privilege.

BIM defines the counsel engagement trigger, the engagement process, the specific attorney or firm to engage, and the authority to authorize that engagement. In most organizations, that authority belongs to the General Counsel. In organizations without a GC, it belongs to the CEO or another designated executive.

Privilege Counsel Readiness

The BIM plan must identify the law firm or attorney authorized to support the legal response, advise on privilege-sensitive communications, manage breach response, advise on notification analysis, and coordinate legal-sensitive work.

The organization should not discover during the incident that its preferred law firm has not cleared conflicts, is not on the carrier panel, has no retainer in place, lacks an emergency activation process, or cannot be engaged without procurement delay.

Privilege counsel readiness should include:

1. primary breach counsel;
2. alternate breach counsel;
3. conflict check status;
4. retainer or engagement status;
5. insurer panel status;
6. emergency contact path;
7. internal engagement authority;
8. relationship to internal General Counsel;
9. relationship to DFIR provider;
10. relationship to coverage counsel;
11. communication protocol for privilege-sensitive work.

BIM does not guarantee privilege. Qualified counsel determines how legal work should be structured. BIM helps leadership ensure that counsel engagement and communication protocols are defined before the incident creates privileged, discoverable, operational, and regulatory communication risks at the same time.

See Addendum Y for the Pre-Approved Incident Vendor and Retainer Register.

Communication Hygiene During the Incident

Not every incident communication will be privileged. Operational communications — telling a system administrator to isolate a server, notifying a department head that a system is unavailable — are not privileged.

Communications that seek or convey legal advice, made through the proper structure with counsel involved, can be privileged.

The problem is that most organizations do not distinguish between these categories during an incident. Leaders send emails. Executives text each other. Slack channels fill with speculation about what happened and who might be liable. None of that is privileged. All of it could be discoverable.

BIM establishes communication hygiene protocols: what goes in writing, what does not, what channels are used for privileged communications versus operational communications, and what instructions are given to workstream owners about what to say and how to say it during the incident.

The Evidence Handling Protocol

Legal counsel will need to instruct the organization on evidence preservation obligations — what must be preserved, what must not be altered, and what legal holds apply.

That instruction cannot happen if counsel is not engaged early. And the organization cannot comply with evidence preservation obligations it does not know exist.

BIM connects the legal workstream to evidence preservation from the first moments of activation, ensuring that the organization is not inadvertently destroying or altering evidence that will be required for insurance recovery, regulatory examination, or litigation defense.

Internal Investigation and Insider Event Protocol

Cyber incidents may involve insider conduct, employee misuse, contractor activity, privileged account abuse, or internal misconduct. These situations require a distinct response structure from external attack scenarios.

When an insider event is suspected, the investigation must be controlled from the beginning to preserve both the legal privilege and the evidentiary integrity of findings. Human Resources engagement, employee access decisions, and communication with the affected individual must be coordinated through the Legal workstream, not managed informally by IT or security teams.

The BIM plan must define when HR is engaged, when Legal controls the investigation, when employee access may be suspended, when interviews occur, when law enforcement is considered, how evidence is preserved, and how employee communications are managed to avoid creating additional legal exposure. See Addendum I for the Insider and Internal Investigation Protocol.

CHAPTER 10

Regulatory, Compliance, and Inquiry Response

Notification, Deadlines, and the Documentation That Proves Compliance

Regulatory notification is not optional. The deadlines are real. The penalties for missing them are real. And the analysis that determines whether notification is required must be completed before the deadline expires.

Every organization operating in a regulated sector — healthcare, financial services, government contracting, critical infrastructure, publicly traded companies — operates under notification obligations that activate when certain conditions are met during a cyber incident.

HIPAA. GLBA. SEC. FTC. CISA. State breach notification laws. Sector-specific regulatory frameworks. Each has its own threshold, its own timeline, its own required content, and its own documentation requirements.

The organizations that manage regulatory exposure well are not the ones with the largest compliance departments. They are the ones that have done the regulatory mapping in advance and know exactly what the notification analysis requires before the incident begins.

Regulatory examples in this guide are illustrative. Notification duties, timing, and content requirements vary by jurisdiction, sector, contract, incident facts, and current law. Organizations should confirm applicable requirements with qualified counsel and current authoritative sources.

The Notification Analysis

Regulatory notification analysis is the process of determining whether a specific security event triggers a mandatory notification obligation under applicable law or regulation.

That analysis requires several inputs: the nature of the data involved, the type of access that occurred, the population affected, the regulatory frameworks that govern those individuals or that data, the jurisdiction of the organization and of affected individuals, and any applicable exemptions or safe harbors.

The analysis must be completed before the notification deadline expires. In some frameworks, that deadline is 24 hours. In others, it is 30, 60, or 72 hours, or calendar days. In some, it is measured from the moment of discovery. In others, it is measured from the moment a determination is made.

BIM defines who leads the notification analysis, what inputs they need, who provides those inputs, and what the decision-making process looks like — including who has final authority to determine that notification is or is not required.

The Documentation Requirement

Regulatory examination after an incident does not focus only on what the organization did. It focuses on what the organization can prove it did.

The notification analysis must be documented. The timeline from discovery to determination must be documented. The basis for the determination must be documented. If notification was made, the timing, content, and recipients must be documented. If notification was determined to not be required, the legal basis for that determination must be documented.

Organizations that have thorough documentation of a reasonable and timely notification process fare significantly better in regulatory examination than organizations that took the same actions but cannot prove it.

BIM builds the documentation structure into the regulatory workstream from the first hours of activation.

Regulator Inquiry Response Protocol

Regulatory response does not end with notification. After a cyber incident, regulators may ask what the organization knew, when it knew it, what safeguards existed, what failed, what was communicated, what corrective actions were taken, and what leadership did.

The organizations that manage regulatory inquiry well are the ones that treat inquiry response as an ongoing obligation, not a one-time notification event. Regulator follow-up can arrive weeks or months after the initial incident. By then, the incident team has dispersed, memories have faded, and the documentation created during the incident becomes the only reliable record of what happened and why.

The BIM plan must define who receives regulator inquiries, who drafts responses, who approves responses, how deadlines are tracked, and where supporting evidence is maintained. Regulatory inquiry responses must be approved by counsel before submission. See Addendum J for the Regulator Inquiry Response Protocol.

CHAPTER 11

Board Reporting, Governance, and Materiality Escalation

What the Board Needs, When It Needs It, and How to Document Oversight

The board is not a passive observer during a serious incident. It has fiduciary responsibilities. It will be held accountable for what it knew and when it knew it. BIM ensures that accountability is managed, not discovered.

In the aftermath of a serious incident, one of the earliest questions asked by regulators, plaintiffs' attorneys, and institutional investors is what the board knew and when it knew it.

If the answer is "they were notified three days after the event when the CEO sent a brief email", that is a governance problem. If the answer is "the board was notified within the first 24 hours through the established reporting protocol, received a structured briefing with the available facts, and has been receiving regular updates through the documented reporting cadence" — that is a governance story.

BIM builds the second story.

Board Notification Thresholds

Not every security event requires board notification. BIM defines the specific thresholds that trigger board notification:

- Events that may constitute a material event under applicable securities law
- Events that may require regulatory notification
- Events affecting critical operational systems, clinical systems, or revenue-generating systems above defined impact thresholds
- Events involving exfiltration or exposure of customer, patient, or employee data above defined thresholds
- Events with potential for significant public disclosure or media coverage
- Events that may trigger insurance claims above defined coverage thresholds
- Events that create significant legal or regulatory exposure

Those thresholds should be defined in advance and agreed with the board. The board should not be surprised by the notification criteria any more than it should be surprised by the notification itself.

What the Board Receives

Board communications during an incident should be structured, factual, and governed by legal review.

The board needs to know what is known, what is unknown, what is being done, what decisions have been made, what decisions are pending, and what the anticipated timeline looks like. It does not need speculation. It does not need unfounded reassurance. It does not need to receive communications that have not been reviewed by counsel.

BIM defines the structure of board communications during an incident — the template, the approval process, the delivery method, the author, and the documentation requirements that preserve the oversight record. See Addendum K for the Board Incident Briefing Template.

The Oversight Record

The board's oversight record is the documentation that proves the board took its responsibilities seriously during the incident.

That record includes: the initial notification and its timing, the board's response and any questions asked, the subsequent updates and their timing, any board resolutions or authorizations during the incident, and the final post-incident briefing.

That record is not created after the incident. It is created during the incident, as part of the BIM governance workstream. The corporate secretary, board liaison, or GC maintains it contemporaneously.

Materiality and Disclosure Escalation

If a cyber incident may materially affect revenue, operations, customer commitments, liquidity, regulatory standing, public reporting, financing obligations, investor confidence, strategic transactions, or board oversight expectations, Executive Command must escalate the matter to General Counsel, CFO, CEO, and board governance leadership for materiality review.

Materiality is a legal and financial determination, not a security determination. The security team does not make it. Legal counsel, the CFO, and the CEO make it — with input from relevant workstream owners. BIM defines the escalation trigger, the escalation path, and the documentation requirements for the materiality review. Decisions about public disclosure, regulatory reporting under securities frameworks, or press statements related to materiality must involve qualified counsel.

Board Governance Acknowledgment

Board members should acknowledge the board notification thresholds, briefing cadence, governance documentation process, and oversight role established by the BIM plan. That acknowledgment does not require board members to become cybersecurity experts. It requires them to understand what they will receive, when they will receive it, and what governance obligations apply to their response.

The board's acknowledgment of its BIM role is part of the Leadership Acknowledgment and Attestation process documented in Addendum A.

CHAPTER 12

Customer, Stakeholder, Status Page, and Trust Communication

The Communication Strategy That Can Save or Damage the Relationship

How leadership communicates with affected parties during an incident is often remembered longer than the incident itself. BIM builds the communication structure before the crisis requires it.

Customer trust is not a soft concept. In a serious incident, it is a measurable business variable. Customers who receive timely, honest, clearly structured communication about what happened are significantly more likely to remain customers than those who hear about it from a news report, receive inconsistent messages, or are left waiting without information.

That difference in outcome is not the result of luck. It is the result of a pre-built communication structure.

The Communication Framework

BIM defines a Customer and Stakeholder Communication Framework that answers the following questions before the incident begins:

- Who has authority to approve customer communications?
- What is the legal review and approval process for external communications?
- At what threshold do customers or patients receive notification?
- What channels are used for customer notification?
- What is the sequencing — when does internal communication happen before external?
- Who is the approved spokesperson for external statements?
- What pre-approved language exists for the first hours before formal communications can be prepared?

Pre-approved language templates are particularly valuable. In the first hours of an incident, the pressure to say something — to customers, to partners, to employees — is intense. Without pre-approved templates, that pressure leads to improvised communications that may be legally problematic, factually inaccurate, or reputationally damaging.

With pre-approved templates, workstream owners can respond immediately with language that has already been reviewed, approved, and structured to preserve both trust and legal position.

The Sequencing Problem

External communication during an incident must be sequenced carefully. Employees should generally hear from leadership before they hear from the news. Partners should generally be

notified before they begin receiving calls from concerned customers. Regulators, in some frameworks, must be notified before customers.

BIM defines the communication sequence. That sequence is not created during the incident — it is activated.

Account-Managed Customer Communication

Enterprise customers, strategic partners, payers, banking partners, providers, distributors, government customers, and major accounts may require direct account-managed communication separate from public statements. Mass customer communications do not serve these relationships. They require personal outreach from a named account owner who can answer questions, acknowledge the relationship, and communicate next steps.

The BIM plan must define who owns strategic account outreach, what can be said, what must be legally approved before it is said, and how customer commitments and responses are tracked throughout the incident. See Addendum L for the Customer and Stakeholder Communication Approval Record.

Status Page and Trust Center Protocol

For SaaS, MedTech, FinTech, technology-enabled healthcare, and platform businesses, the status page and trust center are incident communication assets, not passive marketing tools. During a security incident, customers and partners will check these resources — often before they receive any direct communication.

The BIM plan must define who owns status page updates, what incidents appear, what language is approved, who approves trust center changes, and how customer security teams receive updates. Status page and trust center communications are external communications and must go through the same legal review and approval process as any other external statement. See Addendum M for the Status Page and Trust Center Protocol.

CHAPTER 13

Employee Communication During an Incident

The Internal Audience That Determines Whether the Workforce Holds Together

Employees are the first internal audience affected by an incident and one of the most important sources of stability during the business response. BIM controls what they are told, how, and by whom — before uncertainty becomes rumor.

Employees are often the first internal audience affected by a cyber incident and one of the most important sources of stability during the business response. They may need instructions about system access, credential resets, service disruption, customer questions, media inquiries, phishing follow-up, data handling, remote work, facility access, fraud risk, or their own personal information.

At the same time, employee communication creates legal, regulatory, evidentiary, operational, reputational, and insurance consequences. Informal messages, speculation, screenshots, forwarded emails, internal chat discussions, social media posts, or inconsistent manager briefings can create discoverable records, confuse the workforce, undermine privilege, damage customer trust, or contradict later regulatory, insurer, board, or public statements.

For that reason, employee communication during a BIM activation is not a general HR or communications function. It is a controlled business-response function governed jointly by Executive Command, Legal and Privilege, Communications, HR and Workforce, Security and Technical Response, and Evidence and Defensibility.

Governing Principle

Employees should be told what they need to know to act safely, consistently, and effectively — but only through approved channels, approved messages, and approved spokespersons.

The organization should not delay necessary workforce instructions while waiting for complete incident certainty. However, all employee-facing communication must distinguish between confirmed facts, current instructions, pending analysis, and matters the organization is not yet prepared to address.

What Employee Communication Must Accomplish

Employee communication during an incident must support five outcomes:

- Provide clear workforce instructions.
- Prevent rumor, speculation, and unauthorized disclosure.
- Preserve legal privilege and evidentiary integrity.
- Ensure customer, vendor, media, and public inquiries are routed properly.
- Maintain employee trust without overstating what is known.

The goal is not to tell employees everything. The goal is to tell the right employees the right information at the right time through the right channel with the right approvals.

Communication Authority

The BIM plan must define who has authority to approve employee communications during an incident. At minimum, the following roles should be identified:

Role	Responsibility
Executive Command	Determines whether employee communication is required and approves major workforce messaging strategy.
Legal and Privilege	Reviews employee messages for legal, privilege, regulatory, litigation, and notification impact.
HR and Workforce	Coordinates employee-facing delivery, workforce instructions, manager guidance, and employee support needs.
Communications	Drafts or coordinates approved employee messaging and maintains consistency with external communications.
Security and Technical Response	Provides verified technical facts and workforce security instructions.
Evidence and Defensibility	Preserves approved messages, distribution records, approvals, timing, and recipient groups.

No manager, executive, employee, contractor, or technical team member should issue incident-related workforce communications unless authorized under the BIM plan or directed by Executive Command.

Approved Employee Communication Channels

The BIM plan must define approved channels for employee communication during a cyber incident. Approved channels may include:

- Company email.
- Emergency notification system.
- Approved intranet page.
- Approved collaboration channel.
- Manager briefing script.
- Recorded all-hands briefing.
- Secure out-of-band communication method.
- HR helpdesk or employee hotline.
- Status page intended for internal workforce updates.

The organization must also define which channels are not approved for incident-related communication. Unapproved channels may include informal text chains, personal email, unofficial chat groups, unauthorized collaboration channels, private social media groups, or any channel not preserved under the organization's evidence and recordkeeping requirements.

If normal communication systems are unavailable, compromised, unreliable, or under investigation, Executive Command must approve the alternate employee communication channel.

Employee Message Categories

Employee communication should be separated into defined message categories.

1. Immediate Workforce Instructions

These messages tell employees what to do now. Examples include:

- Do not use specific systems.
- Disconnect from VPN.
- Reset credentials.
- Stop using a compromised application.
- Preserve suspicious emails.
- Report unusual account activity.
- Use alternate business process.
- Work remotely or report to a specific location.
- Route customer questions to a designated team.
- Do not delete, alter, or forward incident-related materials.

These messages may need to be issued quickly. Legal review should occur when practical, but the BIM plan should define an emergency approval path for urgent operational instructions.

2. Manager Guidance

Managers require separate guidance because employees will ask them questions. Manager guidance should include:

- What managers may say.
- What managers must not speculate about.
- How to handle employee questions.
- Where to send technical issues.
- Where to send HR concerns.
- Where to send customer, vendor, media, or legal inquiries.
- How to document material concerns raised by employees.

Managers should not be left to interpret the incident independently. During an incident, inconsistent manager communication can create greater organizational risk than a delayed all-employee message.

3. Employee Data Exposure Communication

If employee personal information, payroll information, benefits information, credential information, personnel files, or other workforce-related data may be involved, employee communication must be coordinated through Legal, HR, Security, and Communications.

The organization should not prematurely confirm employee data exposure before the notification analysis is complete. However, employees may still need protective instructions before final determination. Employee data exposure communication may include:

- Whether employee data may be involved.
- What is currently known.
- What is still being investigated.
- What protective steps employees should take.
- Whether credit monitoring, identity protection, or fraud support may be offered.
- Where employees can ask questions.
- When the next update will be provided.

4. Customer-Facing Employee Instructions

Employees who interact with customers, patients, clients, members, vendors, partners, regulators, or the public require specific instructions. These instructions should define:

- What employees may say.
- What employees must not say.
- Where inquiries should be routed.
- Whether a holding statement exists.
- Whether account teams may contact customers.
- Whether sales teams may discuss the incident.
- Whether support teams may reference the incident in tickets.
- Whether employees may acknowledge outage, investigation, data exposure, ransomware, fraud, or law enforcement involvement.

Customer-facing employees should not improvise. They should receive approved language, escalation paths, and clear limits.

5. Social Media, Media, and Public Discussion Instructions

Employees must be instructed not to post, comment, speculate, confirm, deny, share screenshots, or discuss the incident publicly unless specifically authorized. This includes:

- LinkedIn.
- X/Twitter.
- Facebook.
- Reddit.
- TikTok.
- Industry forums.
- Private groups.
- Vendor communities.
- Customer communities.
- Messaging apps.
- Any other external platform.

The instruction should be direct: employees may not discuss the incident externally, respond to media inquiries, correct public speculation, or share internal updates outside approved channels. All media inquiries must be routed to the approved spokesperson or communications lead.

Message Approval Requirements

Every non-emergency employee communication related to an incident should be approved before distribution. The approval record should include:

- Message title or description.
- Date and time drafted.
- Drafting owner.
- Reviewing attorney or legal approver.
- HR approver.
- Communications approver.
- Executive Command approver, when required.
- Intended audience.
- Distribution channel.
- Date and time sent.
- Sender.
- Recipient group.
- Version number.
- Follow-up obligations.
- Preservation location.

Emergency workforce instructions may follow an expedited approval process. The expedited process must still be documented after the message is sent.

Employee Communication Rules During BIM Activation

During BIM activation, employees must be instructed to follow these rules unless modified by Executive Command:

- Do not speculate about cause, scope, threat actor, fault, data exposure, operational impact, insurance, regulatory notification, or customer impact.
- Do not forward internal incident communications outside the organization.
- Do not take screenshots of internal incident systems, tickets, chats, or dashboards unless directed for evidence preservation.
- Do not delete suspicious emails, logs, files, messages, or other potential evidence.
- Do not discuss the incident with customers, vendors, media, regulators, or public audiences unless authorized.
- Do not post about the incident on social media or professional platforms.
- Do not use unapproved communication channels for incident discussion.
- Report suspicious activity, customer concerns, employee concerns, or media inquiries through the approved escalation path.
- Follow credential reset, access, system use, and evidence preservation instructions exactly as issued.
- Direct all questions to the designated incident communication contact or help channel.

These rules should be included in the BIM plan and adapted into a ready-to-send employee instruction template.

Legal and Privilege Considerations

Employee communications during an incident must be written with the expectation that they may later be reviewed by insurers, regulators, plaintiffs' attorneys, auditors, customers, or the board. Messages should avoid:

- Assigning blame.
- Admitting fault.
- Characterizing the incident before facts are confirmed.
- Minimizing potential impact.
- Overstating containment.
- Promising outcomes.
- Speculating about data exposure.
- Commenting on legal liability.
- Discussing insurance coverage.
- Describing privileged legal advice.
- Referencing unapproved technical findings.

- Making statements inconsistent with external, regulatory, customer, or board communications.

Where legal advice is being sought or provided, counsel must determine the appropriate communication structure. Employee-facing operational instructions should not be labeled privileged unless counsel determines that treatment is appropriate.

Workforce Trust and Message Tone

Employee communication should be controlled, but it should not sound evasive. Employees need enough information to trust the process and perform their roles. A strong employee message acknowledges the disruption, provides clear instructions, explains where questions should go, and commits to updates without speculating beyond known facts.

Effective employee communication should be:

- Factual.
- Calm.
- Direct.
- Instruction-oriented.
- Consistent with other approved messages.
- Clear about what is known and unknown.
- Clear about what employees should and should not do.

Poor employee communication creates silence. Silence creates rumor. Rumor creates risk.

Employee Question Handling

The BIM plan must define how employee questions will be received, triaged, answered, and preserved. The organization should establish a single employee question intake path during the incident. Depending on the incident, this may be an HR inbox, helpdesk ticket queue, internal form, hotline, manager escalation channel, or dedicated incident communications mailbox.

Employee questions should be categorized by type:

- Technical access issue.
- HR or employment concern.
- Personal data concern.
- Customer question.
- Media or public inquiry.
- Suspected phishing or suspicious activity.
- Legal or compliance concern.
- Safety or operational concern.
- Rumor or misinformation report.

Responses should be based on approved language. Material questions, repeated concerns, misinformation patterns, or employee reports that may affect incident scope should be escalated to the appropriate BIM workstream.

Documentation and Preservation

All employee communications related to the incident must be preserved. The evidence record should include:

- Final message version.
- Approval history.
- Distribution list or audience.
- Channel used.
- Date and time sent.
- Sender.
- Acknowledgments, if required.
- Manager briefing scripts.
- Employee FAQs.
- Updates and corrections.
- Employee questions and approved responses.
- Records of escalated concerns.
- Copies of any emergency instructions.

Employee communication records are part of the organization’s defensibility record. They may be needed to support regulatory response, insurance recovery, litigation defense, board oversight, HR action, customer response, or post-incident review.

Stand-Down Communication

When the incident moves toward stabilization or formal stand-down, employees should receive an approved closing or transition message. The stand-down communication should explain:

- What operational restrictions remain.
- What systems or processes have returned to normal.
- What employee obligations continue.
- What evidence preservation requirements remain active.
- Where employees should report delayed concerns.
- Whether additional employee updates will follow.
- Whether post-incident training, credential actions, or policy changes are expected.

Stand-down does not mean the matter is closed. It means the organization is transitioning from active incident communication to remediation, review, claim support, regulatory response, and corrective action governance.

Required BIM Artifact

Each organization-specific BIM plan should include an Employee Incident Communication Protocol containing:

- Employee communication owner.
- Legal approver.
- HR approver.
- Communications approver.
- Executive Command approval threshold.
- Approved communication channels.
- Alternate communication channels.
- Employee message templates.
- Manager briefing template.
- Employee FAQ process.
- Customer-facing employee instructions.
- Social media and public discussion restrictions.
- Employee question intake path.
- Evidence preservation requirements.
- Stand-down communication template.
- Annual review and exercise requirement.

A cyber incident does not only test the technical response. It tests whether the workforce can remain aligned while the organization is under pressure. Employee communication is the mechanism that keeps internal uncertainty from becoming external damage. See Addendum S for the Employee Incident Communication Protocol.

CHAPTER 14

Operations, Finance, Contracts, and Business Dependencies

The Business Domains That Move Fastest During an Incident

Customer trust, operational disruption, financial impact, and contractual exposure can all escalate within hours of a serious incident. BIM ensures the right leaders are tracking and managing each from the moment of activation.

Operational Continuity

When a security event affects operations — production systems, clinical systems, transaction processing, logistics, service delivery — the business continuity response must activate in parallel with the technical response.

The questions in the first hours of operational impact are not technical. They are business questions: Which systems or functions are critical? What can be operated in a degraded mode? What must be shut down entirely? What contractual obligations are affected? What customers or partners need to be contacted?

BIM defines the operational continuity workstream owner, the authority to activate continuity procedures, the communication responsibilities to customers and suppliers, and the documentation requirements for insurance and contractual defense.

Financial Tracking and Revenue Impact

Financial impact documentation begins at incident activation, not at claim submission.

Business interruption insurance coverage requires proof of the financial impact of the interruption. That proof comes from records kept during the incident, not reconstructed from memory weeks later. Every hour of production downtime, every delayed shipment, every missed transaction, every emergency expenditure — all of it must be tracked contemporaneously.

The CFO workstream in BIM owns this documentation requirement. They activate financial tracking procedures at the same moment the security team activates containment procedures.

Contract Exposure

Contracts create obligations. They create notice obligations — the requirement to tell a customer or partner that something has happened. They create performance obligations — the requirement to deliver something by a defined date. They create SLA obligations — the requirement to maintain a defined service level. They create indemnity obligations — the requirement to compensate a party for losses caused by the failure.

During an incident, contract exposure can escalate quickly. Missed notification windows under contract terms can limit or eliminate remedies. Missed SLA thresholds can trigger penalty

provisions. Failure to provide required notice can expose the organization to breach of contract claims.

BIM defines the contract review trigger — the moment at which the contracting workstream owner reviews key contracts for activated obligations — and the authority to make notification decisions under those contracts.

Contract Notification Matrix

Many cyber incidents trigger contractual obligations before regulatory notification is required. Enterprise agreements, master service agreements, data processing agreements, business associate agreements, government contracts, and SLA-bearing customer contracts all may contain cyber notification provisions with their own triggers, timelines, and required content.

The BIM plan must identify key customer, vendor, partner, payer, business associate, DPA, SLA, MSA, government, and enterprise contract notice requirements before the incident begins. Discovering these obligations during the incident is too late. See Addendum N for the Contract Notification Matrix.

Critical Third-Party Dependency Map

A cyber incident may begin with a vendor, cloud provider, managed service provider, payment processor, clearinghouse, business associate, identity provider, or critical supplier. The incident may originate externally and the organization may be responding to consequences it did not cause.

The BIM plan must identify critical third parties, the business functions they support, data they access, incident contacts, notice obligations, and workarounds if the third party is unavailable or implicated. This mapping is essential for both outbound notification and inbound coordination when a supplier or partner is the source of the incident. See Addendum O for the Critical Third-Party Dependency Map.

Business-Critical Asset and Data Map

BIM cannot determine business consequence without understanding which systems, data, and business functions matter most. The activation brief cannot assess potential impact without a pre-existing map of what the organization depends on.

The BIM plan must identify regulated data, customer data, patient data, employee data, payment data, intellectual property, source code, financial records, privileged identity systems, customer-facing systems, revenue-critical systems, and operationally critical systems — along with who owns each, where evidence related to each is located, and what the business impact of unavailability would be. See Addendum P for the Business-Critical Asset and Data Map.

M&A and Transaction Impact Trigger

A cyber incident must be escalated if it may affect an active financing, acquisition, divestiture, strategic partnership, debt facility, major customer renewal, audit, certification, or regulatory

review. These situations carry disclosure obligations, representation and warranty implications, and strategic consequences that extend well beyond the incident itself.

The escalation goes to General Counsel, CFO, and CEO immediately. The materiality review process in Chapter 11 applies. External transaction counsel may need to be engaged separately from breach counsel.

CHAPTER 15

Evidence, Defensibility, Single Source of Truth, and Action Control

The Work That Happens During the Incident That Protects the Organization After It

Every serious incident ends with a review. That review will examine what the organization knew, what it did, why it made the decisions it made, and whether those decisions were reasonable. BIM builds the record that answers those questions.

The concept of defensibility — the ability to demonstrate that leadership acted reasonably under the circumstances — is one of the most important and most consistently underprepared aspects of incident response.

Legal defensibility requires a documented decision record. Insurance defensibility requires documented evidence of the loss and the organization's response. Regulatory defensibility requires documented proof of a timely, compliant notification process. Board defensibility requires documented proof of appropriate governance.

None of that documentation creates itself. BIM creates it, systematically, from the moment of activation.

The Decision Log

The decision log is the most important defensibility tool in BIM.

For every significant decision made during the incident, the decision log captures: what decision was made, who made it, at what time, what information was available at the time of the decision, what alternatives were considered, and what rationale supports the decision.

That log is not a retrospective narrative. It is a contemporaneous record, maintained by the designated evidence and defensibility workstream owner, updated in real time as decisions are made throughout the incident.

The decision log becomes the organization's proof of reasonable conduct. It shows regulators that the notification analysis was completed methodically. It shows insurers that containment decisions were made with appropriate business authorization. It shows the board that leadership was managing the incident with discipline and documentation.

Evidence Preservation

Evidence preservation is not solely a legal concept. It is a business concept.

The forensic evidence gathered during the incident supports the insurance claim, the regulatory notification analysis, the legal defense, and the board governance record. Loss of that evidence

— through normal retention policies, through inadvertent deletion, through system restoration that overwrites forensic artifacts — damages all of those outcomes.

BIM defines evidence preservation requirements at activation: what must be preserved, who is responsible for preservation, where preserved evidence is stored, under whose authority it can be modified or released, and how long it must be retained.

Single Source of Truth

Executive Command must maintain an approved incident fact record. All board, customer, insurer, regulator, law enforcement, vendor, employee, and public communications must align to that approved fact record unless Legal authorizes otherwise.

Without a single source of truth, workstreams begin communicating inconsistent facts to different audiences. Inconsistency creates the appearance of concealment, even when the inconsistency is simply the result of uncoordinated communications. The single source of truth prevents that problem by centralizing the approved narrative and requiring all communications to draw from it.

The approved incident fact record distinguishes between known facts, confirmed unknowns, and prohibited speculation. It is updated as new information becomes available and approved before it is distributed to communicating workstreams. See Addendum Q for the Single Source of Truth Protocol.

Communication Channel Control

The BIM plan must identify approved communication channels for operational coordination, privileged legal coordination, Executive Command, board updates, vendor communications, customer communications, and law enforcement or government coordination. Different types of communication belong in different channels for reasons of privilege, security, auditability, and record retention.

Using personal messaging apps, unauthorized collaboration tools, or informal channels for incident communications creates privilege exposure, evidentiary problems, and records management failures. BIM defines the approved channels before the incident and ensures workstream owners know which channel applies to which type of communication. See Addendum R for the Incident Communication Channel Control.

Open Action Register

The decision log records what leadership decided. The open action register tracks what still must be done.

During a serious incident, decisions generate follow-on obligations. A decision to notify the insurer creates an action item for the insurance workstream owner. A decision to send a customer communication creates an action item for the communications workstream. A decision to suspend a vendor’s access creates an action item for IT. Without a managed action register, follow-on obligations get missed.

The open action register captures each action item, the workstream owner responsible, the deadline, any dependencies, current status, evidence of completion, and escalation needed. It is reviewed at every Executive Command update cycle. See Addendum T for the Open Action Register format.

Situation Report Cadence

BIM requires a defined reporting rhythm. Without a cadence, workstreams either over-communicate — generating noise that obscures critical information — or under-communicate, leaving Executive Command without the current picture needed to make timely decisions.

The situation report cadence defines how often each workstream reports to Executive Command, what each report must contain, who receives it, and how it is documented. The cadence adjusts based on incident velocity — faster in the first hours, slower as the situation stabilizes. See Addendum U for the BIM Situation Report Template and Cadence.

The Post-Incident Review

Every serious incident should close with a structured post-incident review. The post-incident review is not only a technical exercise. It is a business review.

It should answer: What business decisions were made? Were they made correctly? Were they made quickly enough? What did the BIM process do well? What failed? What changes to the BIM structure are indicated by this incident?

The post-incident review is the mechanism by which BIM improves over time. Organizations that conduct rigorous post-incident reviews and implement the resulting changes become progressively more capable of managing the business event. Organizations that treat the incident as over when the technical response concludes forfeit that opportunity.

PART FOUR

Cyber Scenario Development

How BIM Applies Across the Incidents That Actually Happen

CHAPTER 16

Pre-Approved Incident Vendors and Retainers

The Outside Resources That Must Be Ready Before the Incident

A serious cyber incident often requires outside support before the organization has complete facts.

Counsel may need to be engaged. Forensic investigators may need to preserve volatile evidence. Recovery specialists may need to support restoration. Crisis communications advisors may need to prepare internal or external statements. Notification vendors may need to support affected individuals. Call center providers may need to handle stakeholder volume. Coverage counsel may need to advise on insurance recovery. In ransomware or extortion matters, specialized negotiation, sanctions, law enforcement, and carrier coordination resources may be required.

Those vendors cannot be selected for the first time during the incident.

A vendor is not ready because someone knows the name of the firm. A vendor is ready only when the organization has confirmed the vendor's role, 24/7 activation path, contract or retainer status, conflict check status, procurement approval, rates, cyber insurer panel status, consent requirements, data handling requirements, activation authority, emergency spending authority, and coverage risk.

Why Vendor Readiness Matters

During a cyber incident, time is compressed. The organization may need to engage outside counsel, forensics, recovery, communications, and notification support within hours. If the organization has not pre-approved those resources, leadership may lose critical time to procurement review, contract negotiation, insurer consent questions, internal approval delays, or confusion about who has authority to activate the vendor.

Vendor delay creates business risk.

A forensic delay may affect evidence preservation. A counsel delay may affect privilege-sensitive communications. A recovery vendor delay may extend downtime. A notification vendor delay may affect regulatory or contractual timelines. An insurer panel issue may affect reimbursement. A missing business associate agreement or data processing agreement may create additional compliance exposure.

BIM treats incident vendor readiness as a core operating requirement.

The Privilege Counsel Requirement

The BIM plan must identify the law firm or attorney authorized to support the legal response, advise on privilege-sensitive communications, coordinate breach response, advise on notification analysis, and direct legal-sensitive work where appropriate.

The organization should not discover during the incident that its preferred law firm has not cleared conflicts, is not on the insurer's approved panel, has no retainer in place, cannot be reached after hours, or cannot be engaged without procurement delay.

The BIM plan should identify:

1. primary breach counsel;
2. alternate breach counsel;
3. conflict check status;
4. retainer or engagement status;
5. insurer panel status;
6. emergency contact method;
7. authority to engage counsel;
8. relationship to internal General Counsel;
9. relationship to DFIR provider;
10. relationship to coverage counsel;
11. required documentation for activation.

BIM does not establish legal privilege. Qualified counsel determines how privilege-sensitive work should be structured. BIM helps leadership pre-plan counsel engagement and communication protocols that qualified counsel may use to support privilege where available.

DFIR and Recovery Vendor Readiness

Forensics and recovery are related but different functions.

Forensics answers what happened, what systems were affected, what data may have been involved, what evidence must be preserved, and what facts leadership can rely on when making business decisions.

Recovery helps restore systems, operations, data, services, access, and business continuity.

Both may be needed. Both may have insurance implications. Both should be identified, contracted, and validated before the incident.

The BIM plan should determine:

1. which DFIR provider is approved;
2. whether the DFIR provider is on the cyber insurer's panel;
3. who may activate the DFIR provider;
4. whether counsel must direct the DFIR engagement;
5. what evidence the DFIR provider is expected to preserve;
6. which recovery vendors are approved;
7. whether recovery vendors are insurer-approved or require consent;

8. what systems or environments each vendor can support;
9. what emergency spending authority applies;
10. how vendor work will be documented for insurance, legal, regulatory, and board purposes.

Insurance Carrier Panel Verification

Many cyber insurance policies identify approved or preferred vendors. These may include breach counsel, forensic providers, ransomware or extortion advisors, crisis communications firms, notification vendors, credit monitoring providers, and other response resources.

The organization must not assume that a preferred vendor is reimbursable.

The BIM plan must document whether each vendor is:

1. approved by the carrier;
2. approved only with prior consent;
3. not on the panel but accepted by the organization;
4. pending carrier confirmation;
5. not expected to be claim-relevant;
6. available only under emergency exception.

Carrier panel status should be verified at least annually and after every cyber insurance renewal.

Non-Panel Vendor Coverage Risk

There may be situations where the organization chooses to use a vendor that is not approved by the cyber insurer. That decision may be reasonable. The vendor may have unique expertise, existing knowledge of the environment, sector-specific capability, or urgent availability.

But the decision must not be accidental.

When the organization uses a non-panel vendor whose costs may be submitted as part of an insurance claim, the coverage risk must be acknowledged before or as soon as practicable after activation.

The acknowledgment should document:

1. vendor name;
2. vendor category;
3. reason for using the vendor;
4. insurer panel status;
5. whether carrier consent was requested;
6. whether broker or carrier input was obtained;
7. potential reimbursement risk;

8. emergency business justification;
9. approving executives;
10. decision log reference.

Required Pre-Approved Vendor Categories

Every BIM plan should determine which of the following vendor categories are required for the organization:

1. breach counsel / privilege counsel;
2. coverage counsel;
3. DFIR provider;
4. recovery / restoration provider;
5. crisis communications firm;
6. notification vendor;
7. call center surge provider;
8. credit or identity monitoring provider;
9. eDiscovery / legal hold provider;
10. ransomware / extortion advisor;
11. sanctions or payment compliance advisor;
12. identity recovery provider;
13. backup recovery provider;
14. cloud or SaaS recovery specialist;
15. OT / industrial recovery specialist;
16. payment fraud recovery support;
17. translation or accessibility vendor;
18. mailing / print vendor;
19. regulatory response advisor;
20. customer security response support.

Not every organization will need every category. The BIM plan must determine which categories are applicable based on industry, business model, data, systems, regulatory exposure, customer obligations, insurance requirements, and operational dependencies.

Vendor Contract Minimum Requirements

Pre-approved vendors should not be listed in the BIM plan unless the organization has confirmed the minimum conditions for incident activation.

At a minimum, the organization should confirm:

1. 24/7 activation contact;

2. response-time expectation;
3. emergency authorization process;
4. rates and billing terms;
5. confidentiality requirements;
6. data handling requirements;
7. HIPAA business associate agreement or data processing agreement where applicable;
8. evidence preservation obligations;
9. chain-of-custody requirements;
10. privilege or counsel-direction expectations where applicable;
11. insurance cooperation requirements;
12. invoice detail required for claim support;
13. subcontractor restrictions;
14. conflict disclosure requirements;
15. secure communication requirements;
16. report ownership;
17. records retention requirements.

Vendor Activation Authority

Vendor activation is a decision-authority issue, a spending-authority issue, a legal issue, and an insurance issue.

The BIM plan must define who may activate each vendor category, what approvals are required, whether insurer consent must be checked, whether counsel must be involved, what emergency spending authority applies, and how the activation must be documented.

The Decision Authority Matrix should include vendor activation authority for all material incident vendors.

Annual Vendor Readiness Validation

Vendor readiness expires as contracts, people, insurance policies, systems, and business requirements change.

The organization should validate vendor readiness at least annually and after:

1. cyber insurance renewal;
2. change in broker or carrier;
3. change in breach counsel;
4. change in DFIR provider;
5. change in recovery provider;
6. material system or cloud migration;

7. merger, acquisition, divestiture, or restructuring;
8. major change in regulated data;
9. major change in customer or contract obligations;
10. post-incident corrective action.

Core principle: An incident vendor is not ready because it has been identified. It is ready only when it has been contracted, approved, validated against insurance requirements, assigned to an activation owner, and acknowledged for coverage risk.

See Addendum Y for the Pre-Approved Incident Vendor and Retainer Register.

CHAPTER 17

Ransomware and Cyber Extortion Scenario Development

The Business Event Inside the Technical Crisis

Governing Question: *When does the technical recovery decision become a business authorization decision?*

Ransomware events are defined by compression. Time compresses. Information compresses. Options compress. BIM ensures that executive decision authority is available when compression is most severe.

Ransomware is the incident most likely to activate all eleven business pressure domains simultaneously. Production is down or threatened. Insurance notice must go out. Legal must be engaged under privilege from the first hours. Regulatory analysis may be required. The board needs to be briefed. Customers are waiting for information. Operations must shift to contingency procedures. Finance must begin tracking the business interruption loss. Contracts may be triggered. And every decision — including whether to pay, whether to restore from backups, whether to contact law enforcement, whether to engage a ransomware negotiation specialist — is a business decision with legal, insurance, and regulatory implications.

None of those decisions belong to the security team alone.

The Payment Decision

The ransom payment decision is not a technical decision. It is a business decision with legal, regulatory, financial, and reputational dimensions.

BIM defines who has authority to make the payment decision, what inputs are required before the decision is made, what legal review must occur, what insurance implications exist, what OFAC screening is required, what law enforcement implications apply, and how the decision is documented.

Organizations that have not built this structure discover during the incident that nobody is clearly authorized to make the payment decision, that their insurer has specific requirements that must be met before a payment can be covered, that their broker must be notified before a payment is initiated, and that the legal review required to ensure the payment does not violate sanctions law takes time they do not feel they have.

Ransom and Extortion Governance

No individual executive may independently authorize, initiate, negotiate, or facilitate ransom or extortion payment. This constraint exists because the ransom decision carries consequences —

for insurance coverage, for sanctions exposure, for law enforcement coordination, for board oversight, and for public communications — that no single executive can manage unilaterally.

The BIM plan must define who receives extortion communications, who may communicate with threat actors, whether a negotiator is pre-approved, whether carrier consent is required, who checks sanctions implications, who contacts law enforcement, who briefs the board, who can authorize cryptocurrency acquisition, who approves payment, and how rejection or payment is documented. See Addendum V for the Ransom and Extortion Governance Protocol.

The Restoration Decision

Restoration from backups — if backups are available and uncompromised — sounds straightforward. In practice, the restoration decision involves complex business tradeoffs: how long will restoration take, what level of service can be maintained during restoration, which systems are restored in what priority, what data loss is acceptable, and who has authority to accept degraded service during the restoration period.

BIM defines restoration decision authority in advance. The COO or operations workstream owner has pre-defined authority to accept defined levels of operational degradation during recovery. That authority is not discovered during the incident. It was granted before it.

Ransomware BIM Development Questions

Organizations developing ransomware-specific BIM scenarios should work through the following:

- Who activates BIM when ransomware is detected?
- Who is authorized to activate clinical, operational, or financial downtime procedures?
- Who contacts the cyber insurer within the notice window?
- Who initiates legal engagement under privilege?
- What is the board notification threshold for ransomware events?
- Who owns the ransom payment decision governance process?
- Who conducts OFAC and sanctions screening before any payment is considered?
- Who coordinates with law enforcement and under what authorization?
- What evidence must be preserved before restoration begins?
- Who tracks the business interruption financial impact from the first hour?

Vendor Readiness Questions

1. Which breach counsel is authorized to direct the response?
2. Which DFIR provider is approved and available?
3. Which recovery vendor can support restoration?
4. Which ransomware or extortion advisor is pre-approved?
5. Is the ransomware advisor insurer-approved?

6. Who performs sanctions or payment compliance review?
7. Who coordinates law enforcement engagement?
8. Who documents carrier consent and coverage risk?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

- Who approves customer and partner communications about availability?
- What contracts may be triggered by the downtime or data exposure?

CHAPTER 18

Healthcare Cyber Scenario Development

When Clinical Operations, Patient Trust, and Regulatory Obligation Collide

Governing Question: *When does a cyber alert become a clinical, operational, privacy, or executive incident?*

These development questions are for healthcare organizations. They are not a reusable healthcare plan. Every healthcare organization's BIM plan must reflect its specific patient population, clinical environment, regulatory obligations, payer relationships, and business associate ecosystem.

In healthcare, a cyber incident is never solely a technology problem. It is a patient safety problem, a regulatory problem, an insurance problem, and a leadership accountability problem simultaneously. The healthcare sector faces a convergence of pressures that no other sector experiences in exactly the same combination. HIPAA notification requirements. Clinical downtime procedures. Patient safety obligations. Payer relationship impacts. Public trust in the institution. State breach notification laws. CMS obligations. The intersection of legal privilege and HIPAA minimum necessary standards. Medical record integrity.

Each of those pressures has a clock. Each has a decision owner. Each has documentation requirements. And each activates at or near the same time.

Clinical Downtime Authority

One of the most consequential decisions in a healthcare incident is who has authority to activate clinical downtime procedures — the shift to paper-based or degraded-mode clinical operations when electronic health record systems are unavailable.

That authority must be named in advance. Clinical staff cannot wait for committee approval. Patients are present. Clinical decisions are being made. The downtime decision must be made by an authorized clinical or operational leader, and it must be made quickly.

BIM defines that authority, the activation criteria, the clinical communication process, and the documentation requirements for the duration of the downtime period.

The HIPAA Notification Analysis

HIPAA notification analysis in a healthcare incident determines whether a breach of protected health information occurred, whether any applicable exceptions apply, and whether notification to patients, HHS, and potentially media is required.

That analysis is not performed by the security team. It is performed by privacy counsel, the privacy officer, or both, in consultation with the technical team regarding the nature and scope of the potential access.

BIM defines who leads the HIPAA notification analysis, what inputs they need, when the analysis must be completed, who has final authority over the notification determination, and how that determination is documented.

The 60-day notification window under HIPAA is not a cushion. It is a maximum. Analysis that cannot begin because the right people do not know they are responsible for it, or because the inputs required for the analysis are not being gathered during the incident, can result in missed deadlines even in incidents where 60 days feels like adequate time.

Healthcare BIM Development Questions

Healthcare organizations should work through the following when building scenario-specific BIM plans:

- Who owns PHI analysis and what triggers it?
- Who owns clinical downtime activation authority?
- Who determines whether patient safety is at immediate risk?
- Who coordinates with business associates during the incident?
- Who owns patient communication and under what legal guidance?
- Who tracks payer implications — including claims, eligibility, and authorization processing?
- Who preserves EHR access logs and clinical documentation evidence?
- Who coordinates HIPAA notification with HHS and who approves the notification content?
- Who manages state attorney general notification requirements?
- Who owns media response if patient data is involved?
- Who is authorized to communicate with clinical staff about downtime procedures?
- Who tracks the cost of clinical downtime for insurance purposes?

Vendor Readiness Questions

1. Which breach counsel has healthcare privacy experience?
2. Which DFIR vendor can access and analyze EHR-relevant evidence?
3. Which notification vendor has a current BAA and patient notification capability?
4. Which call center vendor can support patient, family, payer, and provider surge volume?
5. Which recovery vendor understands clinical downtime and EHR restoration?
6. Which communications advisor can support patient-facing and media messaging?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 19

Financial Services and FinTech Cyber Scenario Development

Speed, Regulatory Density, and the Hours That Define the Outcome

Governing Question: *Who decides whether to suspend transactions before the full technical picture is known?*

In financial services, the first hours of a serious incident compress months of regulatory and legal consequence into decisions that must be made before the facts are complete. Financial institutions operate under some of the most complex and time-sensitive notification obligations in any regulated sector. GLBA. PCI DSS. Federal banking regulators. State financial services regulators. SEC for public institutions. CISA for critical infrastructure. FinCEN for potential financial crimes.

Those obligations do not wait for the technical investigation to conclude.

Transaction Suspension Authority

The decision to suspend transactions — to halt payment processing, to pause trading, to restrict account access — is one of the most consequential business decisions available during a financial services incident.

It protects customers and the institution from ongoing fraud. It also stops legitimate business activity, creates customer disruption, and may have market implications if the institution is publicly traded or if the suspension becomes known.

BIM defines who has authority to make that decision, at what threshold, with what information, and under what legal and regulatory review. It is not a decision made by the security team. It is an executive decision made by the person BIM has already designated — before the incident — as the transaction suspension authority.

Law Enforcement Coordination

Many financial services incidents involving fraud, business email compromise, or ransomware benefit from early law enforcement coordination. The FBI, the Secret Service, and other agencies have forensic capabilities and intelligence that may assist in the investigation and recovery.

That coordination has legal implications. It has regulatory implications. And it requires executive authorization.

BIM defines the law enforcement coordination decision authority, the legal review required before outreach, the information that can and cannot be shared at various stages, and the documentation requirements that preserve the organization's legal position during the coordination.

Financial Services and FinTech BIM Development Questions

Financial services organizations and FinTechs should work through the following:

- Who can suspend transactions and at what threshold?
- Who contacts banking partners — correspondent banks, card networks, payment processors — and under what authorization?
- Who coordinates with fraud operations and at what point in the incident?
- Who contacts Secret Service, FBI, or IC3 — and who authorizes that contact?
- Who handles account takeover communications to affected customers?
- Who owns customer financial harm tracking and restitution decisions?
- Which policies apply: cyber, crime, technology E&O, D&O?
- Who manages the 36-hour banking regulator notification requirement?
- Who owns GLBA notification analysis?
- Who is authorized to communicate with the primary federal regulator?
- Who manages customer-facing communications about service disruption?
- What is the board notification threshold for regulatory reporting incidents?
- Who tracks the financial fraud loss for claim purposes?

Vendor Readiness Questions

1. Which DFIR provider can support transaction integrity investigation?
2. Which payment fraud recovery contacts are pre-established?
3. Which banking partner escalation contacts are current?
4. Which outside counsel supports regulatory and customer notification?
5. Which insurer policies may apply beyond cyber?
6. Which vendors support customer account security response?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 20

SaaS and Cloud Platform Cyber Scenario Development

When the Product Is the Affected Environment

Governing Question: *When does a technical security event become a customer trust and contractual obligation event?*

SaaS and cloud platform businesses face a distinct incident challenge: the affected environment is the product itself. When the platform is compromised, customer data is at risk, service delivery is impaired, and contractual obligations may be activated — all simultaneously and in the view of customers who are watching the status page in real time.

The business consequences of a SaaS incident extend further and faster than most other environments because the customers are not just notified — they are experiencing the incident. Their workflows are disrupted. Their data may be exposed. Their own customers may be affected. The obligation to communicate runs not just to regulatory bodies but to paying customers with legal agreements that define what must be communicated, when, and how.

Multi-Tenant Boundary Considerations

In a multi-tenant platform environment, a breach affecting one tenant's data may affect the confidence of all tenants. The question of whether a tenant-level incident constitutes an organizational-level incident — with all the BIM activation consequences that follow — must be answered before the incident begins, not during it.

BIM defines the multi-tenant boundary determination process: who makes it, what triggers it, what legal review it requires, and what communication obligations it creates. The technical determination of what was accessed in a multi-tenant environment cannot be separated from the business determination of who is owed notification and under what contractual and regulatory obligations.

SaaS and Cloud Platform BIM Development Questions

SaaS and cloud platform organizations should work through the following:

- Does the incident affect customer data?
- Does it affect multi-tenant boundaries — and who makes that determination?
- Does it affect APIs — and which customers use the affected APIs?
- Does it affect uptime or SLA commitments, and which customers are threshold-affected?
- Who owns the status page and what authorization does an update require?

- Who owns trust center updates and under what approval process?
- Who coordinates with customer security teams who will detect the incident independently?
- Who reviews DPAs, MSAs, and security addenda for triggered obligations?
- Who decides whether customers must be notified before full technical scope is known?
- Who owns customer success outreach for strategic and enterprise accounts?
- Who manages regulator notification if the platform processes data in regulated sectors?
- Who owns the board notification decision if the incident may be material?
- Who tracks financial exposure from SLA penalties and customer churn?

Vendor Readiness Questions

1. Which DFIR provider can investigate cloud, API, identity, and multi-tenant issues?
2. Which recovery vendor understands the platform architecture?
3. Who supports customer security response?
4. Who supports status page and trust center communications?
5. Who can validate customer-facing technical statements before release?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 21

MedTech and Connected Product Cyber Scenario Development

When the Security Incident Is Also a Patient Safety Event

Governing Question: *Who determines whether a product security event creates a patient safety obligation?*

MedTech and connected medical device organizations face a convergence of product security, patient safety, regulatory, and liability obligations that do not exist in the same combination in any other sector. A software vulnerability in a connected device is not only a cybersecurity event. It may be a patient safety event, a regulatory reporting event, a product recall decision, and a coordinated disclosure obligation simultaneously.

The business consequence chain in a MedTech incident can run from the device to the patient, from the patient to the provider, from the provider to the payer, and from all of them to the regulator — across a timeline that may run from immediate safety response to multi-year regulatory scrutiny.

Product Safety and Regulatory Intersection

In MedTech, the security team does not make the patient safety determination alone. Quality, regulatory affairs, clinical, and legal all have roles in determining whether a product security event creates safety obligations. BIM defines the cross-functional governance structure for that determination before the incident requires it.

The FDA's expectations for cybersecurity incident response in medical devices, the coordinated vulnerability disclosure process for device manufacturers, and the intersection of device safety with HIPAA obligations all require a pre-built governance structure that most MedTech organizations do not have.

MedTech and Connected Product BIM Development Questions

MedTech and connected product organizations should work through the following:

- Does the incident affect device safety — and who makes that determination?
- Does it affect remote monitoring or device telemetry?
- Does it affect software update integrity — and what devices may have received compromised updates?
- Does it affect clinical workflow at provider facilities?
- Does it require coordinated vulnerability disclosure, and who manages that process?

- Who owns product security response within the organization?
- Who owns quality and regulatory coordination during the incident?
- Who determines whether provider notification is required and what form it takes?
- Who evaluates product liability implications with counsel?
- Who evaluates FDA or other regulatory expectations with counsel?
- Who manages communications to providers currently using affected devices?
- Who tracks recall or field safety corrective action implications?
- Who coordinates with cyber insurers when product liability may be implicated?

Vendor Readiness Questions

1. Which product security experts are pre-approved?
2. Which regulatory counsel supports product cybersecurity issues?
3. Which communications provider supports provider, customer, and patient communications?
4. Which DFIR vendor understands connected device and cloud architecture?
5. Who supports coordinated vulnerability or safety-related communications?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 22

Manufacturing and OT Cyber Scenario Development

When the Cyber Event Stops Production

Governing Question: *Who can authorize containment if the containment disrupts production?*

Manufacturing incidents are measured in business consequences: production stoppage, delivery failures, supply chain disruption, and revenue loss. BIM ensures those consequences are governed, not discovered.

Operational technology — the systems that run manufacturing plants, production lines, logistics networks, and physical infrastructure — presents incident response challenges that IT-focused frameworks do not fully address. OT systems have different resilience requirements, different downtime tolerances, and different recovery timelines than enterprise IT systems. And in a manufacturing environment, the business consequences of a security event are often measurable in real time.

Production Shutdown Authority

The containment decision in a manufacturing environment is the business decision with the most immediate and measurable consequence. Isolating an OT network segment may stop an attack. It may also stop production.

Who has the authority to make that tradeoff? Who can tell the security team to contain the threat even if containment halts the production line? Who can accept the business cost of that decision and document the rationale?

BIM answers that question before the incident begins. The production shutdown authority is named. The threshold criteria are defined. The decision process is documented. When the security team presents the containment options, the right person is available, authorized, and ready to decide.

Customer and Supply Chain Communication

When production is disrupted, customer commitments are affected and supply chain partners need to be managed. Those communications cannot wait for the technical response to conclude.

BIM activates the customer and vendor management workstream at the same time as the technical response. The CRO or customer success leader begins assessing commitment

exposure. The supply chain or procurement leader begins managing supplier expectations. Communications are drafted under legal review.

The customer hears from the organization, on the organization's terms, before they hear from someone else.

Manufacturing and OT BIM Development Questions

Manufacturing organizations should work through the following:

- Who can authorize production shutdown and at what threshold?
- Who can authorize containment affecting OT systems when containment creates business consequences?
- Who owns safety review when OT systems are affected — including physical safety implications?
- Who tracks production loss for business interruption insurance purposes?
- Who communicates with customers about delivery disruption and under what authorization?
- Who owns supplier coordination when supply chain obligations are threatened?
- Who evaluates product integrity risk if the manufacturing process was affected?
- Who preserves OT logs and engineering evidence before restoration begins?
- Who contacts cyber insurers about business interruption and what evidence do they need?
- Who manages regulatory reporting if safety systems were affected?
- What is the board notification threshold for production events?

Vendor Readiness Questions

1. Which OT or ICS recovery vendor is pre-approved?
2. Which plant restoration vendor is under contract?
3. Which DFIR provider can handle OT evidence?
4. Which safety and operations experts are part of escalation?
5. Which vendor can support production restart validation?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 23

Government Contractor Cyber Scenario Development

When Your Security Obligations Are Also Your Contractual Obligations

Governing Question: *Who is authorized to contact the government customer, and what must they say?*

Government contractors face a cyber incident environment defined by contractual obligations that function as regulatory obligations. CMMC requirements. DFARS clauses. NIST SP 800-171 compliance representations. CUI handling obligations. Mandatory reporting to the prime contractor or directly to the government customer within defined timeframes.

A cyber incident for a government contractor is not just a security event. It is a potential contract performance failure, a representation and warranty event, and a compliance disclosure obligation. The False Claims Act and related statutes create exposure for contractors who certify compliance with security requirements that may not have been met.

These are not issues the security team can manage. They require legal counsel, senior leadership, and pre-built governance that is specific to the contracting environment.

CUI and Contract Notification

If a government contractor incident may have affected Controlled Unclassified Information, the contractor's notification obligations are immediate, specific, and contractually binding. The BIM plan must identify which contracts contain CUI, what notification clauses apply, who the authorized notification contact is, and what information must be provided.

Discovering these obligations during an incident — when the clock is already running — is not a viable response posture. BIM maps these obligations before the incident and assigns the notification responsibility to named individuals who understand both the contractual requirements and the legal implications of the notification.

Government Contractor BIM Development Questions

Government contractors should work through the following:

- Does the incident affect CUI, and who makes that determination?
- Does it trigger contract notification requirements, and what are the timelines?
- Does it affect prime contractor obligations if the organization is a subcontractor?
- Does it affect security representations made during the contract award or compliance certifications?

- Does it affect CMMC or NIST SP 800-171 compliance commitments?
- Who contacts the government customer or prime contractor, and under what authorization?
- Who preserves contract evidence and security documentation?
- Who reviews disclosure obligations with qualified counsel before any notification is sent?
- Who assesses False Claims Act or certification exposure with counsel?
- Who manages the relationship with the contracting officer during the incident?
- What is the board notification threshold if a major government contract may be at risk?

Vendor Readiness Questions

1. Which counsel supports CUI or government contract disclosure?
2. Which DFIR vendor understands evidence requirements for government contracts?
3. Which vendor supports NIST, CMMC, or contract-related technical evidence?
4. Which contract advisory support is pre-approved?
5. Who coordinates customer, contracting officer, or agency communication?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 24

Third-Party and Vendor Cyber Scenario Development

When the Breach Is Not in Your Organization, but the Consequences Are

Governing Question: *When does third-party activity become your executive incident?*

Third-party incidents present a specific challenge: the organization is experiencing consequences it did not cause and may not be able to fully investigate. BIM addresses the business response regardless of where the technical event originated.

Supply chain and third-party incidents have become among the most consequential types of cyber events. An organization's vendor, supplier, service provider, or partner is compromised, and the consequences flow downstream — to the organization and its customers, patients, or partners.

The business response challenges in a third-party incident are distinct from those in a direct incident. The organization may not have full visibility into the technical scope. The vendor may be managing their own incident response, which may or may not be aligned with the organization's interests. The organization's own notification obligations may depend on information that only the vendor possesses.

The Third-Party Incident Decision

One of the first BIM decisions in a third-party incident is whether to declare the event an organizational incident. That declaration triggers BIM activation, which triggers workstream activation, evidence preservation, legal engagement, insurance notice evaluation, and regulatory analysis.

If the vendor's incident has or may have created exposure for the organization's customers, data, operations, or regulatory obligations, BIM activates. The source of the technical event is irrelevant to the business consequences it creates.

Vendor Escalation and Legal Review

The organization's response to a third-party incident must be coordinated with legal counsel from the first hours. The vendor may be managing communications in a way that does not protect the organization's legal position. Contractual provisions — indemnity clauses, notification requirements, cooperation obligations — may be activated.

BIM defines the vendor escalation protocol: who contacts the vendor, under what terms, through what channel, with what legal review of the communications. The organization does not allow its legal position to be defined by a vendor that has different interests during an active incident.

Third-Party Ecosystem Coverage

The BIM plan should include scenario development for the full third-party ecosystem, including:

- Cloud providers — IaaS, PaaS, SaaS
- Managed service providers and MSSPs
- Clearinghouses and payment processors
- Business associates and healthcare data processors
- API providers and integration partners
- Logistics and fulfillment vendors
- Payroll and HR service providers
- Identity providers and authentication services
- Data processors under GDPR, CCPA, or other privacy frameworks

Each of these vendor categories creates different notification obligations, different contractual provisions, and different business consequences when compromised.

Third-Party BIM Development Questions

- Does the third-party incident create data exposure for the organization’s customers or employees?
- Does it trigger the organization’s own regulatory notification obligations?
- What contractual provisions govern the vendor’s obligations to the organization?
- What indemnification rights exist and who manages the claim process?
- Who coordinates with the vendor and under what legal constraints?
- Who notifies customers if their data was exposed through the vendor?
- Who manages business continuity if the vendor is unavailable?
- Who evaluates alternative vendors or workarounds?

Vendor Readiness Questions

1. Which vendors caused, contributed to, or were affected by the incident?
2. Which vendors are needed to respond to the incident?
3. Which vendor contracts contain notification, cooperation, audit, indemnity, or SLA obligations?
4. Which response vendors are approved to investigate vendor-origin incidents?
5. Who coordinates third-party evidence requests?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 25

Business Email Compromise and Cyber-Enabled Fraud Scenario Development

When the Attack Is on the Decision, Not the System

Governing Question: *Who has the authority to attempt payment recall, and what window exists to act?*

Business email compromise and cyber-enabled fraud are among the most financially damaging incident types, and among the most time-sensitive. In a payment fraud event, the window to act — to attempt a recall, to contact the receiving bank, to engage law enforcement — may be measured in hours.

These incidents rarely look like technical security events in their first moments. They look like a vendor changing banking information, an executive authorizing an urgent wire transfer, or an employee receiving instructions from what appears to be a trusted source. By the time the fraud is recognized, decisions have already been made — and money has already moved.

BIM cannot prevent the fraud. It can define who acts in the minutes after discovery, under what authority, and with what pre-built contacts to maximize the chance of recovery and minimize further exposure.

BEC and Fraud BIM Development Questions

Organizations should work through the following when building BEC and fraud-specific scenarios:

- Who contacts the bank fraud desk immediately upon discovery, and does that person have pre-established contacts?
- Who decides whether to contact the Secret Service, FBI, or IC3 — and under what authorization and legal review?
- Which policies may respond: cyber policy, crime policy, or both — and what are the notice requirements for each?
- Who initiates the payment recall process and what information does it require?
- Who communicates with the customer or vendor whose identity was impersonated?
- Who investigates the affected employee's account and mailbox access?
- Who preserves mailbox evidence before it is overwritten or deleted?
- Who tracks the financial loss for insurance and law enforcement purposes?
- Who owns customer or vendor communication if the fraud was impersonating the organization?

- Who manages employee communication about the investigation?
- What is the board notification threshold for significant fraud losses?
- Who conducts legal review before any public statement about the fraud is made?

Vendor Readiness Questions

1. Which treasury fraud desk contacts are pre-established?
2. Which banking partner contacts are current?
3. Which law enforcement reporting path is approved?
4. Which crime policy or cyber policy notice contacts are required?
5. Which email forensic vendor is approved?
6. Who coordinates payment recovery documentation?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

CHAPTER 26

Unauthorized Access and Data Exposure Scenario Development

When the Question Is What Was Accessed, by Whom, and Who Must Be Told

Governing Question: *Who leads the notification analysis, and what inputs do they need before the deadline expires?*

Unauthorized access and data exposure events are defined by a central question the organization must answer under deadline: was data accessed, and if so, whose, what kind, and does anyone need to be told?

That question requires legal analysis, technical investigation, data classification, regulatory mapping, and executive decision authority — all under the timeline pressure imposed by applicable notification laws and contracts.

The organizations that manage these events best are the ones that have done the analytical work in advance: mapping their data, knowing their notification obligations, and naming the people who will lead the notification analysis before the first notification deadline begins to run.

Unauthorized Access and Data Exposure BIM Development Questions

Organizations should work through the following:

- Who owns data classification and can quickly determine what types of data were potentially accessed?
- Who owns the notification analysis and what inputs do they need from the technical team?
- What regulatory frameworks apply to the affected data and affected individuals?
- Who has final authority over the notification determination?
- What is the documentation requirement for a determination that notification is not required?
- Who manages state attorney general notification requirements across multiple jurisdictions?
- What contractual notification obligations exist beyond regulatory requirements?
- Who approves customer and affected individual notification language?
- Who manages the credit monitoring or identity restoration service process if required?
- Who coordinates regulator inquiry response after notification?
- How are identity credential reset decisions made for affected accounts?

- Who owns communications to affected individuals and what is the legal review process?
- Who tracks the notification process and evidence for potential regulatory examination?

Vendor Readiness Questions

1. Which privacy counsel supports notification analysis?
2. Which forensic provider can determine access, acquisition, exposure, or exfiltration?
3. Which notification vendor is approved?
4. Which call center vendor is approved?
5. Which credit or identity monitoring provider is approved?
6. Which customer security response support is available?

Vendor readiness questions should not be treated as generic prompts. The organization-specific BIM plan must answer them with actual vendors, contacts, contracts, authority, insurer status, and activation procedures.

PART FIVE

Sector-Specific BIM v6 Appendices

Reference Models for Industries With Sector-Specific Pressure Points

The chapters that follow are not universal requirements for every organization. They are reference models for industries where the business consequence of a cyber incident creates sector-specific pressure points that the general BIM framework does not fully capture on its own.

Each appendix includes a governing question, required elements, and at least one decision-record template. Every organization must adapt these appendices to its actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. None of the appendices replace review by qualified counsel, compliance, quality, or risk advisors, and none guarantee regulatory compliance, claim payment, or liability reduction.

> *Security response addresses the threat. Business Impact Management addresses what the threat becomes — and in regulated and safety-sensitive sectors, what the threat becomes is rarely generic.*

CHAPTER 36

Healthcare Appendix

Clinical Downtime and Patient Safety Authority Protocol

Governing Question: *Who can activate clinical downtime when patient safety may be affected, and what evidence must be preserved?*

This appendix is a reference model, not a universal requirement. Organizations must adapt it to their actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. It does not substitute for review by qualified counsel, compliance, and risk advisors. Timing and legal obligations referenced in this appendix must be validated by counsel.

Required Elements

1. clinical downtime activation authority
2. patient safety override authority
3. CMO / COO / CISO / Legal coordination
4. affected site and service-line identification
5. EHR downtime procedure location
6. manual documentation process
7. patient diversion or appointment cancellation authority
8. patient safety event escalation
9. clinical communication approval
10. payer and revenue cycle impact tracking
11. clinical downtime evidence for insurance
12. return-to-normal criteria

Clinical Downtime Decision Record

Site / Service Line	
Systems Affected	
Patient Safety Concern	
Downtime Activated By	
Time Activated	
Manual Procedures Used	

Patient Impact	
Revenue / Payer Impact	
Communications Required	
Evidence Location	
Return-to-Normal Approval	

CHAPTER 37

Banking Appendix

Customer Financial Harm and Restitution Protocol

Governing Question: *Who owns customer financial harm when the cyber event affects accounts, transfers, fraud, or payment rails?*

This appendix is a reference model, not a universal requirement. Organizations must adapt it to their actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. It does not substitute for review by qualified counsel, compliance, and risk advisors. Timing and legal obligations referenced in this appendix must be validated by counsel.

Required Elements

1. unauthorized EFT claim intake
2. provisional credit timeline tracking
3. fraud-loss classification
4. reimbursement authority
5. fee reversal authority
6. account lock / restriction authority
7. card, ACH, wire, Fedwire, and digital banking escalation
8. correspondent bank coordination
9. customer communication by harm category
10. bond/crime/cyber claim linkage
11. Reg E and other customer protection analysis
12. Risk Committee reporting threshold

Customer Financial Harm Record

Account / Customer	
Event Type	
Amount	
Reg E / Other Rule Analysis	
Provisional Credit Status	
Reimbursement Decision	
Insurance / Bond Link	

Owner	
Closure Evidence	

CHAPTER 38

MedTech Appendix

Product Safety, CVD, Recall, and QMS/CAPA Protocols

Governing Question: *Who determines whether a product security event creates a patient safety, regulatory, field action, coordinated disclosure, or product liability obligation?*

This appendix is a reference model, not a universal requirement. Organizations must adapt it to their actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. It does not substitute for review by qualified counsel, compliance, and risk advisors. Timing and legal obligations referenced in this appendix must be validated by counsel.

Required Elements

1. product safety decision authority
2. clinical safety input
3. quality/regulatory owner
4. FDA / EU MDR / international regulator analysis
5. coordinated vulnerability disclosure process
6. provider notification process
7. patient/caregiver communication process
8. recall / field safety corrective action decision record
9. product liability coverage coordination
10. QMS/CAPA handoff
11. connected device / firmware / telemetry evidence package
12. notified body / international regulator coordination path

Recall / Field Safety Corrective Action Decision Record

Product / Device / Software Version	
Safety Signal	
Technical Finding	
Affected Population	
Alternatives Considered	
Regulatory Input	

Provider / Patient Comm Need	
Recall / Field Action Decision	
Board / Committee Notification	
Insurance / Product Liability Link	
QMS / CAPA Entry Required?	
Evidence Location	

CHAPTER 39

FinTech Appendix

Customer Funds, Trading Integrity, SAR/BSA, and Clearing/Custody Protocols

Governing Question: *Who protects customer funds, trading integrity, and regulated financial activity when the incident affects both technology and financial obligations?*

This appendix is a reference model, not a universal requirement. Organizations must adapt it to their actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. It does not substitute for review by qualified counsel, compliance, and risk advisors. Timing and legal obligations referenced in this appendix must be validated by counsel.

Required Elements

1. stored-value ledger freeze criteria
2. transfer pause criteria
3. customer funds reconciliation
4. trading halt or restriction authority
5. order routing and execution integrity review
6. clearing partner coordination
7. custody/holdings reconciliation
8. SAR/BSA restricted decision record
9. sanctions / OFAC review
10. SEC / FINRA / FinCEN / state MTL decision tracking
11. customer reimbursement / make-whole authority
12. platform restart criteria

Trading Integrity Decision Record

Affected Trading System	
Impacted Accounts	
Order Types Affected	
Time Window	

Orders Entered/Routed/Modified/Cancelled	
Execution Accuracy	
Holdings Reconciliation Status	
Clearing Partner Status	
Trading Restriction Decision	
SEC / FINRA Analysis	
Customer Communication Decision	
Evidence Location	

SAR / BSA Restricted Decision Record

Suspected Activity Type	
Trigger Facts	
Detection Source	
Account / Customer Population	
Transaction Value	
SAR Deadline	
Sanctions Implications	
Filing Decision	
Filing Date	
Restricted Access List	
Prohibited Disclosure Reminder	

CHAPTER 40

SaaS / HealthSaaS Appendix

Tenant Scoping, Subprocessor Coordination, and Customer Notification Protocols

Governing Question: *When does a tenant-level incident become an organization-level business incident, and who owns downstream customer consequence management?*

This appendix is a reference model, not a universal requirement. Organizations must adapt it to their actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. It does not substitute for review by qualified counsel, compliance, and risk advisors. Timing and legal obligations referenced in this appendix must be validated by counsel.

Required Elements

1. tenant impact scoping authority
2. single-tenant vs. multi-tenant vs. platform-wide determination
3. customer notification support
4. covered entity support where applicable
5. subprocessor coordination
6. status page / trust center approval
7. customer success surge
8. support ticket tagging
9. SLA exposure and service credits
10. tenant isolation validation
11. platform restart criteria
12. mass notification and call center activation

Tenant Impact Scoping Decision Record

Affected System / Service	
Scope Classification	
Tenant List Version	
Included Tenants	
Excluded Tenants	

Basis for Inclusion/Exclusion	
Evidence Reviewed	
Confidence Level	
Customer Notification Consequence	
Approved By	
Timestamp	
Change From Prior Version	

CHAPTER 41

Financial Services / RIA Appendix

Fiduciary Integrity, Custodian Coordination, and Discretionary Trading Authority Protocols

Governing Question: *Was the fiduciary authority relationship itself exploited, undermined, or placed at risk?*

This appendix is a reference model, not a universal requirement. Organizations must adapt it to their actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. It does not substitute for review by qualified counsel, compliance, and risk advisors. Timing and legal obligations referenced in this appendix must be validated by counsel.

Required Elements

1. fiduciary integrity decision authority
2. discretionary trading exposure review
3. custodian interface verification
4. account activity reconciliation
5. trade modification / cancellation review
6. transfer and distribution instruction review
7. client asset restoration / make-whole protocol
8. Form ADV and SEC/state regulator decision tracking
9. professional liability / E&O coordination
10. crime/fidelity bond evidence
11. client relationship tiering
12. client counsel / trustee / family office communication process

Fiduciary Integrity Decision Record

Affected System / Process	
Impacted Client Accounts	
Discretionary Authority Implicated?	
Custodian Credential Exposure?	
Order Entry/Mod/Cancel Risk	

Transfer/Distribution Risk	
Evidence Reviewed	
Unauthorized Activity Known?	
Confidence Level	
Fiduciary Breach Risk Determination	
Client Disclosure Determination	
SEC/Form ADV Analysis Link	
Approver	
Timestamp	N e x t R e v i e w
Next Review	

CHAPTER 42

Manufacturing / IT-OT Appendix

OT Safety, Machine Restart, Shipped Product Conformance, and DFARS/CMMC/ITAR Protocols

Governing Question: *Could the cyber event affect physical machine behavior, worker safety, part conformance, shipped product, or defense/customer contractual obligations?*

This appendix is a reference model, not a universal requirement. Organizations must adapt it to their actual business model, contracts, regulators, insurance program, vendor ecosystem, and governance structure. It does not substitute for review by qualified counsel, compliance, and risk advisors. Timing and legal obligations referenced in this appendix must be validated by counsel.

Required Elements

1. local stop authority
2. plant director independent activation authority
3. OT safety decision record
4. machine / cell / line restart protocol
5. part program and tool offset verification
6. quality record integrity review
7. shipped product / field conformance protocol
8. DFARS / CMMC / ITAR regulatory decision tracker
9. customer quality notification matrix
10. products liability / property BI coordination
11. plant-level production prioritization
12. board OT / production-safety oversight

OT Safety and Conformance Decision Record

Affected Plant	
Line/Cell/Machine	
Controller/PLC/SCADA/MES	
Suspected Cyber Trigger	
Operator Safety Risk	

Machine Behavior Observed	
Part Program/Tool Offset Status	
Safety Interlock Status	
Quality Record Status	
Parts Produced (Suspect Window)	
Parts Shipped (Suspect Window)	
Stop Decision	
Restart Decision	
Safety Verification Performed	
Quality Verification Performed	
Approved By	
Timestamp	
Next Review	

Machine / Cell / Line Restart Protocol

Before restart after a cyber-safety stop, the organization must document:

1. machine isolation confirmation
2. controller configuration verification
3. firmware or logic validation where applicable
4. part program checksum or version validation
5. tool offset verification
6. safety interlock test
7. remote diagnostics access review
8. MES / SCADA / PLC status validation
9. test part production
10. first-article inspection
11. quality sign-off

12. plant director sign-off
13. engineering / OT sign-off
14. residual risk statement
15. restart timestamp
16. post-restart monitoring period

PART SIX

Building and Deploying BIM

The Deliverables, the Implementation Process, and the Executive Value

CHAPTER 27

The BIM Deliverables

What Gets Built and What It Produces

A BIM engagement produces usable executive infrastructure. Not a document library. Not an abstract framework. Not a policy. A functional leadership operating model that activates when the event occurs.

The following twenty-seven deliverables define the standard BIM output. They are not all produced in the same sequence, and not every organization will require all twenty-seven at initial deployment. But the list defines the complete BIM infrastructure that mature organizations should work toward.

1. Business Incident Charter

The foundational BIM document. Defines the purpose, scope, authority structure, and activation rules for the organization's business incident response. Signed by the CEO and, where appropriate, the board. Establishes BIM as a recognized organizational function with executive authority.

2. Business Incident Classification Model

Defines the criteria by which security events are classified as business incidents and the severity levels that determine workstream activation scope. Separates technical severity from business consequence severity and defines the escalation thresholds for each.

3. Executive Decision Authority Matrix

Names the authorized decision-maker for each category of business decision during an incident. Defines alternates, authority limits, escalation triggers, and documentation requirements. The most operationally critical BIM deliverable.

4. Emergency Spending Authority

Defines spending limits by role and BIM level, emergency procurement waiver conditions, patient or customer safety exceptions, forensic evidence exceptions, insurer consent requirements, emergency spend documentation standards, reconciliation requirements, board reporting thresholds, and prohibited spending categories requiring elevated approval.

5. Workstream Ownership Document

Documents the nine executive workstreams with named owners, named alternates, activation triggers, specific responsibilities, escalation paths, and inter-workstream communication protocols.

6. Leadership Acknowledgment and Attestation Register

Captures written acknowledgment from every named executive, workstream owner, alternate, board member, and spending authority. Updated annually and after material organizational change.

7. Business Impact Thresholds

Maps specific event types to their potential operational, financial, customer, contractual, legal, insurance, regulatory, and board consequences. Used to quickly assess the likely business impact of a security event at the moment of activation.

8. Nine-Workstream Response Model

Documents the nine executive workstreams with named owners, named alternates, activation triggers, specific responsibilities, escalation paths, and inter-workstream communication protocols.

9. Insurance Readiness Review

Translates the active cyber insurance policy into an executable operational requirement: notice contacts, deadlines, approved vendors, consent requirements, sublimits, exclusions, and claim evidence standards.

10. Insurance Notice and Claim Evidence Protocol

Defines the insurance notice trigger, the notice process and recipients, the documentation required to support a claim, the financial tracking procedures that begin at activation, and the authority structure for claim decisions.

11. Legal and Privilege Protocol

Defines counsel engagement criteria and process, privilege structure, communication hygiene requirements, evidence handling protocols, and the authority structure for legal decisions during the incident.

12. Law Enforcement and Government Coordination Protocol

Defines who may contact law enforcement or government agencies, which agencies apply by scenario, what legal review is required before contact, what may be shared and under what conditions, and how the contact is documented.

13. Board Reporting Protocol

Defines board notification thresholds, communication structure, reporting cadence, content requirements, approval process, and the documentation requirements for the board oversight record.

14. Customer and Stakeholder Communication Framework

Defines communication thresholds, approval paths, message owners, pre-approved language templates, sequencing protocols, and spokesperson authorities for each stakeholder category.

15. Contract Notification Matrix

Maps key customer, vendor, partner, payer, business associate, DPA, SLA, MSA, government, and enterprise contract notice requirements, timelines, recipients, and evidence requirements.

16. Critical Third-Party Dependency Map

Identifies critical third parties, the business functions they support, data they access, incident contacts, notice obligations, and workarounds if the third party is unavailable or implicated.

17. Business-Critical Asset and Data Map

Identifies regulated data, customer data, patient data, employee data, payment data, intellectual property, source code, financial records, privileged identity systems, and operationally critical systems — with ownership, evidence location, and business impact of unavailability.

18. Evidence Preservation and Decision Log Standard

Defines what evidence must be preserved, who is responsible for preservation, how the decision log is maintained, under whose authority evidence can be modified or released, and how long evidence must be retained.

19. Open Action Register

Tracks all follow-on obligations generated by incident decisions, with owner, workstream, deadline, dependency, status, evidence, and escalation requirements.

20. Situation Report Cadence

Defines how often each workstream reports to Executive Command, what each report must contain, who receives it, and how it is documented. Adjusts based on incident velocity.

21. Communication Channel Control

Defines approved communication channels for operational coordination, privileged legal coordination, Executive Command, board updates, vendor communications, customer communications, and law enforcement or government coordination.

22. Employee Incident Communication Protocol

Defines who may communicate with employees during a BIM activation, what employees may be told, what channels may be used, what employees must not discuss externally, how manager guidance is issued, how employee questions are handled, and how all workforce communications are approved and preserved.

23. Single Source of Truth Protocol

Establishes the approved incident fact record, defines the fact owner, distinguishes known facts from confirmed unknowns, prohibits speculation in communications, and ensures all workstream communications align to the approved fact record.

24. Ransom and Extortion Governance Protocol

Defines who receives extortion communications, who may negotiate, insurer consent requirements, law enforcement coordination, sanctions screening, board approval requirements, payment authorization, and documentation standards.

25. Corrective Action Governance

Defines the post-incident finding and corrective action process, including finding documentation, corrective action assignment, budget authorization, executive sponsorship, board reporting, validation method, and closure evidence requirements.

26. Scenario Development Worksheets

Creates business response development worksheets for the organization’s highest-risk incident scenarios, addressing the specific BIM activation steps, workstream actions, and decision sequences for each scenario type.

27. BIM Validation and Exercise Plan

Defines the activation exercise cadence, exercise format, participant requirements, evaluation criteria, gap documentation process, remediation timelines, and re-attestation schedule.

28. Executive Quick-Start

A one-page first-30-minutes activation sheet that directs Executive Command and workstream owners through the immediate steps required after BIM activation.

29. BIM Activation Notice

The short-form message used to notify Executive Command and required workstream owners that BIM has activated, which channels to use, and what not to speculate about.

30. Initial Business Pressure Domain Screen

An activation-time screen of the eleven business pressure domains identifying whether each domain is active, unknown, or not active; who owns it; what decision is required; and what evidence must be preserved.

31. Evidence Package Index

An index organizing the Single Source of Truth by downstream use: legal, insurance, regulatory, board, operations, communications, customer impact, vendor, and corrective action.

32. Regulatory Notification Decision Tracker

A decision record documenting each potential regulatory notification obligation, trigger facts, clock start, deadline, owner, counsel review, decision, rationale, and evidence location.

33. Affected Individual / Customer Harm Tracker

A cross-sector tracker for direct harm or potential harm to individuals, customers, patients, account holders, clients, tenants, or other affected populations.

34. Multi-Policy Insurance Coordination Matrix

A matrix identifying every insurance policy potentially implicated by the event, including notice, consent, evidence, ownership, and coverage counsel coordination.

35. Board / Committee Incident Oversight Record

A formal oversight record documenting board or committee notification, materials provided, decisions requested, direction given, and follow-up required.

36. BIM-to-Regulated Program Interface Rule

A governance rule requiring BIM findings that affect regulated systems of record to be transferred into the appropriate compliance, quality, safety, supervisory, privacy, or operational remediation process.

CHAPTER 28

The BIM Facilitation Process

Why Building the Plan Requires More Than a Template

A BIM plan is built through facilitated executive decision-making.

Templates are useful. They help organize information. But templates do not resolve authority conflicts, validate insurance requirements, confirm vendor readiness, identify contract obligations, challenge assumptions, or make executives acknowledge their roles.

The BIM facilitation process exists to move the organization from awareness to operational readiness.

The facilitator's role is not to replace the organization's leaders, counsel, insurer, broker, CISO, CFO, board, or incident response vendors. The facilitator's role is to connect the decisions those parties must make together.

Why Facilitation Is Required

Most organizations already have many of the individual parts BIM depends on. They have a security team. They may have a cyber insurance policy. They may have outside counsel. They may have an incident response retainer. They may have a communications team. They may have a business continuity plan. They may have a board reporting process.

The problem is that those elements are usually not connected into one operating model.

The security team may know how to contain the threat, but not who can approve a containment action that disrupts revenue or operations. Legal may know how to advise on notification, but not whether the technical evidence required for that analysis will be available. The CFO may know the insurer must be notified, but not who owns the notice process at 2:00 a.m. Communications may know how to prepare a statement, but not who must approve it before release. The board may expect timely briefing, but no one has defined what threshold triggers that briefing.

BIM facilitation connects those decisions before the incident occurs.

The Ten Functions of BIM Facilitation

A proper BIM facilitation process should:

1. identify business consequence exposure;
2. map required decisions;
3. identify gaps between existing plans and actual authority;
4. validate insurance, vendor, and evidence requirements;
5. challenge assumptions about ownership;
6. surface unresolved conflicts;

7. document the operating model;
8. obtain leadership acknowledgment;
9. test the model through executive exercise;
10. convert findings into corrective action.

The Facilitation Standard

The purpose of BIM facilitation is not to produce a longer document. The purpose is to produce a more executable organization.

A facilitated BIM process should result in:

1. clear activation criteria;
2. named workstream owners;
3. documented decision authority;
4. approved emergency spending limits;
5. verified vendor readiness;
6. defined insurance notice process;
7. counsel engagement process;
8. board reporting thresholds;
9. communication approval workflow;
10. evidence and decision logging process;
11. stand-down authority;
12. corrective action governance;
13. leadership acknowledgment.

Without facilitation, organizations tend to produce plans that describe what should happen. With facilitation, they produce plans that named people have agreed to execute.

What Facilitation Does Not Replace

BIM facilitation does not replace legal advice, insurance brokerage, technical incident response, forensic investigation, crisis communications, executive leadership, or board oversight.

Instead, BIM facilitation creates the shared operating model those parties use to work together.

The facilitator helps leadership ask and answer the questions that are often left unresolved until the incident:

1. Who owns the business response?
2. Who can activate BIM?
3. Who can authorize emergency spending?
4. Who can engage counsel?

5. Who can engage DFIR?
6. Which vendors are approved?
7. Which vendors are insurer-approved?
8. Who notifies the insurer?
9. Who briefs the board?
10. Who approves communications?
11. Who contacts law enforcement?
12. Who preserves evidence?
13. Who tracks open actions?
14. Who decides when the business response can stand down?

Those questions cannot be left to assumption.

BIM facilitation turns them into documented, acknowledged, and tested decisions.

CHAPTER 29

The BIM Implementation Process

From Framework to Maintained Operating Model

Phase 1 — Readiness Assessment

The organization begins by assessing whether it has a business-response operating model or only a technical incident response plan.

This phase reviews existing plans, roles, policies, insurance materials, vendor lists, board reporting practices, communication protocols, and incident governance documents. The goal is not to criticize what exists. The goal is to identify what is missing from the business response model.

Key questions include:

1. Does the organization know when BIM activates?
2. Who owns Executive Command?
3. Who owns each workstream?
4. Who can make business-impact decisions?
5. Who can spend during the incident?
6. Who can engage counsel and vendors?
7. Who notifies the insurer?
8. Who briefs the board?
9. Who controls communications?
10. Who maintains the decision record?

Phase 2 — Organization-Specific Design

The organization then designs its BIM operating model around its actual business.

This phase translates the BIM framework into the organization's industry, revenue model, systems, customers, contracts, data, vendors, insurance policies, regulators, governance structure, and operational dependencies.

The output is not a generic plan. It is a company-specific operating model.

Phase 3 — Vendor, Insurance, and Authority Validation

The BIM plan should not be built on untested assumptions.

This phase validates the core assumptions the plan depends on, including insurance notice requirements, panel vendor requirements, breach counsel readiness, DFIR and recovery vendor status, non-panel vendor risk, emergency spending authority, board notification thresholds,

contract notice obligations, evidence availability, communication approval paths, and law enforcement or government coordination rules.

This phase determines whether the organization's intended response model can actually be executed.

Phase 4 — Executive Attestation

A role is not assigned until it is acknowledged.

This phase requires named leaders, alternates, workstream owners, spending approvers, board liaisons, communications approvers, insurance contacts, legal contacts, and escalation owners to acknowledge their assigned roles.

The acknowledgment should confirm that they understand their responsibilities, authority, limits, escalation obligations, documentation obligations, and any known gaps that would prevent execution.

Phase 5 — Activation Exercise

The organization tests the business event, not only the technical event.

The activation exercise should test BIM activation, Executive Command, workstream coordination, decision authority, emergency spending, insurer notice, vendor activation, board briefing, communications approval, evidence preservation, open action tracking, conflict resolution, and stand-down readiness.

The exercise should expose gaps before a real incident does.

Phase 6 — Remediation and Finalization

The findings from the activation exercise are converted into corrective actions.

This phase updates the BIM plan, closes unresolved authority gaps, corrects vendor readiness issues, updates communication workflows, refines board thresholds, clarifies insurance or counsel processes, and confirms that named leaders understand the final operating model.

The BIM plan should not be finalized until material exercise findings have either been resolved or accepted by leadership with documented risk acceptance.

Phase 7 — Maintenance and Re-Attestation

A BIM plan expires as the organization changes.

The plan should be reviewed at least annually and whenever there are material changes to leadership, board structure, insurance policies, vendors, contracts, systems, business model, critical data, regulatory obligations, incident response partners, or emergency spending authority.

Re-attestation should occur whenever named roles, decision authority, spending authority, or workstream ownership materially change.

BIM readiness is not a one-time project. It is a maintained operating model.

CHAPTER 30

BIM by Executive Role

What Business Impact Management Means for Each Leader

BIM is not an abstract organizational capability. It is a concrete benefit for every executive who will be accountable during a serious incident. The questions it answers are the questions each leader will be asked.

For the CEO

BIM gives the CEO a command model for the business response. When the security team reports a serious event, the CEO does not need to build the response from nothing. The activation is triggered, the workstreams are engaged, the decision authority is clear, and the CEO's role — integrating across workstreams, making the final calls on the highest-stakes decisions, ensuring the board and the organization are protected — is defined and executable.

The CEO's questions during a serious incident: Who is in charge? What gets escalated to me? What decisions require my approval? What does leadership need to know right now? What must be documented for later? BIM answers all of them.

For the CFO

BIM protects the CFO's financial response readiness. When is the insurer notified? What evidence does the claim require? What costs are being tracked? What revenue is at risk? What contractual penalties may apply? What uninsured exposure could emerge?

The CFO owns some of the most time-sensitive financial decisions in a serious incident. BIM ensures those decisions are prepared for in advance, with clear authority, defined processes, and documentation protocols that support insurance recovery and financial defensibility.

For the CISO

BIM gives the CISO a business escalation path that did not previously exist. When technical facts require executive action, BIM defines exactly what that escalation looks like: who to call, what to say, what authority exists, and what happens next.

BIM also removes from the CISO the burden of answering business questions they are not equipped to answer. Insurance decisions. Board communications. Customer notifications. Regulatory analysis. Those belong to the workstream owners BIM has defined. The CISO provides technical intelligence. BIM translates it into business action.

For the General Counsel

BIM creates defensibility for the General Counsel. Every significant legal question in a serious incident — when does privilege attach, who controls communications, what evidence must be preserved, how are notification decisions documented, what decision record will survive scrutiny — has been worked through in advance.

The GC does not enter a serious incident without a structure for managing legal exposure. They enter with pre-built protocols, defined authority, and documentation standards that position the organization for legal defensibility from the first hours.

For the COO

BIM connects cyber response to operational continuity for the COO. Which systems, plants, services, or functions are critical? Who can approve disruption? What fallback procedures activate? Who communicates with suppliers and customers? How do we restore business function safely?

Operational leaders rarely play a central role in security planning. BIM ensures they play a central role in business response — because when the incident creates operational consequences, the COO's decisions are among the most consequential the organization will make.

For the Board

BIM creates oversight clarity for the board. When must the board be informed? What should the board receive? How does management demonstrate readiness? How are material decisions governed? What record proves reasonable oversight?

Boards are increasingly scrutinized for their governance of cyber risk. BIM gives the board an answer to that scrutiny that is built into the organization's incident response infrastructure — not assembled retroactively.

For the Chief Risk Officer

BIM operationalizes cyber risk governance for the CRO. The risk register identifies the risk. BIM defines the response. The CRO's role in BIM is to ensure that the risk assessment, the insurance portfolio, and the BIM response infrastructure are aligned — and that the board risk committee has visibility into the readiness posture.

For the Chief Compliance Officer

BIM gives the CCO an executable regulatory response framework. Notification obligations, documentation requirements, examination readiness, and regulator inquiry response are all defined before the incident. The CCO's role is to own the regulatory workstream and ensure that compliance evidence is contemporaneous, organized, and defensible.

For the Privacy Officer

The Privacy Officer owns the notification analysis in any incident involving personal data. BIM defines the inputs they need, the timeline they must meet, the authority they have to make the notification determination, and the documentation standard their analysis must meet. For organizations in healthcare, financial services, or any sector subject to comprehensive privacy regulation, the Privacy Officer's BIM role is among the most time-sensitive in the incident.

For HR Leadership

HR's role in BIM covers employee data exposure, workforce communications, credential reset decisions, and — in insider event scenarios — employee investigation coordination with Legal. HR leadership must be named in the BIM plan, understand the activation criteria that trigger their workstream, and know when they operate independently versus when they operate under Legal's direction.

For the Board Chair and Risk Committee Chair

The board chair and risk committee chair are the governance anchors of BIM. They receive briefings under the Board Reporting Protocol, their questions become part of the oversight record, and their acknowledgment of board governance thresholds is part of the attestation register. BIM gives the board chair what they need to demonstrate that the board exercised appropriate oversight — the documentation of what they received, when, and what they did with it.

CHAPTER 31

BIM Readiness Maturity Model

Where Your Organization Stands and Where It Needs to Go

Readiness is not binary. Organizations move through maturity levels over time. BIM defines what each level looks like — and what it takes to advance.

Most organizations that begin a BIM assessment discover they are at Level 1 or Level 2. That discovery is not a failure. It is the starting point. The organizations that improve fastest are the ones that assess honestly, remediate specifically, and re-attest consistently.

Level	Status	Description
Level 1	Unowned	No defined business incident owner, activation criteria, spending authority, or evidence standard. The business response is improvised at the moment the incident occurs. No named workstream owners. No acknowledged authority. No insurance notice protocol. No board notification threshold.
Level 2	Informal	Leaders understand some of their responsibilities, but authority, documentation, and process are inconsistent. Some workstream ownership exists informally. Insurance and legal contacts are known but not documented. Board communication happens but without a defined protocol. Evidence preservation is ad hoc.
Level 3	Defined	Roles, activation triggers, authority, and protocols are documented. Named owners exist. Insurance requirements are mapped. Legal engagement criteria are defined. Board notification thresholds are agreed. Evidence preservation standards exist. The plan has not been tested.
Level 4	Tested	Workstream owners have exercised the model through a structured activation exercise. Gaps identified in the exercise have been documented and remediated. The plan reflects lessons from the exercise. Owners have re-attested after remediation.
Level 5	Defensible	BIM is maintained, tested, re-attested, and integrated into insurance, legal, board, and operational governance. Evidence of readiness exists. The model has been exercised across multiple scenarios. Corrective action governance is documented. Attestation is current. The organization can demonstrate readiness to insurers, regulators, and the board.

Moving Between Levels

Advancement from Level 1 to Level 2 requires naming owners and documenting basic contacts and processes. Advancement from Level 2 to Level 3 requires completing the BIM design

process and producing the core deliverables. Advancement from Level 3 to Level 4 requires conducting a structured activation exercise and remediating identified gaps. Advancement from Level 4 to Level 5 requires maintaining the model over time, integrating it into governance structures, and demonstrating readiness through evidence.

Most organizations can reach Level 3 within a single BIM engagement. Reaching Level 4 requires an activation exercise. Reaching and maintaining Level 5 requires organizational commitment over time.

What Maturity Level Is Sufficient?

The answer depends on the organization's risk profile, regulatory environment, and board expectations. Organizations in highly regulated sectors with significant customer data, complex insurance programs, and active board oversight of cyber risk should be working toward Level 4 or Level 5. Organizations with simpler risk profiles and lower regulatory exposure may reasonably target Level 3 as their near-term goal.

The question to ask is not "what is the minimum level required?" It is "what level would be defensible if this organization experienced a serious incident today?"

CHAPTER 32

What Readiness Looks Like

The Standard for Business Response Preparedness

The test of Business Impact Management is not whether the organization prevented the incident. It is whether leadership was ready for the business consequences when the incident arrived.

Most security frameworks measure readiness by the technical controls in place before an incident and the speed of technical response when one occurs. Those are meaningful measurements. They are not sufficient.

The organizations that perform best in serious incidents — that recover their insurance losses, navigate regulatory scrutiny without significant penalties, maintain customer relationships, emerge from board review with confidence intact, and rebuild trust without permanent reputational damage — do not necessarily have better security teams than those that struggle.

They have better business response readiness.

What Readiness Looks Like

Prepared leadership enters a serious incident with:

- A defined activation trigger and a named activation authority
- Executive Command named and authorized
- Workstream owners and alternates who know their roles and have acknowledged them in writing
- A CISO with authority to activate the business response
- Insurance notice requirements documented and assigned to a named person who has confirmed contacts
- Counsel engagement and communication protocols defined subject to counsel direction
- Board notification thresholds agreed with the board and briefing formats documented
- Customer and stakeholder communications with a legal review and approval path
- Regulatory notification analysis with a named owner and defined evidence inputs
- Financial impact tracking that begins at activation, not at claim submission
- Contract exposure review with a defined trigger
- Decisions logged contemporaneously from the first hour
- Evidence preservation that begins in the first hours under legal direction
- A single source of truth that all workstream communications align to
- An open action register that captures follow-on obligations from every decision
- The model tested through an executive activation exercise

- Gaps tracked, remediated, and re-attested

That is not an aspirational list. It is a buildable list. Every item on it can be designed, documented, tested, and deployed before the incident occurs.

The Success Standard

A BIM plan is ready only when the organization has defined activation, authority, emergency spending, insurance notice, legal escalation, law enforcement coordination, board reporting, stakeholder communication, contract notification, evidence preservation, workstream ownership, executive attestation, exercise cadence, and corrective action governance.

Owning a template is not readiness. Named leaders making, documenting, acknowledging, testing, and accepting the decisions required to manage the business consequences of a cyber incident — that is readiness.

The Work That Matters Most

The most important work in Business Impact Management happens before the incident. Not during it. Not after it.

The decisions that define how an organization's incident story ends — the insurance recovery outcome, the regulatory outcome, the legal exposure outcome, the board confidence outcome, the customer retention outcome — are shaped by preparation that happened weeks, months, or years before the event.

That is the Cybantage premise. That is the BIM premise. And it is provable. The organizations with the best outcomes after serious incidents are not the lucky ones. They are the prepared ones.

Business Impact Management does not prevent every incident. It prevents leadership from discovering its business response model during the incident.

Vendor Readiness Criteria

A BIM plan is not ready until its incident vendor ecosystem is ready.

The organization should be able to demonstrate that:

1. breach counsel is identified, conflict-checked, and engagement-ready;
2. alternate breach counsel is identified;
3. coverage counsel is identified where appropriate;
4. DFIR provider is contracted or otherwise engagement-ready;
5. DFIR insurer panel status has been verified;
6. recovery and restoration vendors are identified and contracted where required;
7. crisis communications support is approved;
8. notification and call center vendors are approved where applicable;

9. BAA or DPA requirements are satisfied where applicable;
10. eDiscovery and legal hold support is ready;
11. ransomware or extortion support activation requirements are defined;
12. sanctions or payment compliance review path is defined where applicable;
13. identity recovery and backup recovery vendors are identified where applicable;
14. cloud, SaaS, or OT recovery specialists are identified where applicable;
15. cyber insurer approved vendor panels have been verified;
16. non-panel vendor coverage-risk acknowledgment process is approved;
17. emergency spending authority is sufficient to activate vendors;
18. 24/7 vendor contacts are validated;
19. vendor activation has been tested during a BIM exercise.

A document can be completed by a writer. A BIM plan must be completed by the organization.

Vendor readiness is one of the clearest tests of whether the plan is real. If the organization cannot activate the required outside resources during the first hours of an incident, the plan is not ready.

First-Hour Readiness

A BIM-ready organization has not only assigned owners and built the plan. It has also equipped leadership with the first-hour artifacts needed to execute the plan under pressure.

Readiness now includes:

1. a first-30-minutes quick-start page
2. a tested BIM Activation Notice
3. an activation-time pressure domain screen
4. an Evidence Package Index
5. a Regulatory Notification Decision Tracker
6. an Affected Individual / Customer Harm Tracker
7. a Multi-Policy Insurance Coordination Matrix
8. a Board / Committee Incident Oversight Record
9. a defined interface between BIM corrective actions and regulated systems of record
10. sector-specific protocols for the organization’s actual business model

A BIM Plan is not mature because it describes what should happen. It is mature when leadership can open the plan in the first hour and know exactly what to do, what to preserve, who decides, who must be notified, and which downstream systems of record must receive the resulting corrective actions.

CHAPTER 33

Stand-Down, Post-Incident Review, and Corrective Action Governance

How BIM Closes the Incident and Builds on It

An incident is not over because the technical response is complete. BIM defines what must be resolved before the business response is closed.

The stand-down decision is among the most underappreciated governance moments in incident management. Standing down too early leaves unresolved obligations — insurance claims still open, regulatory responses still pending, customer commitments still unmet. Standing down with discipline ensures that nothing is dropped in the transition from active incident to post-incident management.

Stand-Down Authority

BIM may only be formally stood down by Executive Command after relevant workstreams confirm that no active business-response obligations remain unresolved. The stand-down is not declared by the security team when technical response is complete. It is declared by Executive Command when all workstream leads have confirmed their obligations are resolved or transitioned.

The stand-down checklist must confirm the status of:

- Technical response — confirmed complete and documented
- Legal status — privilege matters resolved or transitioned to post-incident counsel
- Insurance status — claim filed, documentation submitted, or open items assigned
- Regulatory status — notifications complete or ongoing obligations identified and assigned
- Customer communication status — all required communications made, follow-up tracked
- Board status — final briefing delivered, oversight record complete
- Evidence status — preservation confirmed, legal holds in place
- Financial tracking status — business interruption documentation complete for claims
- Open action register — all items resolved or transitioned with named owner
- Corrective action plan — findings documented, owners named, timeline established
- Post-incident review date — scheduled and confirmed

The Post-Incident Review

Every Level 2 or higher BIM incident should produce a structured post-incident review. The review is not a blame exercise. It is a system improvement exercise. Its purpose is to identify

what the BIM operating model did well, what it did poorly, and what changes are required to improve performance in future incidents.

The post-incident review should be led by a facilitator outside the workstream that experienced the most significant gaps — to ensure objectivity. It should include input from every workstream owner. And it should produce a corrective action plan with specific findings, named owners, timelines, and validation methods.

Corrective Action Governance

Every Level 2 or higher BIM incident should produce corrective actions tracked against the following standard. For each finding, the corrective action governance record must capture:

- Finding — what failed or was absent
- Corrective action — the specific change required
- Accountable owner — the named individual responsible for execution
- Budget requirement — any resources required
- Due date — the committed completion date
- Executive sponsor — the leader accountable for the owner's execution
- Board reporting status — whether the finding and corrective action have been reported to the board
- Validation method — how completion will be confirmed
- Closure evidence — the documentation that proves the corrective action was completed

See Addendum W for the Corrective Action Governance Tracker.

Vendor Performance and Readiness Review

Post-incident review should include the performance and readiness of all pre-approved incident vendors.

The organization should determine:

1. Did pre-approved vendors activate on time?
2. Were contracts, retainers, and emergency activation paths sufficient?
3. Was carrier consent required, obtained, delayed, or unavailable?
4. Did any non-panel vendors create claim friction?
5. Did vendor invoices contain sufficient detail to support insurance recovery?
6. Did vendor communications preserve legal, insurance, regulatory, and evidence requirements?
7. Did counsel-directed work remain properly structured?
8. Did DFIR preserve the evidence needed for legal, insurance, regulatory, and board review?

9. Did recovery vendors support restoration within expected timeframes?
10. Did crisis communications, notification, call center, or customer response vendors perform as expected?
11. Were BAA, DPA, confidentiality, or data handling obligations satisfied?
12. Should additional vendors be pre-approved?
13. Should any vendor be replaced?
14. Should any vendor contract, retainer, panel status, or activation process be updated?

Vendor performance findings should be entered into the corrective action governance tracker.

A vendor failure during an incident is not merely a procurement issue. It may affect legal defensibility, insurance recovery, customer trust, operational continuity, and board confidence.

Corrective action governance is not a bureaucratic exercise. It is the mechanism by which BIM improves over time. Organizations that track, complete, and validate corrective actions from serious incidents consistently outperform those that document findings and allow them to age without resolution.

CHAPTER 34

Common Failed DIY Patterns

Why Cyber Business-Response Plans Fail Internally

Many organizations try to build cyber business-response plans internally. Some succeed. Many do not.

The reason is usually not lack of intelligence, effort, or commitment. It is that the plan is treated as a writing exercise instead of a cross-functional decision process.

A cyber business-response plan fails when it describes what should happen but does not prove that the organization has made, assigned, acknowledged, validated, and tested the decisions required to make it happen.

Pattern 1 — The Plan Is Written by One Function

A plan written by one department reflects that department's view of the incident.

Security may focus on containment and recovery. Legal may focus on privilege and notification. Finance may focus on insurance and loss tracking. Communications may focus on messaging. Operations may focus on continuity.

BIM requires all of those views, but it cannot be owned by any one of them alone.

When one function writes the plan, the seams between functions remain unresolved.

Pattern 2 — Roles Are Named Without Acknowledgment

Many plans assign responsibility to titles: CFO, General Counsel, CISO, COO, Communications Lead, Board Chair.

That is not enough.

A role is not assigned until the named person has acknowledged it. The individual must understand when the role activates, what authority it carries, what limits apply, what documentation is required, what must be escalated, and what dependencies could prevent execution.

Unacknowledged responsibility is assumed responsibility. Assumed responsibility fails under pressure.

Pattern 3 — Authority Is Assumed Instead of Approved

Incident plans often say who "will" make decisions without confirming who is authorized to make them.

Who can shut down a revenue-producing system? Who can authorize emergency spending? Who can engage outside counsel? Who can approve a customer statement? Who can contact law enforcement? Who can brief the board?

If the authority was not approved before the incident, it will be questioned during the incident.

Pattern 4 — Insurance Requirements Are Treated as Background

Many organizations own cyber insurance but do not translate the policy into incident operating requirements.

Notice timing, approved vendors, consent requirements, panel counsel, proof-of-loss documentation, cooperation obligations, sublimits, exclusions, and application representations all matter during the incident.

Insurance cannot remain a policy in a drawer. It must become an executable workstream.

Pattern 5 — Vendors Are Listed but Not Ready

A vendor name in a plan is not the same as vendor readiness.

The organization must know whether the vendor is contracted, conflict-cleared, insurer-approved, available after hours, authorized for activation, covered by emergency spending authority, and subject to any data handling or confidentiality requirements.

If those details are missing, the vendor is not ready.

Pattern 6 — Contracts Are Reviewed During the Incident

Customer, vendor, payer, partner, government, BAA, DPA, MSA, SLA, and enterprise agreements may contain cyber-related notice, cooperation, audit, indemnity, service-level, or security incident obligations.

Reviewing those contracts for the first time during the incident creates delay and risk.

BIM requires contract notification mapping before the incident.

Pattern 7 — The Board Is Briefed but Not Integrated

Some organizations assume the board only needs to be updated after management has answers.

That assumption can create governance risk.

The BIM plan must define board notification thresholds, briefing cadence, information format, escalation triggers, and the roles of the CEO, General Counsel, CFO, corporate secretary, board chair, and risk committee.

The board does not manage the incident. But it must be integrated into the governance model.

Pattern 8 — The Plan Is Never Exercised

A plan that has not been exercised is a theory.

The exercise should not test only the technical response. It should test BIM activation, Executive Command, insurer notice, vendor activation, emergency spending, board briefing, communications approval, evidence preservation, conflict resolution, and stand-down.

The purpose of the exercise is not to prove readiness. It is to find the places where readiness is assumed.

Pattern 9 — Emergency Spending Is Undefined

During a cyber incident, leadership may need to authorize counsel, forensics, recovery vendors, notification vendors, call center support, crisis communications, identity protection, business continuity resources, and other emergency expenses.

Decision authority without spending authority is incomplete.

If the organization has not defined who can spend, how much they can authorize, when insurer consent is required, and how spending is documented, the response will slow at the exact moment speed matters.

Pattern 10 — The Fact Record Fragments Across Teams

During an incident, facts move quickly and incompletely.

If each workstream maintains its own version of the truth, leadership will make decisions from conflicting information. Legal may have one timeline. Security may have another. Communications may be working from an outdated statement. The board may receive a briefing based on facts that have changed.

BIM requires a single source of truth, situation report cadence, decision log, and open action register.

Pattern 11 — Law Enforcement Contact Is Improvised

Law enforcement or government coordination may be appropriate in ransomware, extortion, fraud, critical infrastructure disruption, insider misconduct, or significant threat actor activity.

But contact with authorities affects legal strategy, insurance recovery, communications, evidence handling, and board oversight.

The BIM plan must define who may contact authorities, which agencies may be relevant, what information may be shared, how counsel is involved, and how the contact is documented.

Pattern 12 — Corrective Actions Are Documented but Not Governed

Many post-incident reviews produce findings. Fewer ensure that the findings are closed.

Corrective actions require owners, deadlines, executive visibility, board reporting where appropriate, validation, and re-testing.

A corrective action that is merely documented is not governed.

Why These Failures Matter

These are not writing failures. They are implementation failures.

The organization may have a plan, but the plan has not forced the organization to make the decisions that matter. BIM exists to close that gap.

A BIM plan should not merely describe how the organization hopes to respond. It should document what named leaders have decided, acknowledged, tested, and agreed to maintain.

CHAPTER 35

The BIM Implementation Decision

What Leadership Must Decide After Reading This Guide

Understanding BIM is not the same as implementing BIM.

This guide gives leadership the framework. The organization must still decide whether it will build the operating model, validate the assumptions, assign the owners, obtain acknowledgment, test the response, and maintain the plan.

After reading this guide, leadership has three choices.

Option 1 — Do Nothing

The organization can continue relying on its existing technical incident response plan, cyber insurance policy, outside counsel, vendors, business continuity plan, communications process, and executive judgment to converge during the incident.

That may work for minor events. It may not work when the incident creates simultaneous legal, insurance, regulatory, customer, operational, financial, contractual, board, communications, workforce, and evidence pressures.

Doing nothing is still a decision. It means leadership has accepted that the business response will be assembled during the incident.

Option 2 — Build Internally

The organization can use the BIM framework to build its own organization-specific plan.

This requires more than assigning someone to complete a template. Internal BIM implementation requires executive facilitation, cross-functional decision sessions, insurance review, vendor validation, contract review, board threshold design, authority approval, legal review, communications design, evidence planning, leadership acknowledgment, and exercise validation.

An internal build can succeed if the organization has the time, discipline, authority, and cross-functional participation to complete that process.

The risk is that internal builds often stop at documentation. They produce a plan, but not the decisions required to execute it.

Option 3 — Build With Guided Facilitation

The organization can use the BIM framework with guided facilitation to drive the decision process.

Guided facilitation helps leadership identify required decisions, challenge assumptions, resolve ownership gaps, validate insurance and vendor dependencies, document the operating model, obtain acknowledgment from named leaders, and test the plan through an executive exercise.

The facilitator does not replace management, counsel, the insurer, the broker, the CISO, the board, or incident response vendors. The facilitator helps those parties operate from a single business-response model before the incident occurs.

Guided facilitation is appropriate when the organization recognizes that the issue is not merely the absence of a document. It is the absence of pre-made, pre-approved, cross-functional business decisions.

The Decision Leadership Must Make

The important decision is not whether the organization understands BIM.

The important decision is whether the organization is prepared to build it, validate it, and execute it before the incident happens.

A BIM plan is not ready because the document is complete. It is ready when named leaders can demonstrate that they know when BIM activates, what they own, what they can decide, what they can spend, who they must involve, which vendors are approved, what the insurer requires, what the board receives, what can be communicated, what evidence must be preserved, what actions remain open, and when the business response can be stood down.

ADDENDA

BIM Artifacts and Reference Templates

ADDENDUM A

BIM Leadership Acknowledgment and Attestation

Complete for every named BIM role owner. Retain as part of the BIM governance record. Update annually or after material change.

Organization name	
Incident response plan version	
Attestation date	
Acknowledging individual — name	
Acknowledging individual — title	
BIM role assigned	
Workstream assigned	
Alternate for (if applicable)	
I have reviewed the BIM plan and understand my assigned role	
I understand my activation criteria — when my workstream activates	
I understand my authority and its defined limits	
I understand what must be escalated and to whom	
I understand my documentation and evidence obligations	
I understand my communication channel requirements	
I have identified gaps, conflicts, or resource constraints (describe or None)	
Emergency spending authority level (if applicable)	
Board notification role (if applicable)	
Signature	
Date signed	
Annual re-attestation due date	

Attestation Register Summary

Role / Workstream	Named Owner	Alternate	Date Attested	Re-Attestation Due
Executive Command				
Security and Technical Response				
Legal and Privilege				
Insurance and Claims				
Regulatory and Compliance				
Operations and Continuity				
Customer, Partner, and Vendor				
Communications				
Board and Governance				
Board Chair / Risk Committee Chair				
Emergency Spending Authority				

ADDENDUM B

Security-to-Business Activation Brief

Used by the CISO or technical lead to brief Executive Command at BIM activation. Complete with available information. Update as facts develop. This brief does not require complete information. It requires organized information.

Incident detection date and time	
Brief description of what occurred	
Systems affected (known)	
Users or accounts affected (known)	
Data potentially involved	
Regulated data potentially involved (PHI, PII, financial, CUI)?	
Containment actions underway	
Current scope — known facts	
Current scope — confirmed unknowns	
Potential business consequences that may be triggered	
Insurance notice evaluation required?	
Board notification threshold potentially met?	
Regulatory notification analysis required?	
Decisions needed in the next 30 minutes	
Decisions needed in the next 60 minutes	
Decisions needed in the next 120 minutes	
Technical team point of contact	
Brief prepared by	
Brief delivered at (date/time)	
Next update scheduled	

ADDENDUM C

Emergency Spending Authority

Defines spending limits during a BIM-activated incident. Confirm with insurer consent requirements before authorizing significant expenditures. Document all emergency spending contemporaneously.

Role	Spending Authority Limit	Requires Insurer Consent?	Requires Executive Approval?
Workstream Owner (standard)	[Define per organization]	Check policy	[Define per organization]
Executive Command	[Define per organization]	Check policy	No (within limit)
CFO / Risk Manager	[Define per organization]	Check policy	No (within limit)
CEO	[Define per organization]	Check policy	No
Patient / Safety Exception	As required for safety	Check policy	CEO or COO
Forensic Evidence Exception	As required by counsel	Confirm with carrier	GC + CFO

Emergency spend log — expenditure #	
Date and time authorized	
Authorized by (name and title)	
Vendor or recipient	
Amount	
Purpose	
Insurer consent obtained?	
Invoice / documentation reference	
Reconciliation status	

All emergency expenditures must be reconciled and reported to the CFO within [define] business days of incident stand-down. Expenditures above board reporting thresholds must be included in the board post-incident briefing.

ADDENDUM D

Law Enforcement and Government Coordination Protocol

Defines who may contact law enforcement or government agencies, under what authorization, and how that contact is documented. Coordination must be approved by Executive Command and Legal before initiation.

Agency	Scenario Type	Authorized Contact	Legal Review Required?	Insurance Notice Required?
Local Police	Physical crime, initial report	[Define per organization]	Recommended	Confirm with carrier
FBI Cyber Division	Ransomware, data breach, espionage	GC + Executive Command	Yes	Confirm with carrier
U.S. Secret Service	Financial fraud, BEC, wire fraud	GC + Executive Command	Yes	Confirm with carrier
IC3 (FBI)	Internet crime reporting	GC + Executive Command	Yes	Confirm with carrier
CISA	Critical infrastructure, reportable incidents	GC + Executive Command	Yes	Confirm with carrier
State AG / Regulator	Breach notification, inquiry	GC	Yes	Confirm with carrier
Sector Regulator	Sector-specific reporting	GC + Compliance	Yes	Confirm with carrier

Law enforcement contact log — entry #	
Date and time of contact	
Agency contacted	
Contact name and badge / agent ID	
Method of contact (phone, in person, portal)	
Authorized by	
Legal review completed by	
Information shared (describe or reference document)	
Information not shared / withheld	
Next contact scheduled	

Follow-on obligations created	

ADDENDUM E

Emergency Identity and Access Authority

Defines who may authorize emergency identity and access actions during a BIM-activated incident. Actions must be documented contemporaneously and aligned with evidence preservation requirements.

Action	Authorization Required From	Business Impact Notification Required?	Documentation Requirement
Enterprise password reset (all users)	Executive Command + CISO	Yes — HR + COO	Decision log entry
MFA reset (targeted accounts)	CISO + Legal review	Case dependent	Decision log entry
Token / API key revocation	CISO + workstream owner	Customer impact check	Decision log entry
Remote access suspension	CISO + COO	Operational impact check	Decision log entry
Privileged account suspension	Executive Command + GC	Yes	Decision log entry
Vendor / partner access suspension	COO + GC + customer workstream	Yes — vendor notification	Decision log entry
Customer admin account suspension	Executive Command + GC	Yes — customer notification	Decision log entry
Service account restriction	CISO + COO	Operational impact check	Decision log entry

ADDENDUM F

Conflict Resolution Protocol

Defines how Executive Command resolves disputes between workstreams during a BIM-activated incident.

Resolution Process

Step 1: The conflicting workstream owners identify the disagreement and escalate to Executive Command.

Step 2: Executive Command convenes a brief joint briefing from both workstream owners, limited to available facts and options.

Step 3: If the conflict involves legal, regulatory, privilege, sanctions, law enforcement, notification, or insurance exposure, General Counsel must be consulted before the final decision.

Step 4: If the conflict affects patient safety, employee safety, physical safety, or operational safety, the relevant safety or operations owner's recommendation must be formally considered and documented.

Step 5: Executive Command makes the decision, documents the rationale in the decision log, and notifies all affected workstream owners.

Step 6: The resolution is final unless new information materially changes the situation.

Conflict log — entry #	
Date and time of conflict	
Workstreams in conflict	
Nature of disagreement	
Legal, regulatory, or safety implications?	
GC consulted? (date and time)	
Decision made by	
Decision made at (date and time)	
Decision and rationale	
Decision log entry number	
Workstream owners notified	

ADDENDUM G

Cyber Insurance Readiness Review

Complete before the incident. Update annually or upon policy renewal. This document translates the insurance policy into an operational requirement.

Policy number	
Policy period	
Carrier name	
Carrier claims contact — name, phone, email	
Broker name and contact	
Coverage counsel (if pre-identified)	
Notice requirement — timeframe from discovery	
Notice requirement — recipients (carrier, broker, or both)	
Notice requirement — method (portal, email, phone)	
Approved forensic vendor panel (list or None)	
Approved breach counsel panel (list or None)	
Insurer consent required for forensic vendor engagement?	
Insurer consent required for legal engagement above threshold?	
Consent threshold for pre-approved vs. panel vendors	
Cyber policy sublimit — ransomware / extortion	
Cyber policy sublimit — business interruption	
Cyber policy sublimit — regulatory fines and penalties	
Cyber policy sublimit — notification and credit monitoring	
Retention / deductible amount	

Key exclusions relevant to this organization	
Proof-of-loss requirements and deadline	
Business interruption evidence requirements	
Cooperation obligations during investigation	
Application representation evidence location	
Claim communication protocol (what can be said and to whom without carrier approval)	

ADDENDUM H

Insurance Notice and Claim Evidence Tracker

Initiate at BIM activation. Track all insurance-related actions contemporaneously. This tracker supports claim submission and carrier cooperation obligations.

Policy number	
Policy period	
Carrier name	
Carrier claims contact	
Broker name and contact	
Notice sent date and time	
Notice sent to (carrier and/or broker)	
Notice method (portal / email / phone)	
Claim number assigned	
Coverage counsel engaged? (name and date)	
Carrier instructions received (summarize)	
Approved forensic vendor engaged?	
Approved breach counsel engaged?	
Financial impact tracking initiated? (date)	
Business interruption claim evidence — start date	
Business interruption claim evidence — end date	
Emergency expenditures tracker reference	
Vendor invoices for covered services	
Forensic report reference	
Proof-of-loss submission date	
Claim status	

Next required action and deadline	

ADDENDUM I

Insider and Internal Investigation Protocol

Use when a cyber incident may involve insider conduct, employee misuse, contractor activity, privileged account abuse, or internal misconduct. Legal must control the investigation from the outset.

Protocol Sequence

Step 1: Security or technical workstream identifies potential insider indicators. Report immediately to Executive Command and General Counsel. Do not contact the subject employee.

Step 2: General Counsel takes control of the investigation. HR is engaged only under legal direction. No direct employee communication about the investigation without GC approval.

Step 3: Evidence is preserved under legal hold before any account is accessed, modified, or suspended. GC directs evidence preservation scope.

Step 4: Access suspension decision is made by GC with Executive Command authorization. HR is notified of the suspension action simultaneously with execution.

Step 5: Employee interviews, if required, are conducted under GC direction. HR may be present at GC's discretion. No unsanctioned informal conversations about the investigation.

Step 6: Law enforcement referral is evaluated by GC and Executive Command. No law enforcement contact without GC authorization.

Investigation log — entry #	
Date investigation opened	
Subject employee (reference number, not name in this log)	
Nature of suspected conduct	
GC engagement date and time	
HR engagement date and time	
Evidence preserved — description and location	
Legal hold issued by and to whom	
Access suspension date and time (if applicable)	
Employee communication (if any) — approved by GC?	
Law enforcement consideration status	

Investigation status	

ADDENDUM J

Regulator Inquiry Response Protocol

Defines how the organization receives, processes, and responds to regulatory inquiries following a cyber incident. All responses must be approved by counsel before submission.

Inquiry Response Process

Step 1: All regulatory inquiries — written or oral, from any regulatory body — are directed immediately to General Counsel. No individual workstream owner may respond to a regulatory inquiry without GC authorization.

Step 2: GC logs the inquiry and establishes a deadline tracking entry. Deadlines are non-negotiable unless GC obtains an extension.

Step 3: GC assigns a response owner and assembles the required evidence from the relevant workstreams.

Step 4: Response draft is prepared by or under direction of GC. Response is reviewed by Executive Command if the inquiry is significant.

Step 5: Response is submitted by GC or under GC's direction. No response is submitted without GC final approval.

Inquiry log — entry #	
Date inquiry received	
Regulatory body	
Inquiry type (written / oral / examination)	
Subject matter of inquiry	
Response deadline	
Extension requested? (date and outcome)	
Response owner assigned	
Evidence required — description and source	
Draft response prepared by	
GC review completed	
Executive Command review required?	
Response submitted date and method	

Remediation commitments made (if any)	
Follow-on obligations	

ADDENDUM K

Board Incident Briefing Template

Complete under legal review before each board briefing. Maintain a copy in the board oversight record. Update with each subsequent briefing. This template produces the board's oversight record.

Briefing number and date	
Briefing method (call / email / meeting)	
Board members briefed	
Incident summary	
Known facts as of this briefing	
Unknown facts as of this briefing	
Customer or patient impact	
Operational status	
Financial exposure estimate	
Insurance status	
Legal status and privilege notes	
Regulatory and compliance status	
Decisions made since last briefing	
Decisions pending	
Materiality assessment status	
Board questions and management responses	
Next update scheduled	
Briefing prepared by	
Legal review confirmed by	
Date legal review completed	

ADDENDUM L

Customer and Stakeholder Communication Approval Record

Complete for every external communication during the incident. Retain as part of the Evidence and Defensibility record. No external communication may be distributed without the required approvals.

Communication number	
Date and time prepared	
Audience (customers / patients / partners / media / employees / other)	
Communication method (email / portal / press release / direct call / other)	
Message owner (name and title)	
Draft prepared by	
Legal reviewer (name)	
Legal review completed (date/time)	
Final approved language (or document reference)	
Approved by (name and title)	
Approval date and time	
Distribution date and time	
Distribution channel	
Estimated recipients	
Account-managed outreach required? (list accounts)	
Follow-up obligations triggered	
Next communication planned	

ADDENDUM M

Status Page and Trust Center Protocol

For SaaS, MedTech, FinTech, technology-enabled healthcare, and platform businesses. Status page and trust center updates are external communications and require legal review and approval.

Status page owner (name and title)	
Status page update authorization threshold	
Status page legal review requirement	
Trust center owner (name and title)	
Trust center update authorization threshold	
Trust center legal review requirement	
Customer security team notification process	
Threshold for customer security team notification	
SOC 2 / HITRUST / security certification representation — relevant controls	
Approved language for initial availability incident (pre-approved template)	
Approved language for security incident (pre-approved template)	
Approved language for data incident (pre-approved template)	
Escalation if status page owner is unavailable	

Status Page Update Log

Update #	Date/Time	Update Content Summary	Approved By	Legal Reviewed?

ADDENDUM N

Contract Notification Matrix

Complete before the incident. Identify key contracts with cyber notification requirements. Update annually or when significant contracts change.

Customer / Vendor / Partner	Contract Type	Notice Trigger	Notice Deadline	Notice Recipient	Owner	Legal Review?	Evidence Needed
	Enterprise MSA					Yes	
	DPA / BAA					Yes	
	Government Contract					Yes	
	SLA Agreement					Yes	
	Partner Agreement					Yes	

ADDENDUM O

Critical Third-Party Dependency Map

Complete before the incident. Identify critical vendors and their business function, data access, incident contacts, notice obligations, and available workarounds.

Vendor / Provider	Service / Function	Data Access	Incident Contact	Notice Obligation	Workaround / Alternative
	Cloud Infrastructure				
	MSP / MSSP				
	Payment Processor				
	Identity Provider				
	EHR / Core Business System				
	Clearinghouse				
	Payroll / HR System				
	Critical Supplier				

ADDENDUM P

Business-Critical Asset and Data Map

Complete before the incident. Used at BIM activation to assess potential business consequence of technical events.

System / Data Type	Business Function	Data Sensitivity	Regulatory / Contract Relevance	Impact if Unavailable	Owner	Evidence Location
	Revenue-critical					
	Customer-facing					
	Clinical / Patient					
	Financial records					
	Employee data					
	Intellectual property					
	Identity / Access					

ADDENDUM Q

Single Source of Truth Protocol

Maintains the approved incident fact record. All workstream communications must align to this record. Updated by the fact owner as new information is confirmed.

Incident reference number	
Fact owner (name and title)	
Record version and update time	
Known facts — confirmed and approved	
Confirmed unknowns (what is not yet known)	
Prohibited speculation (what must not be asserted)	
Approved incident description (short form)	
Approved incident description (long form for board and regulatory use)	
Approved customer-facing language	
Approved employee-facing language	
Approved media-facing language (if applicable)	
Most recent communications distributed — reference	
Next approved update expected at	
Fact owner approval signature and date	

ADDENDUM R

Incident Communication Channel Control

Defines approved communication channels during a BIM-activated incident. Using unauthorized channels creates privilege exposure, records management failures, and evidentiary problems.

Communication Type	Approved Channel	Records Retention	Who Has Access
Operational coordination	[Define per organization]	Standard retention	Workstream owners
Privileged legal coordination	[Counsel-directed channel only]	Legal hold	GC, counsel, named parties
Executive Command coordination	[Define per organization]	Incident archive	Executive Command only
Board updates	[Secure board channel]	Board oversight record	Board members + GC
Vendor communications	[Define per organization]	Standard retention	Vendor management workstream
Customer communications	[Approved platform only]	Customer record	Customer workstream + GC
Law enforcement coordination	[In-person or GC-directed]	Legal hold	GC + authorized contact
Insurance coordination	[Coverage counsel directed]	Claims file	CFO + coverage counsel

ADDENDUM S

Employee Incident Communication Protocol

Defines who may communicate with employees during a BIM activation, what employees may be told, what channels may be used, what employees must not discuss externally, how manager guidance is issued, how employee questions are handled, and how all workforce communications are approved and preserved.

Employee communication owner (name and title)	
Legal approver (name)	
HR approver (name and title)	
Communications approver (name and title)	
Executive Command approval threshold	

Approved communication channels	
Alternate communication channels (if primary unavailable)	
Employee message templates — location/reference	
Manager briefing template — location/reference	
Employee FAQ process owner	
Customer-facing employee instructions — owner	
Social media and public discussion restrictions — acknowledged by workforce?	
Employee question intake path	
Evidence preservation requirements — owner	
Stand-down communication template — location/reference	
Annual review and exercise requirement — last completed	

ADDENDUM T

Open Action Register

Updated at every Executive Command update cycle. The decision log records decisions made. The open action register tracks obligations those decisions created.

Action #	Action Item	Owner	Workstream	Deadline	Dependency	Status	Evidence	Escalation?
						Open		
						Open		
						Open		
						Open		
						Open		

ADDENDUM U

BIM Situation Report Template and Cadence

Defines the reporting rhythm for Executive Command during a BIM-activated incident. Cadence adjusts by incident velocity. Faster in the first hours; slower as the situation stabilizes.

Incident Phase	Recommended Cadence	Format	Distribution
First 4 hours	Every 30–60 minutes	Verbal brief + written summary	Executive Command + GC
Hours 4–24	Every 2–4 hours	Written situation report	All workstream owners
Days 2–7	Twice daily	Written situation report	All workstream owners + board liaison
Day 7+	Daily or as warranted	Written situation report	All workstream owners + board
Post-active phase	Weekly	Status update	Executive Command + GC

Situation Report Format

Situation report number and date/time	
BIM activation level	
Incident summary (current)	
Known facts (updated)	
Confirmed unknowns (updated)	
Business impact (current estimate)	
Customer / patient impact	
Decisions made since last report	
Decisions pending	
Legal and regulatory status	
Insurance status	
Communications status	
Financial exposure (current estimate)	
Open action register — items added since last report	

Open action register — items closed since last report	
Next update scheduled	
Report prepared by	

ADDENDUM V

Ransom and Extortion Governance Protocol

No individual executive may independently authorize, initiate, negotiate, or facilitate ransom or extortion payment. This protocol governs every ransom and extortion decision from first contact through resolution.

Governance Sequence

Step 1: All extortion communications are reported immediately to Executive Command and General Counsel. No individual who receives extortion communication may respond without authorization.

Step 2: GC evaluates legal implications including sanctions, law enforcement obligations, and insurance requirements. No response or payment decision may proceed before this evaluation.

Step 3: Cyber insurer is notified per the Insurance Notice and Claim Evidence Tracker (Addendum H). Insurer consent requirements for negotiation and payment are confirmed.

Step 4: Law enforcement coordination decision is made per the Law Enforcement and Government Coordination Protocol (Addendum D). OFAC/sanctions screening is completed by GC or external counsel.

Step 5: Board is briefed per the Board Reporting Protocol. Board authorization is obtained if required by the BIM plan or insurance policy.

Step 6: Executive Command makes the payment decision or rejection decision with GC concurrence. Decision and full rationale are documented in the decision log.

Step 7: If payment is authorized: cryptocurrency controls apply, payment is made by authorized party only, transaction is documented in full, and GC confirms compliance with legal requirements.

Step 8: All decisions — including rejection of ransom demand — are documented in the decision log.

Extortion communication received — date/time	
Extortion communication received by	
Executive Command notified — date/time	
GC notified — date/time	
Insurer notified — date/time	
Pre-approved negotiator engaged? (name)	
Insurer consent status	

Law enforcement coordination decision	
OFAC / sanctions screening completed by	
OFAC / sanctions screening result	
Board briefed — date/time	
Board authorization obtained?	
Payment decision (Pay / Decline / Pending)	
Payment decision made by	
Payment decision date/time	
Payment amount (if applicable)	
Cryptocurrency wallet / transaction reference (if applicable)	
Payment authorized by (legal confirmation)	
Decision log entry number	
Post-payment decryption / restoration outcome	

ADDENDUM W

Corrective Action Governance Tracker

Complete for every Level 2 or higher BIM incident post-incident review. Track findings through closure. Board reporting status must be confirmed for significant findings.

Finding #	
Finding Description	
Corrective	
Action	
Owner	
Budget	
Required	
Due Date	
Executive Sponsor	
Validation Method	
Board Reported?	
Closure Evidence	

ADDENDUM X

Annual BIM Validation and Re-Attestation Checklist

Complete annually or after material organizational change. All items must be confirmed before re-attestation is declared complete.

Step	Action	Owner	Completed
1	Confirm all workstream owners are still in role and available	Executive Command	
2	Confirm all alternates are named and current	Executive Command	
3	Validate all contact information for owners, alternates, counsel, carriers, and brokers	All workstream owners	
4	Conduct insurance notice drill — simulate first-hour notice process	CFO + Risk Manager	
5	Conduct board briefing simulation — verify notification threshold and format	GC + Board Liaison	
6	Test emergency spending authority chain — confirm limits and insurer consent requirements	CFO + Executive Command	
7	Review law enforcement coordination protocol — confirm contacts and authorization	GC	
8	Test evidence preservation protocol — confirm legal hold process is understood	GC + Evidence Owner	
9	Test communications approval drill — simulate first customer communication approval	Communications + GC	
10	Review regulatory notification obligations for any changes in law or regulation	Compliance + GC	
11	Review contract notification matrix for new or changed contracts	Legal + Contracting	
12	Review third-party dependency map for new or changed critical vendors	Operations + IT	
13	Review business-critical asset and data map for material changes	IT + Compliance	
14	Update all BIM plan documents for any changes identified in items above	BIM Plan Owner	
15	Collect updated acknowledgment and attestation from all named owners	Executive Command	
16	Document re-attestation completion in the Leadership Attestation Register (Addendum A)	Executive Command	
17	Schedule next activation exercise and confirm participants	Executive Command	

ADDENDUM Y

Pre-Approved Incident Vendor and Retainer Register

This addendum documents the outside vendors, advisors, counsel, and support providers that the organization may need during a BIM activation. It confirms whether those resources are contracted, approved, insurer-aligned, assigned to an activation owner, and ready for emergency use.

A vendor is not ready because it has been identified. A vendor is ready only when the organization has confirmed its contract status, activation path, insurer status, authority requirements, data handling requirements, and coverage-risk implications.

X.1 Vendor Register

Complete for each pre-approved incident vendor category. Enter the actual vendor name, contract status, insurer panel status, and the named activation owner.

Vendor Category	Vendor Name	Contract / Retainer	Insurer Panel Status	Activation Owner	Coverage Risk Status	Last Validated
Breach Counsel / Privilege Counsel			Approved/Non-Panel/Pending		Documented/ Pending	
Coverage Counsel			Approved/Non-Panel/Pending		Documented/ Pending	
DFIR Provider			Approved/Non-Panel/Pending		Documented/ Pending	
Recovery / Restoration Provider			Approved/Non-Panel/Pending		Documented/ Pending	
Crisis Communications Firm			Approved/Non-Panel/Pending		Documented/ Pending	
Notification Vendor			Approved/Non-Panel/Pending		Documented/ Pending	
Call Center Surge Provider			Approved/Non-Panel/Pending		Documented/ Pending	
Credit / Identity Monitoring Provider			Approved/Non-Panel/Pending		Documented/ Pending	

Vendor Category	Vendor Name	Contract / Retainer	Insurer Panel Status	Activation Owner	Coverage Risk Status	Last Validated
eDiscovery / Legal Hold Provider			Approved/Non-Panel/Pending		Documented/ Pending	
Ransomware / Extortion Advisor			Approved/Non-Panel/Pending		Documented/ Pending	
Sanctions / Payment Compliance Advisor			Approved/Non-Panel/Pending		Documented/ Pending	
Identity Recovery Provider			Approved/Non-Panel/Pending		Documented/ Pending	
Backup Recovery Provider			Approved/Non-Panel/Pending		Documented/ Pending	
Cloud / SaaS Recovery Specialist			Approved/Non-Panel/Pending		Documented/ Pending	
OT / Industrial Recovery Specialist			Approved/Non-Panel/Pending		Documented/ Pending	
Payment Fraud Recovery Support			Approved/Non-Panel/Pending		Documented/ Pending	
Translation / Accessibility Vendor			Approved/Non-Panel/Pending		Documented/ Pending	
Mailing / Print Vendor			Approved/Non-Panel/Pending		Documented/ Pending	
Regulatory Response Advisor			Approved/Non-Panel/Pending		Documented/ Pending	
Customer Security Response Support			Approved/Non-Panel/Pending		Documented/ Pending	

X.2 Vendor Panel Verification Record

Vendor	Category	Carrier Panel Status	Confirmation Date	Consent Required?	Broker Confirmed	Policy Year	Notes

Under Carrier Panel Status, use: Approved / Consent Required / Non-Panel / Pending / Not Claim-Relevant

X.3 Non-Panel Vendor Coverage Risk Acknowledgment

Complete when engaging a vendor not on the insurer's approved panel.

— Vendor Name:

— Vendor Category:

— Incident / Activation ID:

— Applicable Policy:

— Carrier:

— Broker:

— Panel Status: Approved / Consent Required / Non-Panel / Pending / Unknown

— Carrier Consent Requested: Yes / No / Not Possible / Pending

— Broker Consulted: Yes / No / Pending

— Reason for Using Vendor:

— Emergency Business Justification:

— Potential Coverage Risk:

— Estimated Spend:

— Emergency Spending Authority Used:

— Decision Log Reference:

Required Acknowledgment: The organization acknowledges that use of this vendor may create reimbursement, consent, sublimit, or coverage risk under applicable insurance policies. The organization has reviewed the business reason for proceeding, the available alternatives, the timing constraints, and the potential claim implications.

— Approved By: _____ Date: _____

— CEO: _____ Date: _____

— CFO: _____ Date: _____

— General Counsel: _____ Date: _____

— CISO / CIO: _____ Date: _____

— Board Chair or Risk Committee Chair, if required: _____ Date: _____

X.4 Vendor Activation Matrix

Vendor Type	Who Can Activate	Pre-Activation Check Required	Carrier Consent Required?	Legal Review Required?	Emergency Exception
Breach Counsel					
Coverage Counsel					
DFIR Provider					
Recovery Vendor					
Crisis Communications					
Notification Vendor					
Call Center Provider					
Ransomware / Extortion Advisor					
eDiscovery / Legal Hold					
Identity Recovery					
Backup Recovery					
OT Recovery Specialist					
Payment Fraud Support					

X.5 Required Incident Vendor Categories

Vendor Category	Required?	Current Vendor	Contract Status	Panel Status	Gap / Action
Breach Counsel / Privilege Counsel	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Coverage Counsel	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
DFIR Provider	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Recovery / Restoration Provider	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Crisis Communications Firm	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Notification Vendor	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Call Center Surge Provider	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Credit / Identity Monitoring Provider	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
eDiscovery / Legal Hold Provider	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Ransomware / Extortion Advisor	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Sanctions / Payment Compliance Advisor	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Identity Recovery Provider	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Backup Recovery Provider	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Cloud / SaaS Recovery Specialist	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
OT / Industrial Recovery Specialist	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed

Vendor Category	Required?	Current Vendor	Contract Status	Panel Status	Gap / Action
Payment Fraud Recovery Support	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Translation / Accessibility Vendor	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Mailing / Print Vendor	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Regulatory Response Advisor	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed
Customer Security Response Support	Yes/No		Active/Pending	Approved/Non-Panel	None/Action needed

X.6 Annual Vendor Validation Checklist

At least annually, and after any material insurance, vendor, business, or system change, the organization should validate:

1. breach counsel retainer is current;
2. breach counsel conflict check is current;
3. breach counsel panel status is verified;
4. coverage counsel activation path is current;
5. DFIR MSA or retainer is current;
6. DFIR insurer panel status is verified;
7. recovery vendor contract is current;
8. crisis communications vendor is current;
9. notification vendor contract is current;
10. BAA or DPA terms are current where applicable;
11. call center surge vendor is current;
12. eDiscovery / legal hold vendor is current;
13. ransomware or extortion advisor path is current;
14. sanctions or payment compliance path is current;
15. identity recovery provider is current;
16. backup recovery provider is current;
17. cloud, SaaS, or OT recovery vendors are current where applicable;
18. broker and carrier contacts are current;
19. non-panel vendor risks are documented;

20. 24/7 contacts have been tested;
21. emergency rates have been verified;
22. vendor activation has been tested during a BIM exercise.

ADDENDUM Z

Executive Quick-Start: First 30 Minutes After BIM Activation

Purpose: The first 30 minutes of a BIM activation determine whether the organization begins with control or confusion. The full BIM Plan governs the business response. This Executive Quick-Start compresses the first required leadership actions into a single operating sheet. It is not a substitute for the BIM Plan. It is the first-hour execution aid used to activate the plan correctly.

This artifact should appear near the front of every organization-specific BIM Plan, immediately after “How to Use This Plan.”

Governing Rule

When BIM activates, Executive Command does not wait for full technical certainty before beginning business consequence governance. The organization must open the business-response structure, preserve the decision record, control communications, begin insurance and regulatory analysis, and identify active business pressure domains immediately.

First 30 Minutes Checklist

Step	Required Action	Primary Owner	Deadline	Required Record
1	Activate BIM when credible business consequence potential exists			
2	Notify Executive Command and required workstream owners			
3	Open the Executive Command channel or bridge			
4	Open the Legal / Privilege channel if legal, regulatory, insurance, personnel, customer, safety, financial, or board exposure may exist			
5	Open the Operations / Technical-to-Business channel			
6	Start the Decision Log			
7	Start the Open Action Register.			
8	Open or confirm the Single Source of Truth.			

Step	Required Action	Primary Owner	Deadline	Required Record
9	Deliver the Security-to-Business Activation Brief			
10	Assess cyber, crime, E&O, D&O, property, business interruption, product, bond, professional liability, or other insurance notice requirements.			
11	Assess regulatory, contractual, customer, patient, account holder, safety, product, or board notification triggers			
12	Complete the Initial Business Pressure Domain Screen			
13	Determine whether board or committee notification threshold may be met			
14	Issue employee communication restrictions if the workforce may become aware of the event.			
15	Confirm first Executive Command cadence.			

Sector Add-On Examples

— Healthcare: Add: assess clinical downtime activation; notify CMO/COO; confirm patient safety status.

— Banking: Add: assess unauthorized EFT exposure; notify fraud operations; confirm account restriction authority.

— MedTech: Add: assess patient safety signal; notify quality/regulatory; confirm CVD process owner.

— FinTech: Add: assess trading/ledger integrity; notify clearing partner contact; confirm SAR/BSA reviewer.

— SaaS / HealthSaaS: Add: assess tenant scope; notify customer success lead; confirm status page approval path.

— Financial Services / RIA: Add: assess discretionary trading exposure; notify custodian contact; confirm fiduciary integrity reviewer.

— Manufacturing / IT-OT: Add: assess OT safety status; notify plant director; confirm local stop authority.

Implementation note: This page should be printed, laminated, or pinned in the Executive Command channel. It is an execution aid, not a record of completion — the Decision Log and Open Action Register remain the system of record.

ADDENDUM Z-2

BIM Activation Notice Template

Purpose: The BIM Activation Notice is the short-form notice that tells leadership BIM is active. It is not the Security-to-Business Activation Brief. The Activation Notice starts the business response. The Activation Brief follows with structured facts, knowns, unknowns, technical status, business implications, and required decisions.

Governing Rule

The BIM Activation Notice must be sent immediately after activation through pre-approved channels. It should be short, factual, and action-oriented. It must not speculate about cause, fault, scope, legal reportability, insurance coverage, regulatory consequences, or customer impact.

Notice Fields

Date / Time Activated: _____

Activated By: _____

Activation Authority Basis: _____

BIM Level: _____

Reason for Activation: _____

Known Systems / Sites / Products / Accounts / Tenants Affected: _____

Known Facts: _____

Unknowns: _____

Potential Business Consequences: _____

Executive Command Channel: _____

Legal / Privilege Channel: _____

Operations Channel: _____

First Activation Brief Due: _____

Immediate Required Action: _____

Issued To: _____

Governing Question: *Join Executive Command. Use approved BIM channels only. Do not speculate in email, chat, SMS, tickets, CRM notes, support channels, or side channels. Preserve relevant records.*

Sector-Specific Field Additions

— Healthcare: Add: affected site/service line; clinical downtime status.

— Banking: Add: affected account population estimate; payment rail involved.

— MedTech: Add: affected product/device/software version; safety signal status.

— FinTech: Add: affected trading system or ledger; customer funds exposure status.

— SaaS / HealthSaaS: Add: affected tenant scope classification; subprocessor involvement.

— RIA / Wealth: Add: affected custodian; discretionary authority exposure status.

— Manufacturing / IT-OT: Add: affected plant/line/cell; OT safety status.

ADDENDUM Z-3

Initial Business Pressure Domain Screen

Purpose: The eleven business pressure domains are not only a planning map. They must be screened during activation. This screen forces Executive Command to determine which business domains may be active, who owns the first decision, what evidence must be preserved, and when the domain will be reviewed again.

Governing Rule

This screen must be completed within the first 60 minutes of BIM activation and updated at each Executive Command cadence until stand-down.

Domain Screen

Domain	Status	Owner	Immediate Decision	Evidence Required	Next Update
Legal and Privilege	Yes / No / Unknown				
Insurance and Claims	Yes / No / Unknown				
Regulatory and Compliance	Yes / No / Unknown				
Board and Governance	Yes / No / Unknown				
Customer / Patient / Account Holder / Stakeholder Trust	Yes / No / Unknown				
Operations and Continuity	Yes / No / Unknown				
Finance and Revenue	Yes / No / Unknown				
Contracts and Third Parties	Yes / No / Unknown				
Communications	Yes / No / Unknown				
HR and Workforce	Yes / No / Unknown				

Evidence and Defensibility	Yes / No / Unknown				

Governing Question: *Any domain marked “Unknown” requires a named owner and a next update time. Unknown is not a passive status. It is an assigned investigation path.*

ADDENDUM Z-4

Evidence Package Index

Purpose: A serious incident creates multiple evidence records for different downstream reviewers: counsel, insurers, regulators, board members, customers, auditors, plaintiffs, vendors, and executive leadership. The Evidence Package Index organizes the evidence record by use. It does not replace the Single Source of Truth. It is the index that makes the Single Source of Truth defensible, navigable, and reviewable.

Governing Rule

Evidence must be organized while the incident is active, not reconstructed after the fact. Every evidence package must have an owner, storage location, update cadence, and closure standard.

Core Evidence Packages

Evidence Package	Owner	Storage Location	Required Contents	Update Cadence	Review / Approval
Executive Decision Record					
Legal / Privilege Package					
Insurance Claim Package					
Regulatory Notification Package					
Board Governance Package					
Communications Package					
Customer / Patient / Account Holder Harm Package					
Operations / Downtime Package					
Vendor / Third-Party Package					

Corrective Action Package					

Sector-Specific Evidence Package Additions

— Healthcare: Add: Clinical Downtime Package; HIPAA Notification Package.

— Banking: Add: Fraud / EFT Claim Package; Reg E Analysis Package.

— MedTech: Add: CVD / Field Action Package; QMS/CAPA Package.

— FinTech: Add: Trading Integrity Package; SAR/BSA Restricted Package.

— SaaS / HealthSaaS: Add: Tenant Scoping Package; Subprocessor Coordination Package.

— RIA / Wealth: Add: Fiduciary Integrity Package; Custodian Reconciliation Package.

— Manufacturing / IT-OT: Add: OT Safety Package; Shipped Product Conformance Package.

ADDENDUM Z-5

Regulatory Notification Decision Tracker

Purpose: Regulatory inquiry response is not the same as notification decision tracking. The Regulatory Notification Decision Tracker documents whether a notification obligation may exist, when the clock may have started, who reviewed the issue, what decision was made, what notice was sent, and where the supporting evidence is stored.

Governing Rule

Every potential regulatory notification obligation must be logged even if the final decision is that notice is not required. A “no notice required” decision is still a decision and must be supported by evidence and counsel review where appropriate. Timing and legal obligations referenced in this tracker must be validated by counsel.

Tracker Fields

Potential Obligation	Trigger Facts	Possible Clock Start	Deadline	Owner	Counsel Review	Decision	Notice Sent?	Rationale	Evidence Location

Each entry must distinguish:

1. confirmed facts
2. assumptions
3. unknowns
4. decision owner
5. counsel reviewer
6. applicable deadline
7. evidence relied upon
8. decision rationale
9. next review date if pending

Sector Examples

— Healthcare: HIPAA Breach Notification Rule; state AG notification; HHS OCR reporting.

— Banking: GLBA Safeguards Rule incident reporting; state banking regulator notification; SAR filing.

— MedTech: FDA MDR/vigilance reporting; EU MDR incident reporting; notified body notification.

— FinTech: SEC/FINRA incident disclosure; state money transmitter notification; SAR/BSA filing.

— SaaS / HealthSaaS: State data breach notification statutes; HIPAA business associate notification; customer contractual notice.

— RIA / Wealth: SEC Form ADV disclosure considerations; state securities regulator notification.

— Manufacturing / IT-OT: DFARS/CMMC incident reporting; ITAR disclosure considerations; customer quality notification.

ADDENDUM Z-6

Affected Individual / Customer / Patient / Account Holder Harm Tracker

Purpose: Cyber incidents often create direct harm or potential harm to people, customers, patients, account holders, clients, tenants, or business partners. Communications alone do not manage that harm. BIM requires a tracker that connects affected populations to evidence, support decisions, restitution, communication, and closure.

Governing Rule

The organization must track harm by affected population and decision status. The tracker should not include unnecessary sensitive personal information. Access should be restricted based on legal, privacy, HR, regulatory, and business need.

Harm Tracker Fields

Affected Individual / Account / Population	Type of Harm	Evidence Basis	Action Taken	Communication Status	Restitution / Support Decision	Owner	Closure Evidence

Sector Adaptation Examples

— Healthcare: patient impact, PHI, clinical downtime, care disruption, patient support.

— Banking: unauthorized EFT, provisional credit, reimbursement, account restriction, fraud recovery.

— MedTech: patient/provider impact, device population, field action, provider outreach.

— FinTech: stored value, transfers, trading, custody, customer reimbursement, account restriction.

— SaaS / HealthSaaS: tenant impact, customer impact, downstream notification support, support surge.

— RIA / Wealth: client account integrity, unauthorized trading, corrective trades, make-whole decisions.

— Manufacturing / IT-OT: worker safety, customer part exposure, shipped product, field inspection, containment.

ADDENDUM Z-7

Multi-Policy Insurance Coordination Matrix

Purpose: A cyber incident may trigger more than the cyber policy. The organization may need to coordinate cyber, crime/fidelity, financial institution bond, E&O, professional liability, D&O, property/business interruption, contingent business interruption, product liability, recall, media, technology E&O, or sector-specific coverage. This matrix prevents the organization from assuming the cyber policy is the only applicable coverage.

Governing Rule

At BIM activation, the CFO, Risk, Legal, and coverage counsel must identify every potentially implicated policy. Notice, consent, evidence, panel vendor, cooperation, and proof-of-loss obligations must be tracked separately by policy.

Coordination Matrix

Policy	Carrier	Applies To	Notice Trigger	Notice Deadline	Consent Required?	Evidence Required	Owner	Coverage Counsel Role
Cyber								
Crime / Fidelity / Bond								
Professional Liability / E&O								
D&O								
Property / Business Interruption								
Product Liability / Completed Operations / Recall								

ADDENDUM Z-8

Board / Committee Incident Oversight Record

Purpose: The board briefing is not enough. The organization must also preserve a record of board or committee oversight. This record documents when the board was notified, what information was provided, what decisions or guidance were requested, what direction was given, and what follow-up was required.

Governing Rule

When a BIM activation meets or may meet a board, committee, materiality, safety, customer, regulatory, financial, fiduciary, or public-trust threshold, the board oversight record must be opened and maintained until final board reporting is complete.

Oversight Record Fields

Board / Committee Notified: _____

Trigger Threshold: _____

Date / Time Notified: _____

Notified By: _____

Materials Provided: _____

Known Facts Shared: _____

Unknowns Shared: _____

Decisions Requested: _____

Direction Given: _____

Follow-Up Required: _____

Next Update Due: _____

Final Board Report Required?: _____

Closure Evidence: _____

Interim Board Oversight Protocol

If the organization lacks a standing board-level function for the relevant risk, the BIM Plan must identify an interim oversight path.

Examples:

- healthcare organization without board clinical/cyber oversight
- SaaS company without board security committee
- manufacturer without OT/production-safety board oversight

- financial services organization without technology risk committee
- MedTech company without product security or safety oversight at board level

The interim protocol must name the committee or board member responsible until the standing structure is formed.

ADDENDUM Z-9

BIM-to-Regulated Program Interface Rule

Purpose: BIM does not replace regulated systems of record. Many BIM corrective actions involve programs that already have their own governance requirements: HIPAA compliance, BSA/AML, broker-dealer supervisory procedures, QMS/CAPA, AS9100D, ISO 9001, DFARS/CMMC, ITAR, product safety, privacy compliance, business continuity, vendor management, investment adviser compliance, or customer contract governance. This rule prevents BIM from creating informal remediation outside the proper system of record.

Governing Rule

BIM corrective actions that involve regulated controls, compliance obligations, quality systems, customer obligations, financial integrity, safety, privacy, fiduciary obligations, product safety, or sector-specific programs must be reviewed by the responsible workstream for entry into the appropriate system of record.

BIM does not independently create, own, or close regulated remediation. The applicable compliance, quality, supervisory, safety, privacy, legal, or operational program remains the system of record.

Interface Tracking Fields

BIM Finding	Regulated Program Implicated	System of Record	Program Owner	BIM Owner	Required Handoff	Validation Method	Closure Evidence

Sector Examples

— Healthcare: HIPAA Security Rule, privacy program, clinical downtime, patient safety, payer obligations.

— Banking: GLBA, BSA/AML, SAR, Reg E, fraud operations, safety-and-soundness remediation.

— MedTech: QMS, CAPA, complaint handling, MDR/vigilance, design controls, labeling, field action.

— FinTech: BSA/AML, sanctions, SAR, broker-dealer supervisory procedures, Reg S-P, trading controls, BCP.

— SaaS / HealthSaaS: HIPAA program, DPA/MSA obligations, subprocessor governance, tenant isolation, platform risk management.

— RIA / Wealth: Investment Advisers Act compliance, Custody Rule, Form ADV, fiduciary disclosure, trading supervision.

— Manufacturing / IT-OT: AS9100D, ISO 9001, CAPA, OT remediation, DFARS/CMMC, ITAR, supplier corrective action.

About Cybantage

Cybantage is a Security Incident Impact Advisory firm headquartered in Nashville, Tennessee.

We help executive leadership teams prepare for the business pressures that follow a security incident — before those decisions have to be made under pressure.

Our work focuses on the eleven business pressure domains that activate during a serious cyber incident: Insurance, Legal, Regulatory, Customer, Board, Revenue, Contracts, Executive Decisions, Communications, Leadership Accountability, and Long-Tail Remediation.

We serve organizations in Healthcare and MedTech, Financial Services and FinTech, Government Contracting, and Manufacturing — sectors where the business consequences of a security incident carry regulatory weight, financial exposure, and executive accountability.

Contact

Rod Andes | Executive Security Impact Advisor

randes@cybantage.com | (629) 275-2770 | www.cybantage.com

Cybantage

Legal Disclaimer

This publication is provided for informational and educational purposes only. The content reflects the views, observations, and professional experience of the author and does not constitute legal advice, insurance advice, regulatory guidance, financial advice, or professional services of any kind.

Nothing in this publication should be construed as establishing an attorney-client relationship, an advisory relationship, or any other professional relationship between Cybantage, Rod Andes, or any affiliated party and the reader.

The frameworks, models, protocols, and deliverable descriptions contained in this publication are general in nature and are not tailored to the specific facts, circumstances, regulatory obligations, legal requirements, insurance policy terms, or organizational structure of any particular organization. Organizations implementing Business Impact Management or any related capability should engage qualified legal counsel, insurance professionals, regulatory advisors, and other qualified professionals appropriate to their specific situation.

Cybantage makes no representations or warranties, express or implied, regarding the accuracy, completeness, or applicability of the content in this publication to any specific organization, incident, regulatory framework, or legal matter. Cybantage expressly disclaims any and all liability arising from reliance on the information contained in this publication.

References to specific regulatory frameworks, legal standards, or industry requirements are provided for illustrative purposes only and may not reflect the most current developments in applicable law or regulation. Readers should consult current legal and regulatory sources and qualified advisors for authoritative guidance.

The framework described in this guide is not a substitute for an organization-specific BIM plan. A generic framework does not create a ready-to-execute plan. The framework must be translated into an organization-specific plan that reflects the organization’s actual obligations, personnel, systems, vendors, contracts, insurance, and governance structure.

Cybantage Press | 2026