BUSINESS RESILIENCE

Threat Readiness Playbook

Know what can interrupt performance. Build the capacity to respond before disruption.

A decision-led guide for business leaders responsible for operations, customers, people, technology and financial continuity.

THE OBJECTIVE

The objective is not to predict every threat. It is to identify the few disruptions that could materially harm the business, reduce the exposure, and demonstrate that people can respond and recover.

What this playbook delivers

- A 2026 view of the changing threat environment and eight practical threat categories.
- An assessment checklist to expose gaps in controls, response and recovery.
- A four-phase, 90-day implementation route with owners, gates and evidence.
- Operational templates for risk registers, incident decisions, exercises and executive reporting.

Contents

Outline and operating model	2	Phase 2: Reduce and prepare	10
What changed in 2026	3	Phase 3: Respond and continue	11
Types of threats	4	Phase 4: Test and improve	12
Assess and prioritize	5	First-response decision card	13
Threat assessment checklist: part A	6	Scenario exercises	14
Threat assessment checklist: part B	7	Working templates	15
Four-phase roadmap	8	Executive readiness dashboard and 90-day plan	17
Phase 1: Understand exposure	9	Sources and method	18

Version 1.0, November 2026. Adaptable guidance for small and mid-sized organizations. It is not a certification, legal opinion or guarantee against disruption.

© 2026 **ilene.ai** · AI to ROI

Outline and operating model

A practical management system, not another risk report.

The decision sequence

Decision	Leadership question	Required evidence
1. Exposure	What would stop us serving customers or meeting obligations?	Critical services, dependencies, credible scenarios
2. Treatment	Which gaps matter enough to fix now?	Likelihood × impact; existing controls; named owner
3. Readiness	Could we make decisions, continue and recover under pressure?	Playbooks, exercises, tested recovery, improvement log

Four implementation phases

- **Phase 1: Understand exposure.** Map critical outcomes, threats, dependencies and risk owners.
- **Phase 2: Reduce and prepare.** Implement high-value controls, alternative methods and authority paths.
- **Phase 3: Respond and continue.** Establish clear escalation, response and recovery routines.
- **Phase 4: Test and improve.** Exercise, verify evidence and embed a monthly risk review.

Who owns what

Role	Accountability
Executive sponsor	Sets risk appetite, funds treatment, and accepts or escalates residual risk.
Readiness lead	Maintains the threat register and coordinates assessments, exercises and action tracking.
Service and process owners	Define tolerable downtime, dependencies and manual continuity.
Specialist owners	Security, IT, privacy, legal, HR, facilities, finance and supplier management: advise and execute.
Incident commander	Coordinates a live event; can convene decision makers and activate plans.

OPERATING RULE

Every material threat needs a business owner, an agreed treatment, a trigger for escalation and a way to prove the control works.

© 2026 **ilene.ai** · AI to ROI

What changed in 2026

The threat environment became more connected, faster moving and harder to isolate.

2026 signal	What changed and why it matters
Geoeconomic pressure	The World Economic Forum ranked geoeconomic confrontation as the most severe risk in its two-year outlook. Trade, sanctions and policy shifts can disrupt suppliers, cost and demand. [S1]
More exposed software	Verizon reported vulnerability exploitation as the leading initial access path (31% of breaches in its dataset). Patch speed and asset visibility are business issues. [S2]
Ransomware persists	Ransomware was present in 48% of breaches in the 2026 Verizon dataset. Canadian authorities continue to flag severe operational impacts. [S2, S3]
Third-party concentration	Verizon reported third-party involvement in 48% of breaches, up 60% year over year in its dataset. Shared platforms multiply single-point-of-failure risk. [S2]
AI increases scale	The UK National Cyber Security Centre assessed that AI makes familiar attacks faster and more efficient, while unauthorized AI use creates data-handling exposure. [S4]
Physical volatility	Canada's Changing Climate Report 2026 assesses increasing climate extremes, including heat, wildfire, drought and flooding, across the country. [S5]

What executives should change now

- Treat cyber, business interruption, supplier and information risks as one connected operating exposure.
- Ask for evidence of recovery, not only policies: restoration tests, manual fallbacks and supplier exit options.
- Assume urgent messages, identities and AI-generated content may be convincingly falsified. Verify high-consequence decisions independently.
- Revisit scenarios when geography, supply chains, insurance terms, key systems or legislation change.

Evidence note: these reports cover different observation windows and populations. The percentages are not a prediction of risk for any particular organization.

Types of threats

Assess threats by their ability to interrupt the business, not by the department that owns them.

Category	Illustrative scenario	Potential exposure
Cyber and data	Ransomware; compromised credentials; software flaw; customer-data leak	Service outage, extortion, remediation costs
AI and information	Sensitive data in unapproved AI; manipulated content; false output; deepfake approvals	Wrong decisions, fraud, confidentiality breach
Supplier and cloud	Critical software-as-a-service (SaaS), telecom, payment processor or logistics provider fails	Single point of failure, recovery delay
Financial and fraud	Payment redirection; treasury fraud; liquidity or credit shock	Cash loss, inability to pay or collect
People and workplace	Critical staff unavailable; workplace violence; skills or access concentration	Safety exposure, service failure, knowledge loss
Physical and climate	Wildfire smoke, flood, heat, earthquake, fire, extended utility outage	Site loss, safety, inventory and delivery impacts
Geopolitical and market	Tariff, sanctions, shipping disruption, political conflict or demand shift	Cost inflation, stranded supply, revenue shock
Legal and trust	Regulatory non-compliance; privacy event; misleading public statement	Obligations, litigation, customer confidence

Look for compound threats

A supplier outage may stop customer support. An emergency may prevent staff reaching a site. A cyberattack may compromise both payment approval and communications. A single event often spans several categories.

Use a consistent scenario statement

Because [trigger] affects [asset or dependency], [critical business service] cannot operate for [duration], causing [specific customer, safety, financial or compliance consequence].

© 2026 **ilene.ai** · AI to ROI

Assess and prioritize

Score the consequence to the business first. Avoid treating every possibility as equally urgent.

Five steps

- Identify 5 to 10 critical services and their dependencies: people, facilities, systems, data, vendors and funds.
- Define one credible scenario per exposure. Name the owner and the relevant geography or business unit.
- Rate likelihood (1 = rare, 5 = frequent or expected) and impact (1 = minor, 5 = severe).
- Record current control strength as evidenced, partial or unverified, and assign one remedial action.
- Rank the top five exposures, check the override conditions below and set decision dates.

Rating anchors

Score	Likelihood in the next 12 months	Impact if it occurs
1	Rare; no known pathway	Minor local interruption; negligible loss
2	Unlikely but plausible	Manageable interruption within normal operations
3	Possible; some precursors	Material disruption to a team or service
4	Likely; active exposure or repeated near misses	Major multi-service, financial or customer harm
5	Expected or recurring in this context	Severe or prolonged harm; critical obligations at risk

Exposure score = likelihood × impact. 1 to 5 Low, 6 to 11 Moderate, 12 to 19 High, 20 to 25 Critical.

Override the score

Escalate immediately, whatever the calculated rating, when life safety is threatened, a legal reporting deadline may have been triggered, a critical service exceeds its approved maximum tolerable downtime, or there is active extortion, compromise or irrecoverable data loss. The rating guides priorities; it is not an actuarial probability.

DECISION

Accept, reduce, transfer or share, or avoid each material risk. Acceptance requires a named executive, an explicit rationale and a scheduled review. Inactivity is not acceptance.

© 2026 **ilene.ai** · AI to ROI

Threat assessment checklist: part A

Mark Yes, Partial, No or N/A. For every Partial or No, record an owner, the evidence gap and a due date.

Area	Assessment question	Y / P / N / N/A
Governance	Is a sponsor accountable for threat readiness across the organization?	☐☐☐☐
Governance	Are the critical services and their business owners documented?	☐☐☐☐
Governance	Are risk appetite, severity triggers and authority limits approved?	☐☐☐☐
Governance	Are incidents, near misses and lessons reviewed regularly?	☐☐☐☐
Operations	Are maximum tolerable outage and recovery time targets set?	☐☐☐☐
Operations	Are dependencies, single points of failure and manual alternatives mapped?	☐☐☐☐
Operations	Can key decisions continue if core systems are unavailable?	☐☐☐☐
Operations	Can the business reach staff and customers through a backup channel?	☐☐☐☐
Cyber and data	Is multi-factor authentication (MFA) enforced for privileged, remote and critical access?	☐☐☐☐
Cyber and data	Are internet-facing systems inventoried and patched by risk?	☐☐☐☐
Cyber and data	Are backups isolated, protected and restoration-tested?	☐☐☐☐
Cyber and data	Are privileged access, logging and alert escalation controlled?	☐☐☐☐
Cyber and data	Are sensitive datasets classified, retained and restricted?	☐☐☐☐
AI and information	Is approved AI use defined for confidential or regulated data?	☐☐☐☐
AI and information	Do AI-assisted high-consequence decisions require human validation?	☐☐☐☐
AI and information	Are impersonation, deepfake and payment-change checks independent?	☐☐☐☐
AI and information	Do staff know where to report suspicious AI output or content?	☐☐☐☐

Suggested evidence: operating reports, architecture, supplier contracts, controls, test records, training logs and incident procedures. Evidence beats assertion: Yes means the control exists, has an owner and can be demonstrated.

© 2026 **ilene.ai** · AI to ROI

Threat assessment checklist: part B

Complete the same ratings and capture priority actions in the threat register.

Area	Assessment question	Y / P / N / N/A
Suppliers	Are critical vendors ranked by dependency and exit difficulty?	☐☐☐☐
Suppliers	Have continuity, security and incident-notice terms been checked?	☐☐☐☐
Suppliers	Are alternative suppliers, offline copies or fallback services viable?	☐☐☐☐
Suppliers	Are supplier access and integrations reviewed regularly?	☐☐☐☐
Finance	Are payment and banking changes verified on a trusted channel?	☐☐☐☐
Finance	Do dual approvals and transaction limits cover urgent transfers?	☐☐☐☐
Finance	Is short-term liquidity sufficient for a material interruption?	☐☐☐☐
People and safety	Are evacuation, shelter and emergency contact processes clear?	☐☐☐☐
People and safety	Are critical responsibilities covered by trained alternates?	☐☐☐☐
Physical	Have local hazards and utility outage exposure been assessed?	☐☐☐☐
Physical	Are insurance cover, deductibles and exclusions current?	☐☐☐☐
Legal and trust	Are privacy, safety, contract and reporting obligations identified?	☐☐☐☐
Legal and trust	Is approval of customer and public communications assigned?	☐☐☐☐
Response	Is there a reachable incident commander and substitute?	☐☐☐☐
Response	Can the crisis team convene without primary email or chat?	☐☐☐☐
Response	Have response scenarios and recovery steps been exercised?	☐☐☐☐
Response	Do post-incident actions have owners and closure evidence?	☐☐☐☐

Interpretation

Each No is an untreated gap; each Partial is an evidence or design gap. Rate the scenario consequence using the anchors on page 5. Escalate any safety, active-incident or statutory deadline issue immediately. Do not total the ticks into a security score.

© 2026 **ilene.ai** · AI to ROI

Four-phase roadmap

A 90-day starting plan. Compress the timetable for active or critical exposures.

Phase	Window	Outcome and evidence	Gate
1. Understand exposure	Days 1 to 10	Critical services; scenario register; scored top five risks	Sponsor accepts the risk baseline
2. Reduce and prepare	Days 11 to 30	Controls, vendor checks, recovery options; evidence of action	Risk owners sign off critical gaps or exceptions
3. Respond and continue	Days 31 to 60	Incident roles, triggers, communications, continuity playbooks	Leaders approve usable response plans
4. Test and improve	Days 61 to 90	Exercises, measured recovery, residual risk decisions, readiness dashboard	Go, improve or escalate decision

Minimum deliverable set

- Critical-service map (one page) and business-impact assumptions.
- Threat register with severity, treatment, owner, due date and evidence.
- Incident commander and escalation roster, with a backup contact channel.
- Recovery and continuity steps for the highest-consequence service.
- Exercise record, open issues and the executive readiness dashboard.

Resource model

Sponsor: 30 to 45 minutes weekly through Day 30, then at gates. Readiness lead: coordinates the work and maintains the register. Process owners, IT and security, finance, HR, facilities, privacy and legal, and supplier managers contribute only where their exposure is material. Timelines are planning examples, not standards.

DEFINITION OF READY

An implementation is ready only when the business owner can show how the service will be protected, interrupted safely and restored within agreed limits.

© 2026 **ilene.ai** · AI to ROI

Phase 1: Understand exposure

Days 1 to 10. Establish what matters and what could interrupt it.

Do the work

- Set scope: functions, sites, systems, operating regions and a 12-month planning horizon.
- Interview critical-service owners: what must stay available, for whom, and for how long?
- Map dependencies: vendors, cloud platforms, payment rails, people, facilities, data and utilities.
- Review incident history, near misses, contract and insurance limits, and current 2026 signals.
- Write credible scenario statements, score likelihood and impact, and identify weak evidence.
- Prioritize the top five and assign a business owner to each.

Critical-service map: example

Service	Primary dependency	Disruption consequence	Business owner
Order fulfilment	ERP, warehouse and carrier	Missed deliveries, customer credits	COO
Billing and cash	Finance software and banking	Missed billing, cash collection delay	CFO
Customer support	Ticketing and connectivity	Response delays, customer attrition	Service lead

Outputs and gate

Produce: scenario register (up to ten scenarios), top five risks, owner map and provisional outage tolerances.

Approve: the sponsor confirms the exposure scope and the highest-consequence priorities.

Block: a critical service has no owner, no dependency map or an unknown material safety exposure.

ASK

If our top service went offline at 9 a.m. tomorrow, who would know first, who could decide, and what would customers experience by noon?

© 2026 **ilene.ai** · AI to ROI

Phase 2: Reduce and prepare

Days 11 to 30. Close high-value weaknesses before investing in lower-consequence work.

Exposure	Minimum treatment	Evidence to request
Account compromise	MFA, least privilege, rapid account disablement	Access review, MFA coverage report
Software exploitation	Inventory and risk-based patching; exposed-service review	Remediation dates; exception decisions
Data loss and ransomware	Protected backups and a tested restore	Restore log and recovered sample
AI misuse and impersonation	Approved tool and data rules; second-channel verification	Policy, sample approvals, staff practice
Supplier dependence	Contract continuity terms, alternate process or exit route	Supplier review and fallback demonstration
Facility or people outage	Alternate location, staff cover, emergency supplies	Drill record, contact validation
Fraud and liquidity	Dual approvals, payment callback, cash-stress assumptions	Payment test and liquidity worksheet

Select treatments using three tests

- **Effect:** does the measure materially reduce the probability or duration of the specific scenario?
- **Feasibility:** is it achievable with the current people, budget and supplier access?
- **Proof:** can someone independent verify that the control is operating?

Exception protocol

When a critical treatment cannot be completed on time, document the residual exposure, the interim compensating control, the accountable executive, an expiry date and the conditions that trigger immediate escalation. Do not mark it closed.

GATE

Protect the highest-consequence services first. A purchased tool is not evidence of reduced exposure until the control is configured and tested.

Phase 3: Respond and continue

Days 31 to 60. Make the first decisions under pressure predictable.

Prepare five connected playbooks

- **Detect and classify:** who receives reports, validates signals, records facts and declares severity?
- **Command and contain:** who is incident commander, which actions require approval, and who covers absences?
- **Maintain service:** manual work, alternate suppliers or sites, maximum tolerable outage and restoration targets.
- **Communicate:** staff, customers, board, insurer, regulator and public. Who verifies facts and signs off messages?
- **Recover and learn:** validation before restart, evidence preservation, customer remediation and after-action review.

Working severity model

Level	Example trigger	Response expectation
1. Monitor	Contained anomaly with no material service impact	Owner investigates; log and track
2. Material	Key system degraded; potential customer, financial or privacy impact	Lead convenes the response team; update the sponsor
3. Crisis	Life safety concern; widespread critical outage; active extortion or serious regulated event	Incident commander activates the crisis team immediately; obtain specialist advice

Record recovery tolerances

For each service, document the maximum tolerable outage, the recovery time objective (RTO) and the recovery point objective (RPO, the acceptable data-loss window). Obtain business-owner approval and test actual capability. Contractual uptime is not the same as recoverability.

GATE

Can the team coordinate while primary email, messaging and telephony are unavailable? If not, the response process is not operational.

Phase 4: Test and improve

Days 61 to 90. Replace policy confidence with observed performance.

Run a 90-minute cross-functional exercise

- **10 minutes:** issue a plausible incident alert and ask who declares severity.
- **20 minutes:** test how decision makers convene and use verified backup contacts.
- **25 minutes:** present escalating customer, supplier, financial and legal consequences.
- **20 minutes:** make recovery, communication and risk-acceptance decisions using the plans.
- **15 minutes:** review missing owners, unclear authorities, delays and residual exposure.

Pass or fail on evidence

Test	Pass condition
Response activation	Commander and required deputies reached; severity declared consistently.
Business continuity	Fallback works for a representative transaction or workflow.
Restore and data integrity	A protected backup or sample can be restored and reconciled.
External communications	Customer notice drafted from verified facts, with an approval owner.
Improvement closure	Each material gap has an owner, a date and a retest method.

Sustain the system

Hold a monthly 30-minute exception review for the top risks. Refresh dependencies quarterly and whenever an acquisition, new vendor, AI workflow, major market shock or actual incident changes the exposure. Re-run the relevant scenario after any material change.

GATE

Label readiness as demonstrated only for controls and scenarios that were tested. Record untested items as assumptions, not successes.

© 2026 **ilene.ai** · AI to ROI

First-response decision card

Use this card during a suspected material incident. Adapt it to local obligations and professional advice.

When	Incident lead action	Business decision
Immediately	Protect life and safety; verify the alert; record a timeline; assign a commander.	Should normal operations pause to protect people or data?
First 15 to 60 minutes	Contain with qualified specialists; preserve evidence; activate alternate contacts.	Which systems, transactions or locations must be isolated?
First 1 to 4 hours	Confirm affected services and data; invoke continuity; contact insurer, legal and security as needed.	What must be prioritized, disclosed or escalated now?
First 24 hours	Validate facts, estimate recovery, give approved updates, track decisions and obligations.	Can service safely resume? What is still unknown?
After stabilization	Confirm restoration and integrity; assess harm; conduct an after-action review.	Which corrective actions prevent recurrence?

Non-negotiable rules

- Do not let an unverified caller, email or AI-generated message override payment or disclosure controls.
- Do not destroy potential evidence. Use trained responders for containment and forensic decisions.
- Do not commit to a return-to-service time until recovery owners confirm it.
- Do not assume notification requirements are identical across jurisdictions. Obtain legal and privacy guidance promptly.

Incident log: capture at minimum

Time and source; observed facts and confidence; affected services and customers; severity and decision owner; action and approval; external notifications considered; next update time; open unknowns.

Customer message structure: what is affected; what is not yet known; what you are doing; any customer action; when the next update will come. Avoid speculation.

© 2026 **ilene.ai** · AI to ROI

Scenario exercises

Three cross-functional drills expose linked risks that single-department tests often miss.

A Ransomware plus software-as-a-service outage

Inject: a critical vendor reports suspicious activity; order processing stops and backups may be affected. At the same time, customers request delivery commitments.

- **Decide:** declare severity; isolate access as appropriate; verify vendor facts; activate a manual queue; prioritize customers; validate the restore path.
- **Pass:** roles reached, approved continuity works, customer message fact-checked, recovery confidence documented.

B AI voice spoofing and payment redirection

Inject: finance receives an urgent, convincing voice message apparently from an executive, followed by new bank details in a supplier email.

- **Decide:** use a trusted callback or second channel; stop or hold the transaction; preserve the message; assess whether credentials or vendor accounts are compromised.
- **Pass:** payment remains controlled despite the urgency; staff can explain the verification exception process.

C Severe weather and supplier failure

Inject: a regional extreme-weather event closes an operating site; power and connectivity are unstable and a carrier cannot meet commitments.

- **Decide:** protect people; transfer work; invoke alternate staffing, location or suppliers; revise service commitments and the cash outlook.
- **Pass:** staff safety confirmed; essential workflow continues within tolerance; customer prioritization is defensible.

Debrief template

Observed failure	Business consequence	Owner and retest date

© 2026 **ilene.ai** · AI to ROI

Working templates

Copy these fields into your operating register, project tracker or management system.

A Threat register

ID and service	Scenario and trigger	L × I	Control and gap	Owner and due date
T-01				
T-02				
T-03				
T-04				
T-05				

Also capture: expected impact, control evidence, treatment decision, residual risk, validation method, exception approver and next review date.

B Business impact and recovery

Critical service	Maximum tolerable outage	RTO and RPO	Manual or alternate route

© 2026 **ilene.ai** · AI to ROI

Working templates (continued)

Record each decision at the gate and keep escalation details where the response team can reach them.

C Gate decision

Phase and date

Sponsor and attendees

Evidence reviewed

Decision: approve, approve with conditions, return for remediation or stop

Conditions and owner

Next review and proof due

D Incident escalation

Incident commander and alternate

Backup contact channel or bridge

Business continuity owner

Security, legal, insurer and communications contacts

Keep contact details in a protected, reachable location. Do not circulate personal phone numbers in shared copies of this playbook.

Executive readiness dashboard and 90-day plan

Keep reporting to one page: risk exposure, evidence, exceptions and the decision needed.

Five decision metrics

Metric	How to read it	Expected direction
Top five risks with owner and treatment	Count out of 5, with signed dates	Toward 5 of 5
Critical services with approved tolerances	Count with owner-approved recovery requirements	Toward 100%
High-risk actions overdue	Number and age; show unaccepted exceptions	Toward zero
Controls independently demonstrated	Count tested divided by count selected for test	Increasing coverage
Scenario exercises passed	Passes divided by exercises, with tracked remediation	Increasing, with gaps closed

90-day execution calendar

By	Leadership milestone	Required decision
Day 10	Approve critical services, owners and top five risks	Fund or assign immediate treatments
Day 30	Review control evidence and unresolved material gaps	Accept the exception or escalate
Day 60	Approve incident, continuity and communication playbooks	Authorize exercises and fallback
Day 90	Review test results, residual exposure and the dashboard	Close, extend or re-scope the work

What goes to the board or owner

One page: the top exposure and its consequence; change since the last review; overdue actions; capability proven by exercise; residual exceptions requiring acceptance; the next investment or policy decision. Do not replace consequences and evidence with an aggregate maturity percentage.

NEXT ACTION

Appoint an executive sponsor and name the three services whose interruption would most damage customers, safety, cash or obligations. Start the checklist there.

© 2026 **ilene.ai** · AI to ROI

Sources and method

Where the figures come from, and how to use this playbook responsibly.

Sources

S1 World Economic Forum, Global Risks Report 2026 (14 January 2026). Open source

S2 Verizon, 2026 Data Breach Investigations Report. Open source

S3 Canadian Centre for Cyber Security, National Cyber Threat Assessment 2025-2026. Open source

S4 UK National Cyber Security Centre, Annual Review 2026 (3 November 2026). Open source

S5 Environment and Climate Change Canada, Canada's Changing Climate Report 2026. Open source

S6 NIST, Cybersecurity Framework 2.0 (2024). Open source

S7 ISO 22301:2019, Business continuity management systems. Open source

S8 Canadian Centre for Cyber Security, Developing your business continuity plan. Open source

S9 NIST, AI Risk Management Framework: Generative AI Profile (NIST AI 600-1, 2024). Open source

S10 Government of British Columbia, Economic Preparedness Guide for Businesses. Open source

Public sources were checked for this edition on 7 November 2026.

About the model

The four phases, score bands, example thresholds, templates, gate criteria and timelines are ilene.ai working conventions. They are not a certified method or the stated requirements of NIST, ISO or any other authority. The approach is informed by NIST CSF 2.0, business continuity guidance, AI risk guidance and current threat reporting.

When to refresh

Review the threat assumptions after a material cyber incident, service outage, acquisition, regulatory change, AI deployment, insurer or supplier change, financial shock or severe-weather exposure.

Related ilene.ai resources

- **Writing Your AI Acceptable Use Policy:** set the approved tools and data rules that Phase 2 asks for.
- **Questions to Ask Any AI Vendor:** check continuity, security and incident-notice terms before you sign.
- Both are free on the Resources page at ilene.ai.

Want an independent view of your exposure?

Through AI Governance, ilene.ai helps leadership teams set the controls, ownership and decision rights that keep AI and the systems around it safe to run.

Talk to ilene.ai