Enterprise Risk Intelligence

A decision-centered operating playbook for converting uncertainty, external change and enterprise exposure into actionable intelligence.

REQUIRE	COLLECT	ANALYZE	ASSESS	DECIDE	LEARN
Questions	Evidence	Meaning	Exposure	Action	Feedback

EXECUTIVE PURPOSE
Create an enterprise capability that tells leadership what is changing, why it matters, how confident the assessment is, what could happen next and which decisions deserve attention.

YAKAMICHI PERSPECTIVE

Risk intelligence is valuable only when it changes the quality or timing of a decision.

Contents & Operating Principles

OPERATING PRINCIPLE

Do not build an intelligence function around information volume. Build it around recurring executive questions, material uncertainty and decisions where earlier insight creates advantage.

Executive Intelligence Mandate

Enterprise risk intelligence connects external developments and internal exposure to executive decisions. It complements risk management by adding forward-looking collection, structured analysis, warning and scenario thinking.

CAPABILITY	EXECUTIVE VALUE
Environmental scanning	Detect meaningful external change
Protective / threat intelligence	Recognize emerging security concerns
Geopolitical intelligence	Translate political and policy change into business implications
Competitive intelligence	Understand market, competitor and technology movement
Third-party intelligence	Identify supplier and partner deterioration
Strategic intelligence	Challenge assumptions beneath plans and investments

- Define the decisions intelligence should support.
- Establish lawful, ethical and proportionate collection standards.
- Require separation of fact, judgment and confidence.
- Ensure business exposure is part of every material assessment.
- Create feedback so intelligence improves after decisions and outcomes.

MANDATE TEST

If the intelligence team cannot name the decision, assumption or exposure an assessment supports, the requirement is probably too broad.

Priority Intelligence Requirements

Priority Intelligence Requirements, or PIRs, convert executive uncertainty into answerable questions. They prevent collection from becoming an endless stream of interesting but irrelevant information.

PIR ELEMENT	EXAMPLE
Decision	Whether to enter, expand, pause or exit a market
Core question	What developments could materially change the investment case?
Indicators	Policy, security, currency, sanctions, competitor or infrastructure changes
Time horizon	Immediate / 90 days / 12–36 months
Owner	Executive or business function that needs the answer
Review trigger	Decision completed, assumptions changed or requirement no longer material

Good PIRs

- Are specific enough to guide collection and analysis.
- Address uncertainty rather than request a general topic update.
- Have an identifiable decision-maker or business owner.
- Include a time horizon and materiality threshold.
- Are reviewed as strategy and exposure change.

PIR DISCIPLINE

'Monitor geopolitical risk' is a topic. 'Which policy changes could interrupt our ability to source component X during the next 12 months?' is an intelligence requirement.

Collection, Sources & Validation

Collection should be lawful, authorized and proportionate. Source diversity matters because every source has access limitations, incentives and potential error.

SOURCE TYPE	USE / LIMITATION
Official / regulatory	Authoritative for formal action; may lag emerging conditions
Commercial data	Structured and scalable; quality varies by provider
Open-source media	Fast and broad; requires verification and bias awareness
Internal data	Directly relevant to exposure; can reflect organizational blind spots
Subject-matter experts	Context-rich; judgments may be subjective
Third-party / supplier reporting	Useful for dependency status; incentives may affect disclosure

Validation Rules

- Record source origin and date.
- Distinguish primary reporting from repetition of another source.
- Corroborate consequential claims where practical.
- Assess source access, reliability and possible incentives.
- Flag information that cannot yet be independently confirmed.
- Protect confidential and personal information according to policy and law.

COLLECTION PRINCIPLE

More sources do not automatically create more confidence. Ten reports repeating one unverified claim are still one underlying claim.

Analysis, Confidence & Alternative Views

Analysis turns evidence into judgments. Structured discipline reduces the risk that urgency, hierarchy or a compelling narrative quietly becomes certainty.

ELEMENT	REQUIREMENT
Key judgment	State the assessment clearly
Evidence	Identify the strongest supporting information
Assumptions	Make important unverified premises visible
Confidence	Low / Moderate / High with reason
Alternatives	Consider credible competing explanations
Gaps	State missing information that could change the judgment
Implications	Explain what the assessment means for the enterprise

Analytic Techniques

- Competing hypotheses for ambiguous events.
- Key-assumptions checks before major strategic decisions.
- Pre-mortems to explore how a decision could fail.
- Scenario analysis for high-uncertainty futures.
- Red-team or independent challenge for consequential assessments.

CONFIDENCE PRINCIPLE

Confidence describes the strength of the assessment, not the importance of the issue. A high-impact risk may still have low-confidence evidence.

Enterprise Exposure & Risk Translation

An external event becomes enterprise risk only through exposure. Intelligence should connect developments to specific markets, people, assets, suppliers, data, technology, revenue, obligations or strategic assumptions.

EXPOSURE	QUESTIONS
People	Who could be affected and where?
Operations	Which critical services or facilities depend on the condition?
Supply chain	Which suppliers, routes or upstream dependencies are exposed?
Technology / data	Which platforms, data flows or jurisdictions are implicated?
Financial	What revenue, cost, liquidity or capital assumptions could change?
Legal / reputation	Which obligations, stakeholders or trust relationships matter?

Translation Sequence

- What changed?
- Where do we intersect with it?
- What plausible consequences follow?
- How quickly could those consequences emerge?
- Which controls or alternatives reduce exposure?
- What decision is required now, later or only if an indicator changes?

EXPOSURE PRINCIPLE

A dramatic event with no meaningful enterprise intersection may deserve monitoring, not escalation. A quiet policy change affecting a critical dependency may deserve immediate executive attention.

Indicators, Warning & Escalation

Warning converts intelligence from explanation into anticipation. Indicators should be observable, relevant to a scenario and linked to a predefined escalation or review action.

INDICATOR TYPE	EXAMPLES
Political / regulatory	Draft rules, enforcement posture, sanctions or licensing changes
Security	Threat reporting, incidents, unrest or access restrictions
Financial	Credit deterioration, liquidity stress, payment delays
Supplier	Service degradation, ownership change, layoffs or repeated outages
Technology	Critical vulnerability, provider change or infrastructure failure
Competitive	Pricing, hiring, partnerships, patents or market-entry signals

Escalation Model

LEVEL	MEANING	ACTION
Green	Baseline conditions	Routine monitoring
Amber	Meaningful change / uncertainty increasing	Focused collection + owner review
Red	Threshold crossed / material consequence plausible	Executive escalation + contingency decision
Black	Material disruption underway	Crisis / continuity governance

WARNING PRINCIPLE

An indicator without an action threshold becomes dashboard decoration. Decide in advance what would cause leadership to review, prepare or act.

Scenario Intelligence & Strategic Options

Scenarios help leaders operate when a single forecast would create false precision. The objective is to test whether strategy remains robust across plausible pathways.

SCENARIO COMPONENT	CONTENT
Baseline	Current conditions and assumptions
Pathway	How conditions could plausibly evolve
Implications	Consequences for enterprise exposure
Indicators	Observable signs the pathway is becoming more likely
Options	Actions that preserve or create strategic flexibility
Decision points	When leadership must commit, pause, hedge or exit

Option Design

- No-regret actions useful across several scenarios.
- Hedges that reduce downside without abandoning upside.
- Contingent actions activated only when indicators cross thresholds.
- Exit or stop-loss conditions for irreversible exposure.
- Opportunity plays that become attractive under a specific pathway.

SCENARIO PRINCIPLE

Scenarios are not predictions. Their value is in revealing assumptions, vulnerabilities and options before events remove decision time.

Intelligence Products & Executive Briefing

Executives need concise products that distinguish what is known from what is assessed and make the business implication immediately visible.

PRODUCT	PURPOSE
Flash alert	Material development requiring immediate awareness
Executive brief	Judgment, evidence, confidence, implication and next indicators
Risk outlook	Periodic view of priority exposures and changes
Scenario paper	Alternative futures, signposts and strategic options
Decision support note	Focused assessment for a specific executive decision
Board intelligence brief	Strategic assumptions, material changes and decisions

Five-Part Executive Brief

1. Judgment What we assess.

2. Evidence Why we assess it.

3. Confidence How strongly the evidence supports the judgment.

4. Enterprise implication What it could change for the organization.

5. Watch / Decide Indicators to monitor and action required.

BRIEFING RULE

Lead with the judgment and implication. Do not make senior leaders excavate the conclusion from several pages of background.

Governance, Ethics, Metrics & Assurance

Enterprise intelligence must operate within clear legal, privacy, ethical and corporate boundaries. Governance protects both the organization and the credibility of the intelligence function.

AREA	CONTROL
Authority	Document mandate, ownership and escalation
Collection	Lawful, ethical and proportionate methods
Privacy	Minimize personal data and restrict access
Source handling	Protect confidential sources and sensitive records
Analysis	Separate evidence, judgment, confidence and uncertainty
Conflicts	Disclose material analyst or provider conflicts
Retention	Apply approved information lifecycle rules

Performance Metrics

- Priority requirements answered on time.
- Material warnings delivered before the decision point.
- Assessments that explicitly map enterprise exposure.
- Executive decisions informed by intelligence.
- Forecast/indicator performance reviewed after outcomes.
- Intelligence gaps and recurring collection failures.
- User feedback on relevance, clarity and timeliness.

ASSURANCE PRINCIPLE

Measure whether intelligence improved decisions, not how many reports were produced.

180-Day Enterprise Risk Intelligence Program

WINDOW	PRIORITY	DELIVERABLES
0–30 Days	Mandate & questions	Sponsor, governance charter, initial PIRs and priority exposures
31–60 Days	Sources & workflow	Source register, validation rules, collection plan and intake process
61–90 Days	Analytic standard	Assessment format, confidence language, alternative analysis and review
91–120 Days	Warning & scenarios	Indicators, thresholds, escalation and two priority scenarios
121–150 Days	Executive products	Flash alert, executive brief, outlook and board reporting cadence
151–180 Days	Assurance & learning	Metrics, decision review, feedback loop and improvement roadmap

Success at Day 180

- Executive intelligence requirements are explicit.
- Priority enterprise exposures are mapped.
- Sources and validation standards are governed.
- Assessments show confidence, alternatives and gaps.
- Indicators are tied to escalation thresholds.
- Executive products lead with implications and decisions.
- Performance is measured through decision relevance and learning.

PROGRAM PRINCIPLE

Start with a small number of consequential questions. A focused intelligence capability that executives use is more valuable than a large reporting operation they ignore.

Priority Intelligence Requirement Template

FIELD	RECORD
Executive / owner	______________
Decision supported	______________
Intelligence question	______________
Why it matters	Enterprise exposure / assumption
Time horizon	Immediate / 90 days / 12+ months
Indicators	Observable signs to monitor
Collection priorities	Sources / information needed
Escalation threshold	What change requires review/action
Review date	______________

Source & Validation Register

SOURCE	TYPE	ACCESS / RELIABILITY	CORROBORATION	LIMITATIONS
______	Official / OSINT / internal / expert	______	______	______
______	______	______	______	______
______	______	______	______	______
______	______	______	______	______

Record enough provenance to understand where consequential information originated and whether apparently independent reporting shares the same underlying source.

Intelligence Assessment Record

ELEMENT	ASSESSMENT
Key judgment	______________
Supporting evidence	______________
Key assumptions	______________
Confidence	Low / Moderate / High + rationale
Alternative explanation	______________
Information gaps	______________
Enterprise exposure	______________
Implication / decision	______________
Next indicators	______________

Warning & Escalation Register

INDICATOR	BASELINE	AMBER	RED	OWNER / ACTION
______	______	______	______	______
______	______	______	______	______
______	______	______	______	______
______	______	______	______	______

WARNING DESIGN

Thresholds should be observable enough that different analysts can recognize the same change and understand the expected response.

Executive Intelligence Brief Template

KEY JUDGMENT

State the conclusion in one or two sentences.

WHAT CHANGED

The material development, not a news digest.

EVIDENCE & CONFIDENCE

Strongest evidence, confidence level and important gaps.

ENTERPRISE IMPLICATION

Affected strategy, people, operations, suppliers, technology, financials or reputation.

SCENARIOS / ALTERNATIVES

Credible competing pathways where material.

WATCH / DECIDE

Indicators, thresholds, recommended decision or contingency.

Risk Intelligence Maturity Model & Executive Checklist

LEVEL	CHARACTERISTICS	EXECUTIVE MEANING
1 — Informational	Ad hoc news/reporting; weak decision linkage	High information, low insight
2 — Developing	Defined topics, some analysis and exposure mapping	Useful but inconsistent
3 — Managed	PIRs, analytic standards, warning and executive products	Repeatable decision support
4 — Adaptive	Integrated indicators, scenarios, feedback and learning	Intelligence shapes strategic timing

Executive Checklist

☐ Intelligence mandate and sponsor defined

☐ Priority intelligence requirements approved

☐ Material enterprise exposures mapped

☐ Source and validation standards operating

☐ Assessments distinguish fact, judgment and confidence

☐ Alternative views considered for consequential issues

☐ Indicators and escalation thresholds defined

☐ Executive products lead with business implications

☐ Collection and privacy practices governed

☐ Decision outcomes feed back into intelligence improvement

Yakamichi Perspective

The strongest intelligence capability does not attempt to know everything. It knows which uncertainties matter, gathers the right evidence, challenges its own assumptions and gives leaders enough warning to preserve choice.

REQUEST A CONFIDENTIAL CONSULTATION

United States: +1 202 413 3763 | Maryland, USA
Nigeria: +234 811 095 0651 | Abuja, Nigeria

YAKAMICHI • Artificial Intelligence • Cybersecurity • Counter-Surveillance • Corporate Risk Intelligence