Corporate Intelligence Operating Model

A practical operating model for building an enterprise intelligence capability that converts external change, threat and uncertainty into executive advantage.

DIRECT	COLLECT	ANALYZE	DELIVER	DECIDE	LEARN
Requirements	Evidence	Judgment	Insight	Action	Feedback

EXECUTIVE PURPOSE
Establish the mandate, people, processes, governance, technology and products required to make intelligence a repeatable enterprise capability rather than an ad hoc research function.

YAKAMICHI PERSPECTIVE

Corporate intelligence earns its place when leaders use it before decisions, not merely after events.

Contents & Operating Model

OPERATING MODEL PRINCIPLE

Design the function around the decisions it must improve. Structure, staffing and technology should follow the intelligence requirements, not precede them.

Mandate, Scope & Intelligence Charter

A corporate intelligence function requires an explicit mandate defining what it exists to support, what it may collect, which activities are prohibited and how its work connects to enterprise governance.

CHARTER ELEMENT	DEFINITION
Purpose	Decisions and enterprise outcomes the function supports
Scope	Geographies, threats, markets, competitors, suppliers and strategic issues
Customers	Board, executives, security, strategy, operations and other authorized users
Authority	Approved information sources and internal access
Boundaries	Legal, privacy, ethical and corporate restrictions
Escalation	Conditions requiring executive, legal or security attention
Assurance	Quality, audit, review and performance expectations

- Name an executive sponsor.
- Define the intelligence leader's authority and accountability.
- Separate legitimate corporate intelligence from covert or unlawful activity.
- Specify handling requirements for confidential and sensitive information.
- Review the charter when strategy, geography or enterprise exposure changes.

CHARTER TEST

If the function cannot explain what it is authorized to do and what it will not do, the operating model is incomplete.

Customers, Decisions & Intelligence Requirements

The intelligence cycle begins with customers and decisions. Requirements should capture uncertainty that matters to strategy, protection, investment, resilience or operations.

CUSTOMER	TYPICAL DECISION
Board	Strategic risk, market exposure and material threats
CEO / Executive Committee	Investment, expansion, response and prioritization
Strategy / M&A	Market entry, transaction assumptions and competitive position
Security	Threat, protective intelligence and incident anticipation
Operations	Supply, geography, disruption and continuity
Legal / Compliance	Regulatory, jurisdictional and integrity exposure

Requirement Hierarchy

Priority Intelligence Requirements Executive questions whose answers materially affect enterprise decisions.

Standing Requirements Recurring intelligence needs that remain relevant over time.

Requests for Information Specific short-duration questions supporting an immediate issue.

Indicators Observable developments that signal a scenario or risk is changing.

CUSTOMER PRINCIPLE

Intelligence requirements should be agreed with decision-makers, not inferred indefinitely by analysts.

Organization, Roles & Talent

ROLE	CORE RESPONSIBILITY
Head of Intelligence	Mandate, priorities, executive relationships and quality
Requirements Manager	PIRs, customer engagement and tasking
Collection Manager	Source strategy, gaps, validation and provider coordination
Analyst	Structured analysis, warning and intelligence products
OSINT / Research Specialist	Lawful open-source discovery and verification
Data / Technology Specialist	Data integration, automation and analytic tooling
Knowledge Manager	Archive, taxonomy, retrieval and institutional memory

Talent Profile

- Analytical reasoning and intellectual humility.
- Clear executive writing and briefing.
- Source evaluation and verification.
- Business and enterprise-risk literacy.
- Regional, sector or technical specialization where required.
- Understanding of privacy, legal and ethical boundaries.
- Ability to challenge assumptions without becoming argumentative.

ORGANIZATION PRINCIPLE

A small function with strong requirements discipline and executive access can outperform a large team producing disconnected research.

Collection Management & Source Governance

Collection management converts intelligence requirements into an evidence plan. The objective is to close important information gaps using lawful, proportionate and reliable sources.

COLLECTION STEP	OUTPUT
Requirement decomposition	Specific information needs
Source mapping	Potential internal, official, commercial, expert and open sources
Tasking	Who or what will collect each information need
Validation	Reliability, provenance, corroboration and limitations
Gap review	What remains unknown and why
Re-tasking	New collection based on analytic findings

Source Governance

- Maintain provenance for consequential reporting.
- Distinguish primary evidence from secondary repetition.
- Record commercial provider limitations and licensing conditions.
- Protect confidential sources and internal information appropriately.
- Avoid collecting personal information without a legitimate, authorized purpose.
- Review source quality after major analytic errors or surprises.

COLLECTION PRINCIPLE

Collection is not browsing. It is a managed process for acquiring evidence against defined information gaps.

Analytic Standards & Quality Control

STANDARD	EXPECTATION
Objectivity	Evidence is not selected to fit a preferred outcome
Transparency	Judgments, assumptions and confidence are visible
Alternatives	Credible competing explanations are considered
Relevance	Analysis connects to enterprise exposure and decisions
Timeliness	Insight arrives while decision options still exist
Consistency	Common estimative language and review standards
Learning	Outcomes are compared with prior assessments

Analytic Review

- Is the key judgment supported by the strongest available evidence?
- Are facts separated from assessment?
- Are important assumptions explicit?
- Is confidence calibrated to source quality and information gaps?
- Has a credible alternative been considered?
- Does the product explain why the issue matters to the enterprise?
- What would cause the judgment to change?

QUALITY PRINCIPLE

Analytic confidence should survive challenge because the reasoning is visible, not because the analyst sounds certain.

Intelligence Products & Dissemination

PRODUCT	USE
Flash Intelligence Alert	Immediate material development requiring awareness
Executive Intelligence Brief	Concise judgment, implication and watch indicators
Daily / Weekly Digest	Curated developments tied to priority requirements
Risk Outlook	Forward view of priority threats and enterprise exposure
Scenario Assessment	Alternative futures, indicators and strategic options
Decision Support Note	Focused intelligence for a named decision
Board Intelligence Brief	Material strategic changes, assumptions and decisions

Dissemination Rules

- Match product length and cadence to the decision-maker.
- Lead with judgments and enterprise implications.
- Use classification and need-to-know appropriate to sensitivity.
- Maintain distribution records for highly sensitive products.
- Avoid flooding executives with low-value alerts.
- Create feedback channels so products evolve with customer needs.

PRODUCT PRINCIPLE

The intelligence product is an interface between analysis and action. Design it for the person who must decide.

Technology, Data & Knowledge Management

Technology should improve discovery, verification, collaboration, analysis and retrieval while preserving security, provenance and human judgment.

CAPABILITY	OPERATING REQUIREMENT
Source ingestion	Approved feeds and controlled data acquisition
Search / discovery	Fast retrieval across authorized sources
Entity / relationship analysis	Connect people, companies, events and dependencies
Alerting	Indicators linked to priority requirements and thresholds
Collaboration	Secure analyst workflow and review
Knowledge repository	Searchable assessments, sources and decision history
AI assistance	Governed summarization, classification and analytic support with human review

AI in Intelligence

- Use AI to accelerate processing, not to conceal source uncertainty.
- Require human validation for consequential judgments.
- Protect sensitive information when using external AI services.
- Preserve source provenance through AI-assisted workflows.
- Test for hallucination, bias and automation overconfidence.
- Define which intelligence tasks may not be delegated to autonomous systems.

TECHNOLOGY PRINCIPLE

Tools should reduce analyst friction and increase evidence quality. They should not create an automated fog of unverified content.

Governance, Ethics, Security & Legal Boundaries

AREA	CONTROL
Legal authority	Collection and processing have a legitimate corporate purpose
Privacy	Personal data is minimized and appropriately protected
Ethics	No deception, harassment or intrusive conduct outside authorized lawful practice
Information security	Sensitive sources, assessments and identities are access-controlled
Conflicts	Analyst/provider conflicts are disclosed
Retention	Records follow approved lifecycle and legal requirements
Escalation	Suspected criminal, security or integrity concerns move to appropriate functions

Prohibited or Restricted Conduct

- Unauthorized access to systems or accounts.
- Impersonation or deceptive collection outside lawful approved activity.
- Acquisition of unlawfully obtained personal or confidential data.
- Harassment, stalking or intrusive surveillance.
- Circumvention of legitimate security or law-enforcement controls.
- Intelligence activity used for personal, political or discriminatory purposes.

ETHICS PRINCIPLE

Corporate intelligence protects enterprise decision quality. It loses legitimacy the moment information advantage is pursued without lawful authority and ethical discipline.

Performance, Maturity & Executive Assurance

Performance should measure decision relevance, warning and analytic quality rather than report volume.

METRIC	WHAT IT REVEALS
PIR coverage	Whether priority questions are being answered
Warning lead time	Whether insight arrives before decision windows close
Executive utilization	Whether products inform actual decisions
Analytic accuracy review	How judgments perform against outcomes
Source gap closure	Whether important information gaps are improving
Customer feedback	Relevance, clarity and timeliness
Remediation / learning	Whether errors and surprises change the operating model

Assurance Questions

- Are intelligence priorities aligned to enterprise strategy?
- Does the function operate within documented authority?
- Can major judgments be traced to evidence?
- Are alternative views encouraged?
- Are sensitive records protected?
- Does leadership receive warning early enough to act?
- Are analytic failures reviewed without creating a blame culture?

PERFORMANCE PRINCIPLE

The best measure of intelligence is not whether every forecast was correct. It is whether leaders were better prepared for consequential uncertainty.

180-Day Corporate Intelligence Build Program

WINDOW	PRIORITY	DELIVERABLES
0–30 Days	Mandate	Executive sponsor, charter, customers and initial PIRs
31–60 Days	Operating structure	Roles, workflow, source register and collection plan
61–90 Days	Analytic standard	Tradecraft guide, confidence language and quality review
91–120 Days	Products & technology	Product catalogue, repository, alerting and secure collaboration
121–150 Days	Executive integration	Briefing cadence, scenarios and decision-support workflow
151–180 Days	Assurance	Metrics, customer feedback, maturity assessment and 12-month roadmap

Day-180 Outcomes

- The function has a documented mandate and executive sponsor.
- Priority intelligence requirements drive work.
- Collection is managed against information gaps.
- Analytic standards are repeatable.
- Executives receive a defined product suite.
- Sensitive intelligence is appropriately governed.
- Performance is measured through decision relevance and learning.

BUILD PRINCIPLE

Do not wait to build a perfect intelligence center. Establish the minimum viable operating model, prove decision value, then scale where demand and consequence justify it.

Corporate Intelligence Charter Template

FIELD	CHARTER ENTRY
Purpose	____________
Executive sponsor	____________
Customers	____________
Authorized scope	____________
Collection authorities	____________
Restricted / prohibited activities	____________
Information handling	____________
Escalation	____________
Review cycle	____________

PIR & Requirements Register

ID	REQUIREMENT	OWNER	HORIZON	INDICATORS / DECISION
PIR-01	______________	_______	_______	______________
PIR-02	______________	_______	_______	______________
PIR-03	______________	_______	_______	______________
PIR-04	______________	_______	_______	______________

Collection Management Plan

INFORMATION NEED	SOURCE	OWNER	VALIDATION	GAP / STATUS
____________	____________	______	____________	____________
____________	____________	______	____________	____________
____________	____________	______	____________	____________
____________	____________	______	____________	____________

Analytic Quality Review

- ☐ Key judgment is explicit
- ☐ Material facts are sourced
- ☐ Facts and assessments are distinguishable
- ☐ Assumptions are visible
- ☐ Confidence is stated and justified
- ☐ Credible alternatives are considered
- ☐ Information gaps are identified
- ☐ Enterprise implications are clear
- ☐ Indicators that could change the judgment are stated
- ☐ Product is timely for the decision

Reviewer Notes

____

____

____

____

Corporate Intelligence Product Catalogue

PRODUCT	AUDIENCE	CADENCE	MAXIMUM PURPOSE
Flash Alert	Executives / relevant owners	Event-driven	Immediate material change
Executive Brief	Senior leaders	As required	Decision-relevant assessment
Intelligence Digest	Defined users	Daily / weekly	Curated priority developments
Risk Outlook	Executives / risk	Monthly / quarterly	Forward risk and warning
Scenario Assessment	Strategy / executives	Periodic	Alternative futures and options
Board Brief	Board / committee	Quarterly / event	Material strategic intelligence

Corporate Intelligence Maturity Model & Executive Checklist

LEVEL	CHARACTERISTICS	EXECUTIVE MEANING
1 — Ad Hoc	Individual research, weak requirements and inconsistent products	Information without operating discipline
2 — Developing	Charter, initial PIRs, analysts and recurring products	Useful but uneven capability
3 — Managed	Requirements, collection, analytic standards, governance and metrics	Repeatable enterprise intelligence
4 — Adaptive	Integrated warning, scenarios, AI-enabled workflows and decision feedback	Intelligence shapes strategic timing

Executive Checklist

☐ Executive sponsor and intelligence charter approved

☐ Customers and decision requirements defined

☐ PIR register operating

☐ Roles and talent model established

☐ Collection plan and source governance operating

☐ Analytic standards and quality review established

☐ Product catalogue and dissemination rules defined

☐ Technology and knowledge repository governed

☐ Legal/privacy/ethical boundaries documented

☐ Performance and maturity reviewed with executives

Yakamichi Perspective

Corporate intelligence is not a newsroom inside the enterprise. It is a decision system: requirements focus attention, evidence reduces uncertainty, analysis creates judgment and feedback turns experience into institutional advantage.

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