CYBER RISK ASSURANCE & RESILIENCE

AI Governance & Cyber Risk Readiness Assessment

Secure the AI. Govern the Agent. Assure the Outcome.

A structured, board-ready assessment of where artificial intelligence is already operating inside your organization — and what it means for your data, your controls, your regulatory exposure and your cyber risk profile.

01 — SERVICE OVERVIEW

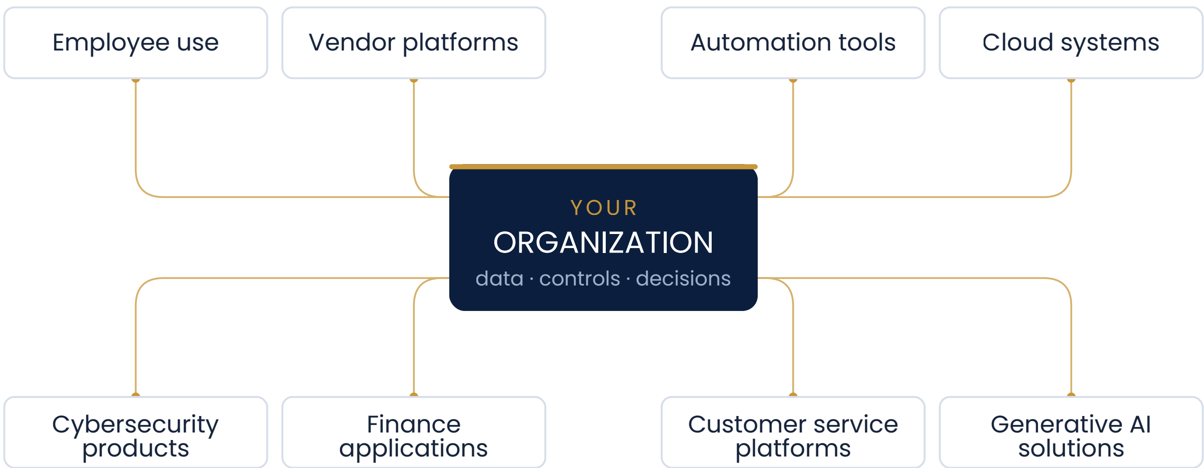
AI is already in your organization. The question is whether it is governed.

Artificial Intelligence is already entering organizations through employee use, vendor platforms, automation tools, cloud systems, cybersecurity products, finance applications, customer service platforms, and generative AI solutions.

> *The opportunity is significant, but so is the risk. Without proper governance, AI can expose confidential data, produce unreliable outputs, weaken internal controls, increase cyber risk, create regulatory exposure, and undermine board confidence.*

Dawgen Global's **AI Governance & Cyber Risk Readiness Assessment** helps organizations understand their current AI exposure and build a practical roadmap for secure, responsible, and assurance-ready AI adoption.

HOW AI ENTERS THE ORGANIZATION



MOST AI EXPOSURE ARRIVES WITHOUT A FORMAL ADOPTION DECISION — WHICH IS PRECISELY WHY IT GOES UNMAPPED, UNCLASSIFIED AND UNREPORTED

TYPICAL DURATION	DELIVERY MODEL	OUTPUT
2 to 4 weeks	**Hybrid, digital or onsite**	**Executive report, roadmap & briefing**

02 — WHY THIS MATTERS

Six questions the board should be able to have answered

Boards and audit committees are increasingly expected to demonstrate oversight of AI — not to understand the technology, but to know where it sits, what it touches, and who is accountable for it. These are the questions the assessment is designed to answer.

01
Where is AI being used across the organization?

02
What data is being entered into AI systems?

03
Are AI tools approved, monitored, and governed?

04
Are AI vendors using organizational data?

05
Are cybersecurity controls adequate for AI-enabled systems?

06
Can management provide assurance to the board?

> *Where these questions cannot be answered with evidence, the organization is not making a decision about AI risk — it is inheriting one.*

THE GAP THE ASSESSMENT IS DESIGNED TO CLOSE

AI capability enters an organization faster than the policies, controls, vendor terms and reporting lines that are meant to govern it. The assessment measures that distance and converts it into a prioritized, ownable set of actions.

03 — OUR ASSESSMENT COVERS

Seven review areas, one integrated view

AI Usage Discovery	Identify formal and informal AI use across business units, including generative AI tools, AI-enabled platforms, vendor systems, automation tools, and emerging AI agents.
AI Risk Classification	Classify AI use cases based on business impact, data sensitivity, regulatory exposure, cybersecurity risk, autonomy level, and potential stakeholder harm.
Cybersecurity Exposure Review	Assess AI-related cyber risks, including data leakage, prompt injection, unauthorized tool use, insecure integrations, access control weaknesses, and AI-enabled vendor exposure.
Data Governance and Privacy Review	Evaluate how personal, confidential, financial, customer, employee, and regulated data may be accessed, processed, stored, or transmitted through AI systems.
AI Governance Maturity Review	Assess current policies, procedures, approval workflows, accountability structures, risk ownership, monitoring, reporting, and board oversight.
AI Vendor Risk Screening	Review exposure from third-party platforms that may already include embedded AI capabilities.
Board and Management Reporting	Provide a practical executive report with key risks, control gaps, maturity rating, and prioritized recommendations.

Each area is assessed against the same standard: can the position be evidenced, owned by a named party, and reported to the board with confidence?

ANCHORED IN RECOGNIZED FRAMEWORKS

NIST CSF 2.0

Govern, Identify, Protect, Detect, Respond and Recover — extended to AI-specific exposure and data flows.

IIA Cybersecurity Topical Requirement

Governance, risk management and control process expectations that internal audit functions are now measured against.

Your own policy set

Findings are mapped back to your existing policies, delegations and board reporting calendar — not to a generic template.

04 — KEY DELIVERABLES

Findings you can act on — and report

01 AI usage and exposure summary

02 AI risk heat map

03 Cybersecurity and data protection gap analysis

04 AI governance maturity scorecard

05 Vendor AI exposure review

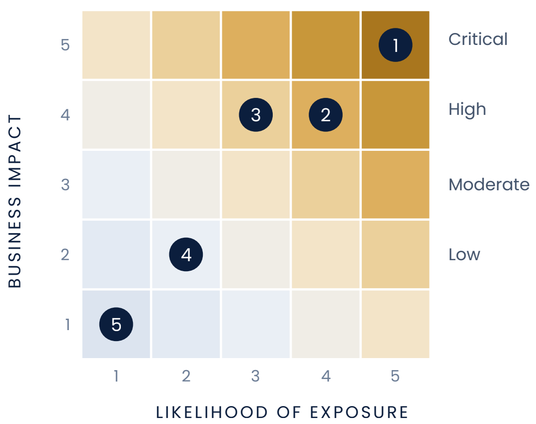
06 Priority remediation roadmap

07 Board-ready executive summary

Every deliverable is written for two audiences at once: the technical owners who must fix the issue, and the board that must oversee it.

AI risk heat map

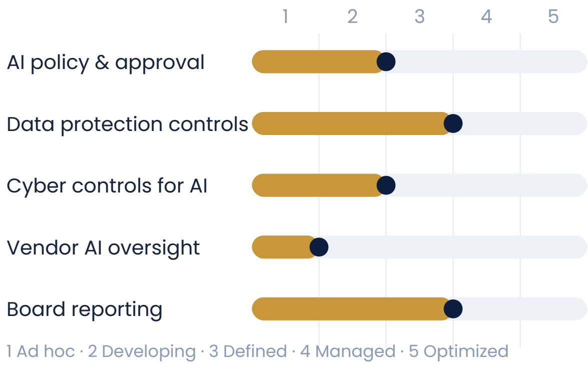
ILLUSTRATIVE OUTPUT



1 Generative AI in customer communications · 2 AI-assisted credit and underwriting · 3 Vendor platform with embedded AI · 4 Automated document drafting · 5 Internal productivity tools

Governance maturity scorecard

ILLUSTRATIVE OUTPUT



Overall maturity rating DEVELOPING

Each dimension is rated on a five-level scale, with the gap to the next level expressed as specific, owned actions in the remediation roadmap.

Priority remediation roadmap

ILLUSTRATIVE EXTRACT

PRIORITY	ACTION	OWNER	TARGET
CRITICAL	Approved AI use policy and tool register issued	Chief Risk Officer	30 days
HIGH	Vendor contracts reviewed for AI data-use clauses	Procurement / Legal	60 days
MODERATE	Quarterly AI exposure reporting added to board pack	Company Secretary	90 days

05 — WHO SHOULD CONSIDER THIS SERVICE

Built for regulated, data-rich and stakeholder-accountable entities

- Financial institutions
- Credit unions and insurance companies
- Public sector entities
- Utilities and telecoms
- Healthcare and education institutions
- Manufacturing, distribution, retail and professional service firms

06 — BENEFITS TO YOUR ORGANIZATION

From uncertainty to a governed position

- ✓ Gain visibility over AI use and exposure
- ✓ Reduce data leakage and cyber risk
- ✓ Strengthen board and audit committee oversight
- ✓ Prepare for regulatory and stakeholder scrutiny
- ✓ Build a practical AI governance roadmap
- ✓ Support responsible AI adoption

COMMON TRIGGERS FOR THIS ASSESSMENT

Staff are already using generative AI tools, with no approved policy behind them.

A vendor has added AI features to a platform that holds your data.

The board or audit committee has asked a question no one can evidence.

A regulator, insurer or counterparty has begun asking about AI controls.

07 — ENGAGEMENT FORMAT

A short, disciplined engagement with a defined end point

Typical duration: 2 to 4 weeks | **Delivery model:** Hybrid, digital or onsite as required | **Output:** Executive report, risk roadmap, and management briefing

WEEK 1	WEEK 1–2	WEEK 2–3	WEEK 3–4
01	02	03	04
Mobilize	Discover	Assess	Report
Scope, stakeholders, information request	AI usage discovery, data flows, vendor screening, interviews	Risk classification, cyber and privacy gaps, maturity rating	Executive report, roadmap, management briefing

> *The assessment is scoped so that it does not compete with the operating calendar. It begins with what you already have, and ends with a document the board can use.*

08 — WHY DAWGEN GLOBAL

Independent. Integrated. Caribbean.

An independent firm

Dawgen Global is an independent, integrated multidisciplinary professional services firm — not affiliated with any international network. Our judgement is our own.

Assurance-led, not tool-led

We do not sell the AI platforms we assess. That independence is what makes the resulting report usable as evidence.

Multidisciplinary by design

Audit & Assurance, Cybersecurity, IT & Digital Transformation, Risk Management and Advisory work from a single engagement view.

Regional reach and context

Headquartered in New Kingston, Jamaica and operating across 15+ Caribbean territories, with an understanding of local regulatory and board expectations.

CALL TO ACTION

Begin the conversation

Is your organization using AI without a clear governance and cyber risk framework? Contact Dawgen Global today to request an AI Governance & Cyber Risk Readiness Assessment.

REQUEST THE ASSESSMENT

EMAIL
info@dawgen.global

WHATSAPP GLOBAL
+1 555-795-9071

ONLINE
dawgen.global/contact-us

HEAD OFFICE
47 Trinidad Terrace
New Kingston, Jamaica

JAMAICA
876-929-3670
876-665-5926

UNITED STATES
855-354-2447

Secure the AI. Govern the Agent. Assure the Outcome.

ONE FIRM. MANY DISCIPLINES.

Audit & Assurance · Tax Advisory · IT & Digital Transformation · Risk Management · Cybersecurity · HR Advisory · Mergers & Acquisitions · Corporate Recovery · Business Advisory · Accounting BPO & Virtual CFO · Legal Process Outsourcing

Dawgen Global is an independent, integrated multidisciplinary professional services firm serving clients across 15+ Caribbean territories. Big Firm Capabilities. Caribbean Understanding.