Dawgen GLOBAL

CYBER RISK ASSURANCE & RESILIENCE

Cybersecurity & AI Continuous Control Monitoring

Move from annual reviews to standing confidence.

Ongoing visibility over cyber risk, AI exposure, control exceptions, vendor issues, data leakage risk, and remediation progress — reported to management and the board on a fixed cadence.

01 — SERVICE OVERVIEW

Cyber and AI risks do not wait for annual assessments.

Threat actors adapt, systems change, vendors update platforms, users adopt new tools, and AI models evolve.

> *A control environment that is reviewed only once per year may not provide sufficient confidence.*

Dawgen Global's **Cybersecurity & AI Continuous Control Monitoring** service helps organizations maintain ongoing visibility over cyber risk, AI exposure, control exceptions, vendor issues, data leakage risk, and remediation progress.

ONE POINT OF EVIDENCE, OR TWELVE

ANNUAL ASSESSMENT

one point of evidence

eleven months in which the position is assumed, not known

CONTINUOUS MONITORING

exceptions surfaced when they occur · remediation tracked to closure · the board sees the same picture management does

The question is never "was it fine last November?" It is "as of when?"

TYPICAL FORMAT

Monthly or quarterly managed service

DELIVERY MODEL

Remote monitoring & management meetings

OUTPUT

Recurring Cyber & AI Control Monitoring Report

WHAT CAN CHANGE BETWEEN TWO ANNUAL ASSESSMENTS

A vendor adds AI capability to a platform holding your data.

A privileged account is created for a project and never removed.

Staff adopt a generative AI tool nobody has approved.

An assurance report expires and is not replaced.

02 — WHY THIS MATTERS

Nine exposures that change between assessments

Each of these can appear, worsen or resolve inside a single reporting period. None of them announces itself. All of them are visible if somebody is looking on a fixed cadence.

- Generative AI data leakage
- Shadow AI usage
- Vendor AI exposure
- Prompt injection
- Insecure integrations
- Access control weaknesses
- AI-enabled cyber threats
- Weak incident response
- Limited board visibility

> *An annual assessment tells you the position on one date. Everything after that date is an assumption — and assumptions are what incidents are built on.*

03 — OUR ASSESSMENT COVERS

Seven monitoring areas, one cadence

Cyber Risk Monitoring	Monitor key cyber control indicators, including vulnerabilities, access exceptions, phishing exposure, endpoint risk, privileged access, patch status, and incident trends.
AI Usage and Exposure Monitoring	Track approved and unapproved AI tools, high-risk AI use cases, data exposure indicators, and policy exceptions.
Vendor and Third-Party Risk Monitoring	Review changes in high-risk vendors, AI-enabled platforms, assurance reports, security issues, and contract-related risk areas.
Access and Identity Review	Assess whether access rights, privileged accounts, AI agent permissions, and user roles remain appropriate.
AI Audit Trail and Evidence Review	Review whether AI-supported processes maintain sufficient logs, approvals, validation records, and exception reports.
Incident Response Readiness	Assess readiness to respond to cyber and AI-related incidents, including data leakage, unauthorized AI actions, harmful outputs, or vendor breaches.
Executive Dashboard Reporting	Provide management and board-level dashboards with risk indicators, exceptions, remediation status, and priority actions.

> *The value is not in the individual indicator. It is in seeing the same indicators, in the same format, period after period — so that movement is obvious.*

ANCHORED IN RECOGNIZED FRAMEWORKS

NIST CSF 2.0

Govern, Identify, Protect, Detect, Respond and Recover — with Detect and Respond monitored continuously rather than annually.

IIA Cybersecurity Topical Requirement

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

Your own reporting calendar

The cadence is set to your board and audit committee cycle — the pack arrives before the meeting, not after it.

04 — KEY DELIVERABLES

The same picture, every cycle

01 Monthly or quarterly cyber and AI control dashboard

02 Exception and remediation tracker

03 AI usage and exposure monitoring summary

04 Vendor risk watchlist

05 Access control review summary

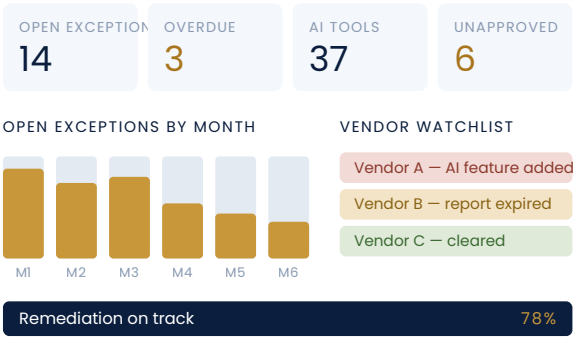
06 Incident readiness observations

07 Board and audit committee reporting pack

Nothing is rebuilt each period. The format holds, so the only thing that changes is the position — which is the point.

Cyber & AI control dashboard

ILLUSTRATIVE OUTPUT



Reported monthly or quarterly · same picture for management and the board

Exception and remediation tracker

ILLUSTRATIVE EXTRACT

EXCEPTION	OWNER	STATUS
Privileged accounts not reviewed	IT	OVERDUE
Unapproved AI tool in finance	CFO	IN PROGRESS
Vendor assurance report expired	Procurement	IN PROGRESS
Patch backlog above threshold	IT	CLOSED
AI log retention below policy	CIO	CLOSED

Open items are carried forward until closed. Nothing falls off the list because a reporting period ended.

AI usage and exposure monitoring summary

ILLUSTRATIVE EXTRACT

CATEGORY	APPROVED	UNAPPROVED	EXPOSURE
Generative AI assistants	4	3	CLIENT DATA
Embedded vendor features	11	2	UNDER REVIEW
Automation and agents	6	1	UNDER REVIEW
Productivity tools	10	0	LOW

05 — WHO SHOULD CONSIDER THIS SERVICE

For organizations that need the capability without the headcount

- Organizations without a full internal cyber governance team
- Boards requiring regular cyber and AI visibility
- Regulated entities
- Credit unions and financial institutions
- Public sector agencies
- Utilities and telecoms
- SMEs with high data sensitivity

06 — BENEFITS TO YOUR ORGANIZATION

From periodic comfort to standing confidence

- ✓ Move beyond periodic assessments
- ✓ Improve cyber and AI risk visibility
- ✓ Support board and audit committee oversight
- ✓ Detect control exceptions earlier
- ✓ Track remediation progress
- ✓ Strengthen regulatory readiness

COMMON TRIGGERS FOR THIS SERVICE

The last assessment surfaced findings that nobody has tracked since.

The board wants cyber and AI on the agenda every quarter, not once a year.

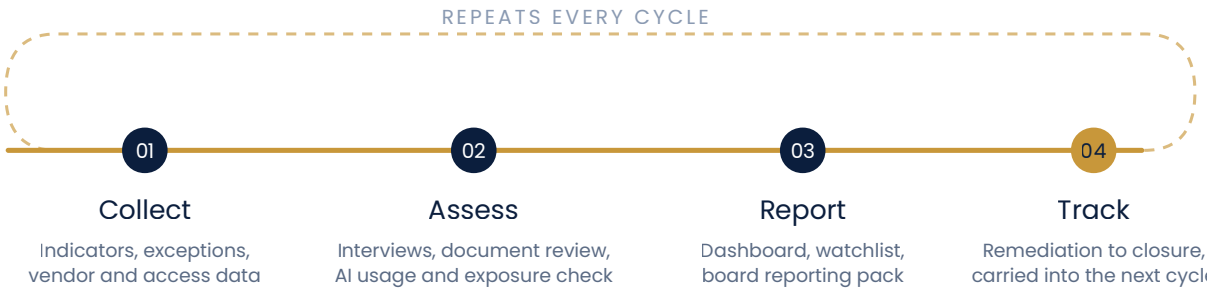
There is no internal capacity to monitor between assessments.

A regulator has asked how exceptions are identified and closed.

07 — ENGAGEMENT FORMAT

A managed advisory service on a fixed cadence

Typical format: Monthly or quarterly managed advisory service | **Delivery model:** Remote monitoring, interviews, document review, dashboard reporting, and management meetings | **Output:** Recurring Cyber & AI Control Monitoring Report



> *There is no mobilisation to repeat and no relationship to rebuild. Each cycle starts from the last one, which is what makes the trend meaningful.*

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.

We monitor; we do not operate

We do not run the systems we report on. That separation is what allows the dashboard to be used as evidence rather than as self-assessment.

Capability without headcount

A standing capability for organizations that cannot justify a full internal cyber governance team — at a cadence you set.

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

Are you relying on annual cyber assessments while AI and cyber risks change every day? Contact Dawgen Global today to request a Cybersecurity & AI Continuous Control Monitoring Consultation.

REQUEST A CONSULTATION

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

Move from annual reviews to standing confidence.

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

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