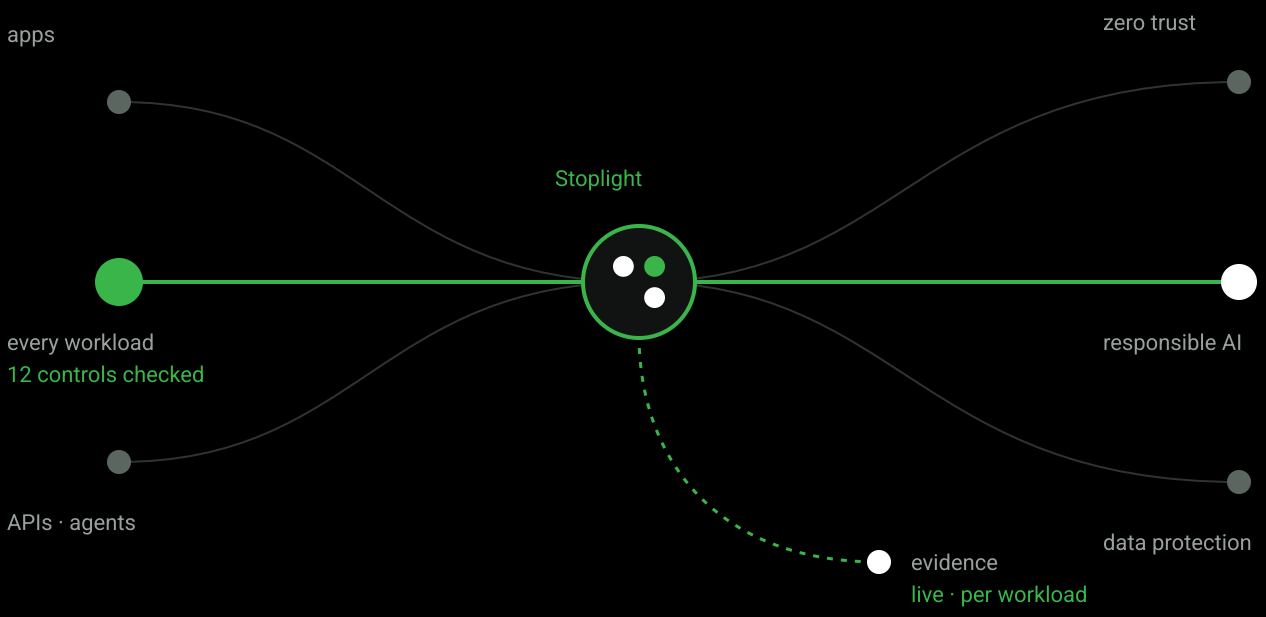
Greymatter.io

WHITE PAPER
GREYMATTER 2.5.0 · NOVEMBER 2026



Stoplight: score every app, API and agent against the standards

How Greymatter checks twelve controls on every workload it manages, lays recognized frameworks over them, and shows the evidence live.

© 2026 Greymatter.io, Inc.

Contents

	SECTION		PAGE
THE CASE	1	Executive summary	1
	2	Snapshots fall behind	3
	3	Evidence from every stage of the path	4
THE STOPLIGHT SCORECARD	4	One page, twelve controls	6
	5	How each control is judged	9
	6	Frameworks laid over the controls	10
	7	Readiness against a maturity model	13
	8	Support for the rest of the stack	14
EVIDENCE	9	Evidence an assessor can take away	15
	10	Faster assessment inside your boundary	16
	11	Twenty-three frameworks, one set of controls	18
	12	Limits, stated precisely	20
PROOF	13	Evidence for security frameworks	21
	14	Operational and mission benefits	22
	15	Ask Greymatter	23

How to read the status marks

Every capability in this paper carries one mark. Nothing marked Fielded is aspirational.

FIELDED

Ships in Greymatter 2.5.0 today.

PREVIEW

Ships in 2.5.0 as a technology preview.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

1

Executive summary

Greymatter checks twelve security controls on every app, API and agent it manages, around the clock. One page shows where each control stands and which standards it supports.

IN BRIEF

Stoplight, the Greymatter scorecard, measures the platform itself, not a questionnaire about it. Each number comes from the traffic, certificates and configuration Greymatter already manages.

WHO THIS IS FOR

CIOs, CISOs and heads of IT and software, who must run many apps safely. Also program offices, authorizing officials and assessors, who must show that controls are in place everywhere, today.

Most compliance evidence is a snapshot. A team fills in a spreadsheet, gathers screenshots, and attests that a control is in place. By the time an assessor reads it, the system has changed. New services ship, certificates expire and a team turns a setting off.

Greymatter measures instead. Its scorecard, called Stoplight, checks twelve controls on every workload it manages. They cover identity, certificate renewal, encryption, validated cryptography and who may call each service. They also cover protection at every edge, AI guardrails, sensitive data detection, the audit trail, policy reach, change logging and Console access. Each control shows how many workloads and edges it covers, of how many it applies to.

Stoplight then lays recognized frameworks over those controls. A reader picks a framework and sees each pillar, mandate or article with the controls it rests on. Where another tool owns a part, Stoplight says so.

Greymatter runs inside the boundary an organization already accredits. Every stage of its security path supplies evidence, so each assessment starts from live reads and the ongoing forensic audit, not screenshots.

THE CENTRAL POINT

Compliance becomes a reading of the live system, for every workload, not a claim about it.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Six properties a program office can test

Measured, not attested

FIELDED

Every count comes from the platform itself: certificates, listeners, filters and configuration.

Every workload

FIELDED

Each control counts the services or edges it covers, of how many it applies to.

Live

FIELDED

The page refreshes on its own and says when it last read the platform.

Mapped to standards

FIELDED

23 frameworks in eight groups, from ISO/IEC 27001 to the EU AI Act, laid over the controls.

Evidence on demand

FIELDED

Each control downloads its rows as a file. The whole page prints as a report.

Honest about gaps

FIELDED

A control that could not be read says so. It never shows as zero or as in place.

STATED PRECISELY, SO IT IS NOT OVER-READ

Stoplight shows where the Greymatter controls are in place. It does not certify a system against any framework. The mapping from controls to frameworks is guidance that an assessor can check.

Some controls count only the workloads that turn them on, such as AI guardrails and sensitive data detection.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

2 Snapshots fall behind

A control that was in place at audit time is not evidence that it is in place now, on every workload.

THE GAP

Attestation describes the system a team believes it runs. Measurement describes the system it does run.

THE COST

Each audit becomes a project. Engineers stop shipping to gather screenshots that are stale before anyone reads them.

Zero trust programs, federal mandates and data protection laws ask the same questions. Does every service have its own identity? Is every connection encrypted? Who may call what? Is there a trail of every request? Programs usually answer with documents.

Documents cover the services someone remembered. They do not cover the service a team deployed last week, the certificate that expires tomorrow, or the listener someone opened for a test. Coverage gaps hide between audits.

Greymatter already carries the traffic, issues the identities and holds the configuration. It can settle those questions from the system itself, for every workload, at any moment.

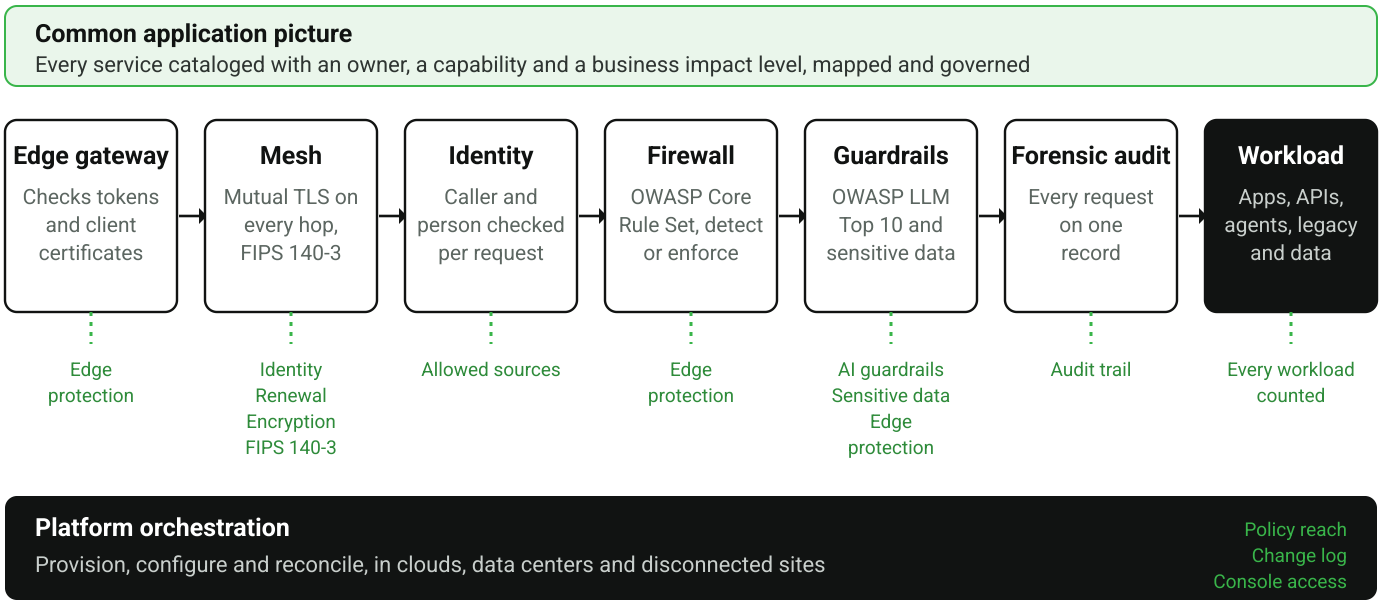
QUESTION	SNAPSHOT EVIDENCE	GREYMATTER EVIDENCE
Does every service have an identity?	A diagram and a policy	10 of 10 workloads and 7 of 7 edges, with a list of any that do not
Is traffic encrypted?	A configuration screenshot	Each service checked for mutual TLS and plaintext callers
Is there an audit trail?	A logging policy	Each service checked for the audit filter on its listener
When was this true?	The audit date	The time of the last read, refreshed continuously

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

3 Evidence from every stage of the path

Greymatter is the security path in front of each workload, not one stage of it. So every stage can supply evidence. **FIELDED**

FIGURE 1 · THE APPLICATION SECURITY PATH, AND THE STOPLIGHT CONTROLS EACH STAGE SUPPLIES



MANY ENVIRONMENTS

Workloads run in public and sovereign clouds, data centers and disconnected sites. The same path and the same controls apply in each.

MANY KINDS OF WORKLOAD

Apps, microservices, APIs, AI agents, long-lived legacy services and data services all sit behind the same path.

Point products each see one stage. A gateway sees the edge. A firewall sees web attacks. A logging tool sees what someone sent it. None of them can say whether every workload has every control.

Greymatter runs every stage, so it can. Each stage reports what it enforced into the same record and the same Stoplight scorecard. Green dotted lines in the figure show which control each stage supplies.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

LEAST PRIVILEGE BY DESIGN

Each workload admits only the callers it needs. The caller limits control counts which services narrow admission.

POLICY PER WORKLOAD

Each workload carries its own policy, written as code. The policy delivery control checks that it arrived.

A catalog, not a routing table

A routing registry knows where a service lives. An assessor also needs to know who owns it, what it does and what harm a failure causes. Greymatter keeps those facts in its catalog for each service, beside the controls that protect it.

Each catalog entry can carry an owner, a link to the owning team, a capability, documentation and a business impact level. The level is low unless a team sets it. An assessor can rank gaps by impact and send each one to its owner.

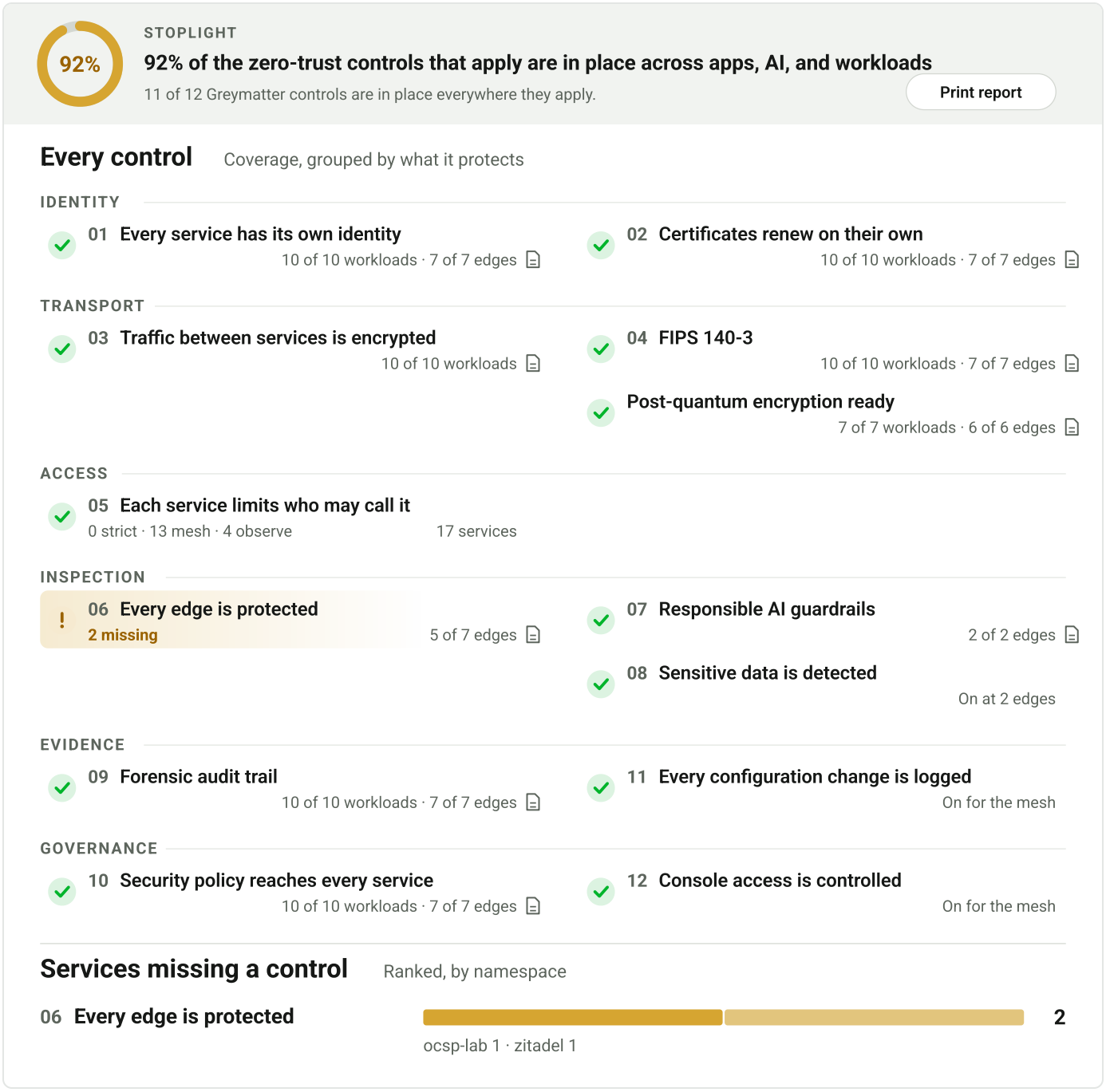
STAGE	WHAT IT ENFORCES	EVIDENCE IT SUPPLIES
Edge gateway	Checks of sign-in tokens and client certificates at the edge	The verified caller on every record
Mesh	Mutual TLS between every pair of workloads, with FIPS 140-3 validated cryptography	Identity, renewal, encryption and cryptography controls, per service
Identity	The calling workload and the person it acts for, checked on every request	Allowed sources, and the person and workload on each record
Firewall	The OWASP Core Rule Set, in detect or enforce mode	Edge protection, and every firewall decision on record
Guardrails	Checks of prompts, outputs, tools and sensitive data	AI guardrails and sensitive data controls, and each finding on record
Forensic audit	One record of every request	The audit trail control, and the rows an assessor reads
Management plane	Policy as code, sign-in to the Console through the identity provider, and a ledger of changes	Policy reach, change log and Console access controls

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

4 One page, twelve controls

Stoplight lists every control by what it protects, with how many workloads and edges it covers. FIELDED

FIGURE 2 · STOPLIGHT IN THE CONSOLE



© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

ONE SCORE

The ring shows the share of controls that apply and are in place. It never reads 100 while any control has a gap.

PRINT REPORT

The whole page prints as a report, or saves as a PDF. It carries the score, every control, every framework and the gaps.

The headline states how many controls are in place everywhere they apply. The controls are grouped by what they protect: identity, transport, access, inspection, evidence and governance. Stoplight lists them as a checklist. Each line carries a check mark when the control is in place, and counts workloads and edges apart, such as 10 of 10 workloads and 7 of 7 edges. A line with a gap is shaded and says how many are missing.

A panel ranks the controls that some service or edge lacks, most first. Each bar splits by the namespaces that hold the gap, so the owner of each gap is clear.

GREYMATTER APPLIES THE CONTROLS, THEN MEASURES YOUR OWN STACK

Greymatter puts these controls in place on its own, as workloads come and go. It issues each identity, renews each certificate, encrypts each connection and delivers each policy. The firewall, guardrails and DLP run wherever a team turns them on. Stoplight then shows, live, that each control is in place.

Most controls measure the apps, APIs and AI agents your teams already run, and name each one with a gap. Only the change log and Console access measure the Greymatter platform itself. A workload Greymatter does not manage still shows up, as a gap or as an unidentified peer.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

The twelve controls

CONTROL	IN PLACE WHEN	COUNTS
01 Every service has its own identity	Each service has its own certificate, issued by Greymatter	Workloads and edges
02 Certificates renew on their own	No certificate is expired, expiring or failing to rotate	Workloads and edges
03 Traffic between services is encrypted	The service requires mutual TLS and accepts no plaintext callers	Workloads
04 FIPS 140-3 and post-quantum cryptography	Validated cryptography. Post-quantum encryption ready, and active, each on its own line	Workloads and edges
05 Each service limits who may call it	The service runs in an access posture: observe, strict mesh or strict identity	Every service
06 Every edge is protected	A WAF in detect or enforce mode, Guardrails or DLP runs at the edge	Every tenant edge
07 Responsible AI guardrails	Guardrails inspect prompts, outputs, tools and agents	Where a team turns it on
08 Sensitive data is detected	DLP inspects the traffic	Where a team turns it on
09 Forensic audit trail	The audit filter records every request	Workloads and edges
10 Security policy reaches every service	No data plane has lost the management plane or drifted from policy	Workloads and edges
11 Every configuration change is logged	The change ledger is on and answering	The platform
12 Console access is controlled	People sign in through the identity provider, with roles from their groups	The platform

A service with no data plane, or with no running pod, is listed under the controls that apply to every service. An unmanaged workload shows up as a gap.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

5

How each control is judged

Only the Greymatter API decides whether a control is in place. The Console draws its result and decides nothing on its own. FIELDED

NEVER ZERO BY ACCIDENT

A count the API did not send is shown as not read, never as zero. A newer API cannot make an older Console show something in place.

NO DOUBLE COUNTING

Each control stands on its own reads. One failed read affects only the controls that need it.

Controls come in three kinds. **Always-on** controls apply to every service, such as identity, encryption and who may call each service. Every service in scope counts toward them, and an unmanaged one counts as a gap. Edge protection applies to every tenant edge in the same way. **Opt-in** controls apply where a team turns them on: AI guardrails and sensitive data detection. They count the services that turn them on. **Platform** controls have one result for the whole mesh, such as change logging and Console sign-in.

A control is in place when every workload it counts is in place. An opt-in control nobody turned on, or an always-on control with nothing measured yet, is neither in place nor a gap. It is left out of the score and says why on its card.

THE CARD SAYS	WHAT IT MEANS
In place	Every workload the control counts meets it
Not in place	Some workloads or edges do not meet it. The rows name them
Not configured	The control does not apply to this platform
Not turned on anywhere	No workload turns it on yet, so it is left out of the score
Not measured yet	Nothing is counted yet, so it is left out of the score
Not read	The source behind it did not respond. The card says so
Stale	The last result stands while a new read is pending, marked as stale

THE SCORE, STATED PRECISELY

The score is the share of applicable controls that are in place everywhere. While any applicable control has a gap, the score shows at most 99 percent, so a full ring always means no gap.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

6 Frameworks laid over the controls

Stoplight lays 23 frameworks over the same twelve controls, in one matrix. A square marks each control a framework rests on, in its live standing. FIELDED

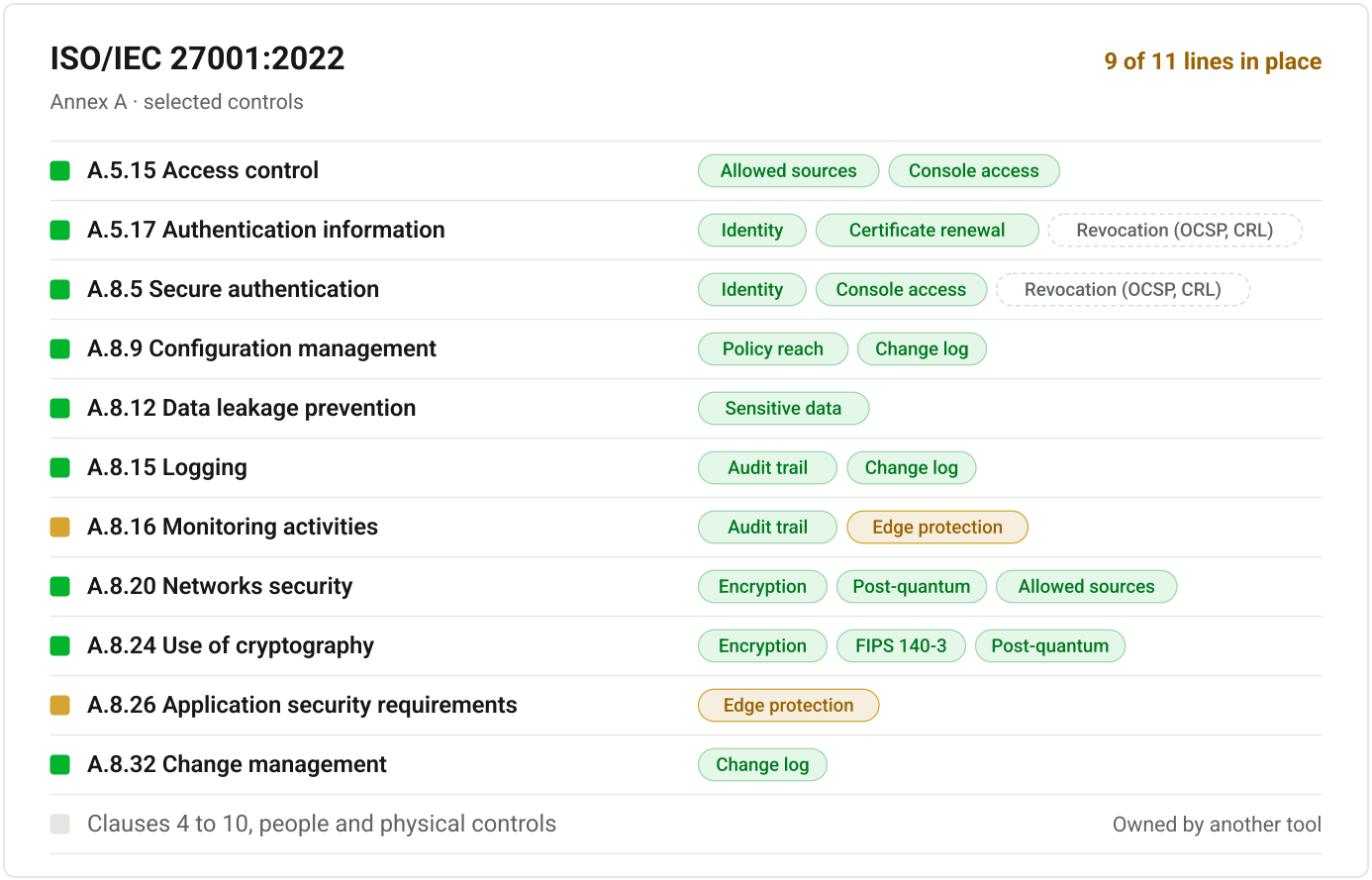
FIGURE 3 · THE COVERAGE MATRIX IN STOPLIGHT

		IDENTITY		TRANSPORT		ACCESS	INSPECTION			EVIDENCE		GOVERNANCE	
FRAMEWORK		01 Identity	02 Certificate renewal	03 Encryption	04 FIPS and post-quantum	05 Allowed sources	06 Edge protection	07 AI guardrails	08 Sensitive data	09 Audit trail	11 Change log	10 Policy reach	12 Console access
INTERNATIONAL STANDARDS													
ISO/IEC 27001	9/11	■	■	■	■	■	■		■	■	■	■	■
ISO/IEC 42001	4/4					■		■	■	■			
ZERO TRUST													
DoD Zero Trust	6/7	■	■	■	■	■	■	■	■	■	■	■	■
CISA ZTMM	6/7	■	■	■	■	■	■	■	■	■	■	■	■
UNITED STATES													
Federal mandates	5/5	■		■	■	■				■	■	■	
NIST SP 800-53	10/12	■	■	■	■	■	■	■	■	■	■	■	■
NIST CSF 2.0	4/6	■		■	■	■	■	■	■	■	■	■	■
FedRAMP	6/7	■		■	■	■	■			■	■	■	■
HIPAA	6/6	■		■	■	■			■	■	■		■
CANADA													
ITSG-33	8/10	■	■	■	■	■	■	■	■	■	■	■	■
PIPEDA	4/4	■		■	■	■			■	■			■
AUSTRALIA AND NEW ZEALAND													
ISM	5/7	■		■	■	■	■		■	■	■	■	■
NZISM	6/7	■		■	■	■	■			■	■	■	■
FINANCIAL SERVICES													
PCI DSS	8/11	■		■	■	■	■		■	■	■	■	■
SOC 2	5/7	■		■	■	■	■	■	■	■	■	■	■
EU DORA	5/6	■		■	■	■	■	■	■	■	■	■	■
OSFI B-13	5/7	■		■	■	■	■	■	■	■	■	■	■
APRA CPS 234	3/5	■		■	■	■	■		■	■		■	■
EUROPEAN UNION													
GDPR	4/4	■		■	■				■	■			
EU NIS2	5/7	■		■	■	■	■			■	■	■	■
EU AI Act	3/4			■			■	■		■			■
AI GOVERNANCE													
Responsible AI	11/12	■	■	■	■	■	■	■	■	■	■	■	■
OECD AI	3/4			■			■	■	■	■	■		

■ In place ■ Gap ■ Not used by the framework

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

FIGURE 4 · ONE FRAMEWORK'S LINES, ISO/IEC 27001



STATIC MAPPING, LIVE STANDING

Which controls a line rests on is fixed guidance. Whether those controls are in place is read live from the platform.

OWNED ELSEWHERE

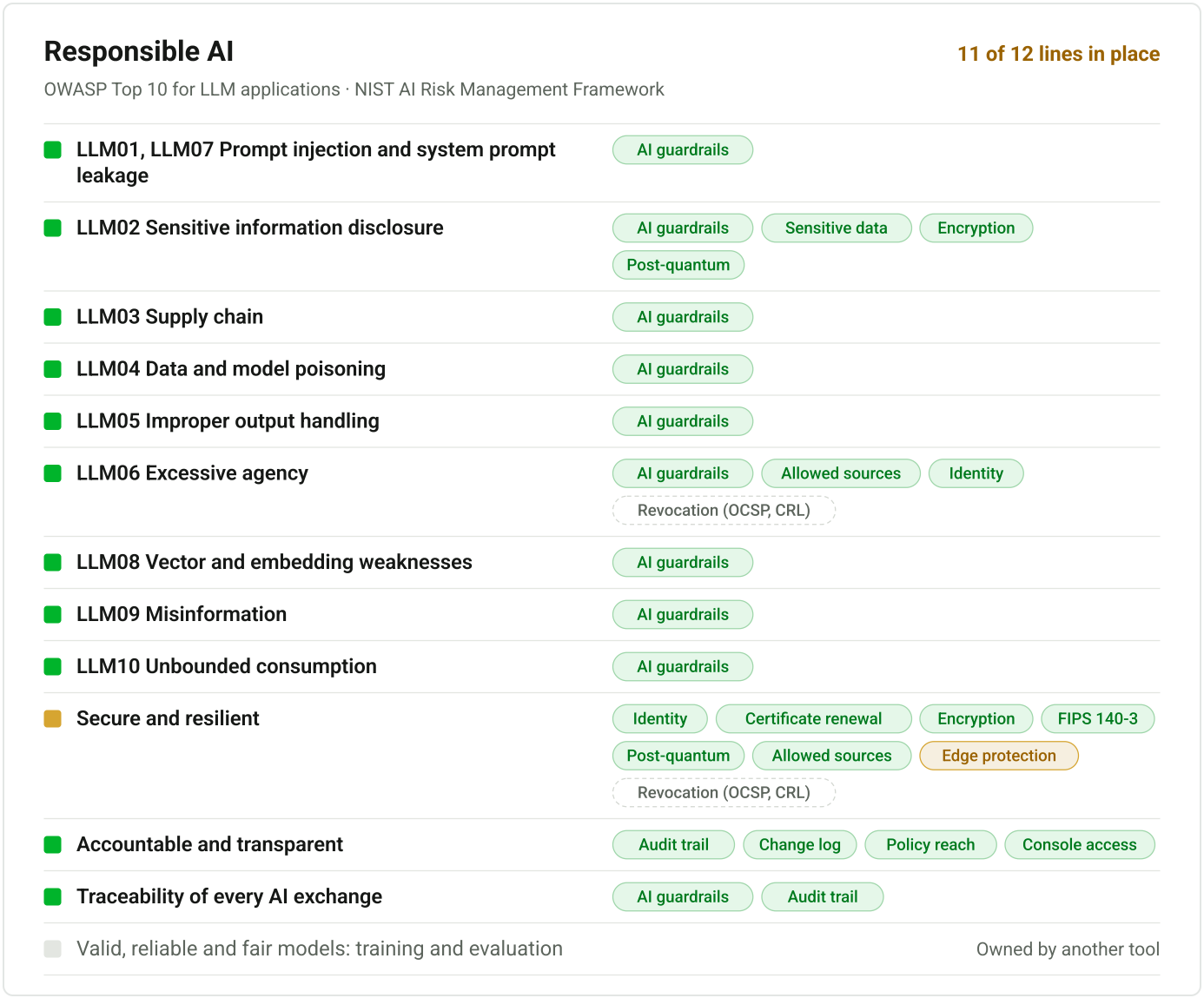
A line no Greymatter control covers says another tool owns it. It is left out of the framework's count.

Choosing a row lists the framework's lines. A line is in place when every control it rests on is in place. Each framework shows how many of its lines are in place, such as 9 of 11.

In this example, ISO/IEC 27001 A.8.16 and A.8.26 rest on edge protection. Two edges lack it, so those two lines show the gap. One fix moves every framework that rests on the same control.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

FIGURE 5 · RESPONSIBLE AI IN STOPLIGHT



MORE THAN THE SCORE

Some chips show what Greymatter does that no control scores yet, such as certificate revocation checks.

Responsible AI lays the OWASP Top 10 for LLM Applications and the NIST AI Risk Management Framework over the controls. Greymatter covers what happens in traffic: prompts, outputs, tools, agents and the trail of every AI call.

Model training, evaluation and provenance belong to the AI program, and Stoplight says so.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

7 Readiness against a maturity model

Maturity models ask how far a program has come, pillar by pillar. Stoplight shows which pillars rest on controls that are in place today. FIELDED

FIGURE 6 · MATURITY STAGES OF THE CISA ZERO TRUST MATURITY MODEL



Your program judges the stage.

Stoplight supplies the evidence, pillar by pillar.

EVIDENCE, NOT A GRADE

CISA publishes no coverage score. Greymatter does not assign a stage. It shows the controls behind each pillar and where they have gaps.

SAME VIEW FOR DOD

The DoD Zero Trust Strategy view lays the same controls over its seven pillars.

The CISA model has five pillars and three capabilities that cut across them. Each moves through four stages, from Traditional to Optimal. A program must show where it stands and what holds it back.

Stoplight answers the second question with live rows. Pick the CISA view, and each pillar shows the controls it rests on and whether they are in place on every workload. A pillar with a gap names the services that cause it.

CISA PILLAR OR CAPABILITY	STOPLIGHT CONTROLS BEHIND IT
Identity	Identity, Console access
Devices	Owned by device tools. Greymatter enforces their decisions at the edge
Networks	Encryption, FIPS 140-3 and post-quantum
Applications and workloads	Allowed sources, Edge protection, AI guardrails
Data	Sensitive data
Visibility and analytics	Audit trail
Automation and orchestration	Certificate renewal, Policy reach
Governance	Change log

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

8 Support for the rest of the stack

No single product meets a framework alone. Stoplight says which parts other tools own, and what Greymatter feeds them. FIELDED

FIGURE 7 · HOW GREYMATTER SUPPORTS THE REST OF THE STACK, IN STOPLIGHT

How Greymatter supports the rest of your stack

Other tools own some lines of the frameworks. The following table shows how Greymatter can support those tools.

Identity, credential, and access management (ICAM)

Greymatter carries the verified identity of each request across the mesh. It records that identity at every hop. The forensic audit trail names who started each request and every service that the request passed through. At the edge, Greymatter checks the sign-in tokens from your identity provider and the client certificates before a request reaches any service.

Observability

Every app that Greymatter manages can send its metrics, traces, and logs to your collector over the OpenTelemetry Protocol (OTLP). The app's own sidecar sends them, so you do not install an agent.

SIEM and SOAR

Greymatter records security evidence across your applications, AI, and workloads: the forensic audit trail, the service-to-service flows, and every configuration change. Greymatter can stream this evidence to your SIEM. Greymatter manages policy as code, so your SOAR can act through that policy.

Devices

Greymatter enforces the decisions of your device and identity tools. The edge stops a request that carries a token or certificate that those tools do not trust.

Data protection

Greymatter shows your data teams which services send sensitive data, such as personal data, health data, and data with classification markings. It also shows who requested that data.

AI governance

Your AI program owns model training, evaluation, and provenance. Greymatter gives that program evidence of how production systems use models: every prompt and its response, who sent the prompt, and what the guardrails found.

GDPR

The forensic audit trail shows which service handled personal data and for whom. This trail supports your records of processing and your breach reports.

Workloads outside the mesh

Greymatter reports any service that sends unencrypted traffic to a destination that Greymatter cannot identify. These reports make unmanaged workloads visible.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

9

Evidence an assessor can take away

A score is only as good as the rows behind it. Each control gives its rows, and Ask Greymatter takes questions about them. FIELDED

ROWS, NOT SUMMARIES

Each row names the namespace, the service and, where it matters, the pod or edge, with its status.

SAME RULES FOR EVERYONE

Stoplight, its rows and its Ask Greymatter tools read under one permission. Each reader sees only the namespaces their role allows.

Download per control. Each control that counts workloads or edges downloads its rows as a CSV file. An assessor gets the exact list of what is in place and what is not, at the moment of the read.

Printed report. Print report turns the page into a report, or a PDF. It holds the score, every control, each framework the Platform turns on, and the services where each control is not in place.

Daily security report. A daily per-service report records each service's FIPS mode, post-quantum readiness, weakest TLS version, mutual TLS and data plane. It states the time it was taken.

Ask Greymatter. A reader can ask in plain language. Read-only tools return the twelve controls with their counts, and the services where one control is not in place. They also return the daily report and the health rules behind Stoplight's words.

ASK GREYMATTER TOOL	WHAT IT RETURNS
Controls	Each of the twelve controls, its count of total, and whether it is in place
Control gaps	For one control, the services or pods where it is not in place, with each status
Security report	The daily per-service report, with the time it was taken
Stoplight and health rules	What is wrong in the mesh and why, and the rules that decide each word

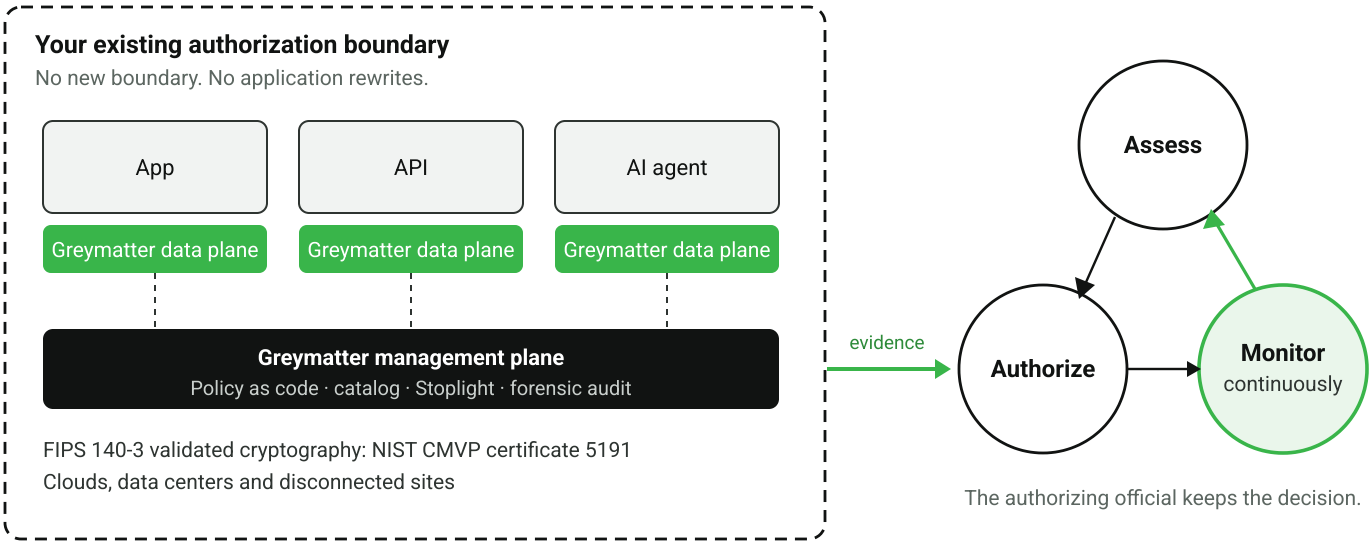
© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

10

Faster assessment inside your boundary

Greymatter runs inside the boundary an organization already accredits. It feeds each assessment with evidence and does not replace the process. FIELDED

FIGURE 8 · GREYMATTER INSIDE THE AUTHORIZATION BOUNDARY, FEEDING THE ASSESSMENT CYCLE



NO NEW BOUNDARY

Greymatter is an overlay on the workloads already inside the boundary. Teams change no application code.

VALIDATED CRYPTOGRAPHY

The data plane uses the Greymatter.io Cryptographic Module, NIST CMVP certificate 5191. It is active through 26 August 2029.

A new product often means a new boundary and a new accreditation. Greymatter avoids that. Its data plane runs beside each workload, and its management plane runs inside the same boundary.

Each assessment then starts from evidence, not a project. Controls show their standing on every workload. Rows, records and the change ledger are files an assessor can keep. Between assessments, the same reads support continuous monitoring.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Evidence at each step of the risk management cycle

STEP	WHAT THE STEP NEEDS	WHAT GREYMATTER SUPPLIES
Implement	Controls in place on every system component	Controls enforced by the data plane on every managed workload, with no code change
Assess	Evidence that each control works as intended	Live standing per control, CSV rows per control, and the forensic record
Authorize	A risk decision on a clear picture	Stoplight, the framework views and the named gaps. The authorizing official decides
Monitor	Ongoing checks, and a record of every change	Continuous reads, a daily report, and a ledger of every configuration change

FED, NOT REPLACED

The steps stay with the program and its assessors. Greymatter supplies the evidence each step asks for.

ARTIFACTS, NOT SCREENSHOTS

Each control downloads its rows as a file. Each record states when it was taken.

Policy as code. Each tenant keeps its configuration in its own Git repository. The same policy can move from development through test to production, and to disconnected sites. Every change has a history in Git.

Continuous monitoring. Forensic events and configuration changes go to the SIEM an organization already runs. Stoplight shows when policy has not reached a data plane, or a data plane has drifted from it.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

11

Twenty-three frameworks, one set of controls

Stoplight lays 23 frameworks over the same twelve controls. Each framework lists its lines and the controls each line rests on. FIELDED

International frameworks come first. United States frameworks come last, on the next page. A line no Greymatter control covers is named as owned by another tool, and is left out of the count.

FRAMEWORK	WHAT STOPLIGHT MAPS	LINES	OWNED BY ANOTHER TOOL
ISO/IEC 27001:2022	Annex A · selected controls	11	Clauses 4 to 10, people and physical controls
ISO/IEC 42001:2023	AI management system · Annex A	4	A.5 impact assessment, A.6.2.4 verification and validation
GDPR	Security of processing	4	Art. 17, 30, 44
EU NIS2 Directive	Directive (EU) 2022/2555 · Article 21(2)	7	21(2)(a), (c), (d), (g) Risk policy, continuity, supply chain, training
EU AI Act	Regulation (EU) 2024/1689 · high-risk systems	4	Art. 9, 10, 11, 13 Risk system, data, documentation, transparency
PCI DSS v4.0.1	Payment card industry · 12 requirements	11	Req. 3, 5, 9, 12 Stored data, malware, physical, policy
SOC 2	AICPA Trust Services Criteria · security	7	CC1–CC5, A1 Control environment, risk, availability
EU Digital Operational Resilience Act	Regulation (EU) 2022/2554 · ICT risk management	6	Art. 11, 12, 24–28 Continuity, backup, testing, third parties
OSFI Guideline B-13	Technology and cyber risk management · 3 domains, 17 principles	7	1.1 to 1.3 Governance and risk management, 2.9 Disaster recovery
APRA CPS 234 Information Security	Prudential Standard · paragraphs 13 to 36	5	13 to 19 Roles and policy framework, 32 to 34 Internal audit
Responsible AI	OWASP Top 10 for LLM applications · NIST AI Risk Management Framework	12	Valid, reliable and fair models: training and evaluation
OECD AI Principles	OECD Recommendation on AI · 5 principles	4	1.1 Inclusive growth and well-being

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Canada, Australia and New Zealand

FRAMEWORK	WHAT STOPLIGHT MAPS	LINES	OWNED BY ANOTHER TOOL
ITSG-33 and the CCCS Medium cloud profile	Annex 3A controls · CCCS Medium cloud profile (formerly PBMM)	10	PE, PS, CP and other program families
PIPEDA	Schedule 1 · Principle 4.7 Safeguards	4	4.1 Accountability, 4.7.4 staff awareness, and the other principles
Australian Government Information Security Manual (ISM)	ASD · selected cyber security guidelines	7	Personnel, physical and other guidelines
New Zealand Information Security Manual (NZISM)	GCSB · selected chapters	7	Physical, personnel and infrastructure security

United States frameworks

FRAMEWORK	WHAT STOPLIGHT MAPS	LINES	OWNED BY ANOTHER TOOL
United States DoD Zero Trust Strategy	7 pillars · target level due 30 Sep 2027	7	None
United States CISA Zero Trust Maturity Model	v2.0 · 5 pillars, 3 cross-cutting	7	Devices
United States Federal mandates	5 mandates	5	None
United States NIST SP 800-53 Rev. 5	Security and privacy controls · selected controls	12	PE, PS, CP, AT, PL and other program families
United States NIST Cybersecurity Framework 2.0	6 functions · selected categories	6	GV, ID, RS, RC Govern, identify, respond, recover
United States FedRAMP	Rev. 5 baselines · continuous monitoring	7	SSP, POA&M and 3PAO assessment
United States HIPAA Security Rule	45 CFR 164 · technical safeguards	6	§ 164.308, § 164.310 Administrative and physical safeguards

Using Greymatter does not make a system compliant with any framework. The mapping from controls to lines is guidance an assessor can check. A Platform can turn any framework off, and Stoplight then leaves its row out and names it in a note.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

12

Limits, stated precisely

A scorecard earns trust by being exact about what it does not show. FIELDED

LIMIT	WHAT IT MEANS
Not a certification	Stoplight shows Greymatter's controls. An assessor decides compliance
Mapping is guidance	Which controls a framework line rests on is fixed guidance, open to review
Opt-in controls	AI guardrails and sensitive data detection count only where a team turns them on
Observe posture	A service in observe counts as limiting its callers. The line shows how many services are in each posture
Frameworks turned off	A Platform can turn a framework off. Stoplight leaves its row out and names it in a note
Other tools' parts	Lines that other tools own are named and left out of the counts
Daily report	The security report is a daily snapshot. The controls themselves are read live
Unread sources	A control whose source did not respond shows as not read, and is left out of the score
Certificates you supply	Where an organization supplies its own mesh certificates, the identity and renewal controls do not apply

WHY IT MATTERS

An assessor can trust a green card because Stoplight refuses to show green when it has no reading.

Stoplight reports what Greymatter manages. A workload Greymatter does not manage shows up as a gap on the controls that apply to every service, or as an unidentified peer. It never disappears from the count.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

13

Evidence for security frameworks

Frameworks require that an organization checks its controls work. Stoplight is that check, run on the live platform. FIELDED

MEASURE, THEN PROVE

The same reads that drive Stoplight drive its rows, so the evidence and the score always agree.

International frameworks require more than controls. They require that an organization measures whether its controls work, and keeps doing so. Stoplight turns that duty into a reading of the platform, for every workload it manages.

FRAMEWORK	WHAT IT REQUIRES	WHAT GREYMATTER SUPPLIES
ISO/IEC 27001:2022	Clause 9.1: monitoring, measurement, analysis and evaluation	Twelve controls measured on every managed workload, with rows behind each count
EU NIS2 Directive	Article 21: policies to assess whether risk-management measures work	A live score, framework standings, and the gaps by service
NIST SP 800-207	Monitor and measure the security posture of every asset	Per-service checks of identity, encryption, policy and audit, refreshed continuously
United States CISA Zero Trust Maturity Model	Visibility and analytics, and governance, across every pillar	Stoplight's CISA view, pillar by pillar
United States DoD Zero Trust Strategy	Visibility and analytics pillar, and progress toward the target level	Stoplight's DoD view, pillar by pillar

Using Greymatter does not make a system compliant with any framework. It supplies controls and evidence an assessor can test. National rows come last.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

14 Operational and mission benefits

Each outcome, what produces it, and its status.

OUTCOME	WHAT PRODUCES IT	STATUS
Audit readiness every day	Twelve controls measured live on every managed workload	FIELDED
No spreadsheet attestation	Counts read from the platform, with rows per control	FIELDED
Gaps found before an audit	Unmanaged workloads and failed reads shown, never hidden	FIELDED
Standards in one view	23 frameworks in eight groups over the same controls	FIELDED
Clear ownership	Lines owned by other tools named, with how Greymatter supports them	FIELDED
Evidence on request	CSV per control, a printed report, a daily report and Ask Greymatter tools	FIELDED
Access by role	Each reader sees only the namespaces their role allows	FIELDED
No new boundary	Runs inside the accredited boundary, with no application rewrites	FIELDED
One crosswalk	International and United States frameworks over one set of controls	FIELDED

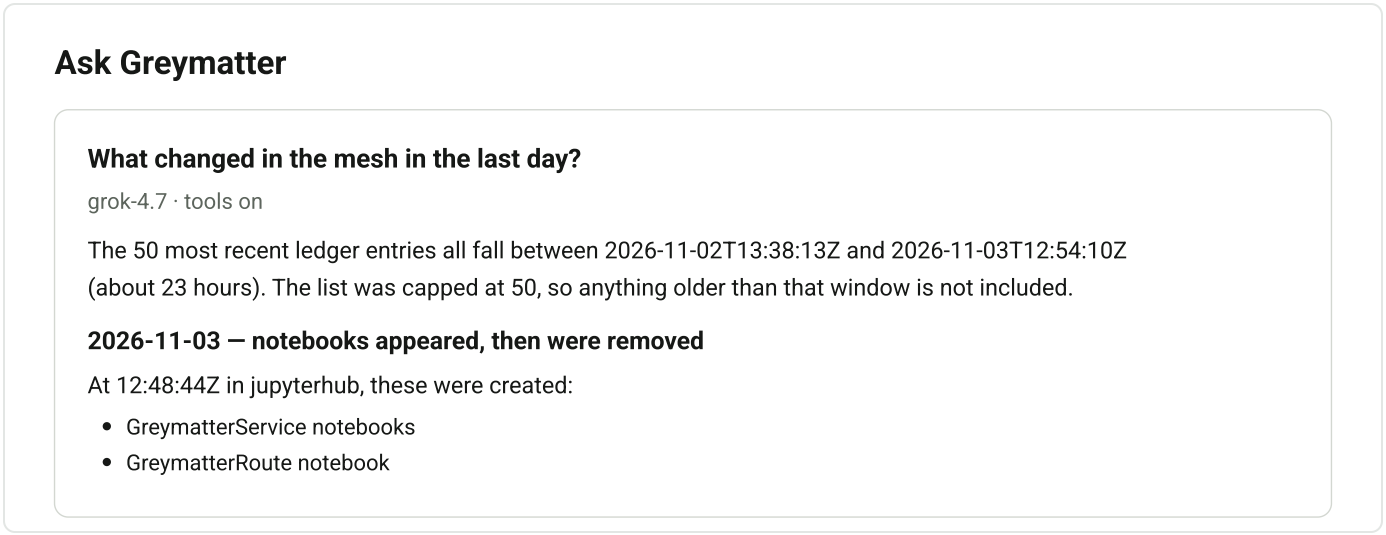
© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

15

Ask Greymatter

Ask Greymatter answers questions about the twelve controls and their gaps, from the same reads as Stoplight. FIELDED

FIGURE 9 · ASK GREYMATTER IN THE CONSOLE



READS AS YOU

Each tool reads the platform as the person who asked, and only reads. An answer holds only what that role allows.

GOVERNED LIKE ANY AI USE

Guardrails and DLP check each model call. The audit trail names the person and the agent.

Ask Greymatter is on every page of the Console. A person types a question in plain language. A model the organization chooses answers it from the platform's own data, through read-only tools.

For readiness and compliance, it reads the twelve controls, the gaps behind each one, the daily security report and the change ledger.

Tools come in groups: Health, Security, Traffic, Changes and Docs. Health and Docs are on by default. A person turns on the others in the Tools menu.

Questions a team can ask

“How many of the Greymatter controls are in place? Which are not?”
`Security` · the twelve controls and their counts

“Which services fail the encryption control, and what depends on them?”
`Security and Traffic` · one control's gaps, then dependents

“Where is FIPS not in place?”
`Security` · one control's gaps

“From the daily security report, which services lack mutual TLS?”
`Security` · the daily security report

“Is the change ledger intact?”
`Changes` · the change ledger's integrity

“When does Stoplight say security policy has not reached a service?”
`Docs` · the Greymatter documentation

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Key takeaways

1

Measured, not attested

Stoplight reads twelve controls from the platform itself, for every app, API and agent it manages.

2

Live

It refreshes on its own and says when it last read the platform.

3

Honest

A control that could not be read says so. The score never shows full over a gap.

4

Mapped

23 frameworks, from ISO/IEC 27001 and GDPR to PCI DSS and the EU AI Act, sit over the same controls.

5

Shared work

Parts owned by other tools are named, with how Greymatter supports them.

6

Evidence ready

Rows per control, a daily report and Ask Greymatter tools, under one permission.

IN ONE SENTENCE

Greymatter turns compliance into a live reading of every workload it manages, mapped to the standards and backed by rows an assessor can check.

© 2026 Greymatter.io · Greymatter.io is a trademark of Greymatter.io, Inc.

Greymatter.io

Measured live. Mapped to standards. Proven by evidence.

LEARN MORE

greymatter.io

Greymatter.io is a trademark of Greymatter.io, Inc.

© 2026 Greymatter.io, Inc.