COMPLIANCE AUDIT & CONSULTING

Pass the audit — not just read about your gaps

Lawyers, security testers and cloud engineers on one engagement, with one report and one roadmap. We find which rules apply to you, where you fall short, and then close the gaps in your infrastructure, so you reach audit-ready instead of collecting findings.

10
audit modules you can combine

8
ready-made packages by framework

3
disciplines: engineering, legal, security testing

4.9 / 5
on Clutch, 15 reviews

How it works

STEP 1 · FREE
Applicability call
30 minutes on your markets, customers and deadline, and which frameworks are in play.

STEP 2 · FIXED PRICE
Express Diagnostic
3 business days to know where you stand and what it takes to pass.

STEP 3
Compliance package
A full audit against your target framework, with a remediation roadmap.

STEP 4 · OPTIONAL
Fix & monitor
We build the controls, then keep you audit-ready with Compliance-as-a-Service.

START HERE
Express Compliance Diagnostic
3 business days · fixed price · about 2 hours of your team's time. A kickoff call and short questionnaire, our review with an external security scan, and a readout call on day 3.

- Regulatory applicability matrix: what applies, why, in what order
- Compliance Health Scorecard across five pillars
- Top 5 risks most likely to block an audit, deal or licence
- A fixed-price proposal for the full audit or certification

One team instead of three vendors

Engineering · Gart
Audit lead and the fix
Scoping, architecture and access review, control implementation, the report, and ongoing monitoring.

Legal partner
Which rules apply
Regulatory applicability, policies and contracts, DPAs and cross-border transfers, breach-notification duties, licensing.

Cybersecurity partner
Proof under test
Penetration testing, vulnerability scans, incident response, leaked-credential monitoring, KYC/KYB checks.

When teams bring us in

SITUATION	WHAT THE ENGAGEMENT IDENTIFIES
An enterprise customer sent a security questionnaire	Whether your current controls satisfy the buyer's requirements, and what to fix first
Preparing for SOC 2 or ISO 27001	Control gaps, evidence readiness and audit-blocking issues
Entering a new regulated market	Which frameworks apply, where jurisdictions conflict, and the readiness gap

New regulation: NIS2, DORA, EU AI Act	The gap between your current posture and the new requirements
Fundraising, M&A or investor due diligence	Compliance liabilities and gaps that could affect valuation, found before the other side's lawyers do
iGaming licensing (UKGC, MGA, Curaçao)	Licensing-specific technical and governance requirements
After a breach or security incident	Root cause, notification obligations and the controls that failed
New CISO or DPO, or annual re-certification	An independent baseline, drift since the last audit, and priorities
High vendor or third-party exposure	Vendor compliance gaps, missing contract terms and concentration risk

STEP 3

Packages

Frameworks share 60–85% of their controls, so one engagement can cover several. Each package is adjusted after the Express Diagnostic.

PACKAGE	GOAL	MODULES	TEAM
SOC 2 Readiness & Certification	Prepare for a SOC 2 Type I or Type II audit	1 2 4 5 8 10	Engineering lead · Security · Legal as needed
ISO 27001 Certification Readiness	Close the gap to ISO 27001 certification	1 2 4 5 6 8 10	Engineering lead · Security · Legal
GDPR & Data Privacy	Achieve and maintain GDPR and data-privacy readiness	1 3 4 7 8	Legal lead · Engineering
HIPAA / HITECH	Meet healthcare data-protection requirements	1 3 4 5 7 8	Legal lead · Engineering · Security
PCI DSS	Secure cardholder data and meet payment-industry rules	1 4 5 7 8	Engineering lead · Security
Vendor & Third-Party Risk	Reduce exposure from vendors and subprocessors	1 2 6 8	Engineering lead · Legal · Security
iGaming Regulatory Compliance	Meet UKGC, MGA or Curaçao licensing requirements	1 2 3 4 5 7	Legal lead · Engineering · Security
Enterprise Full Compliance Health Check	A complete evaluation across all compliance domains	1–10	Engineering · Legal · Security

DORA and NIS2 gap assessments are scoped from modules 1, 2, 4, 6, 7 and 8 to match your sector and entity type.

Optional add-ons

Policy & Documentation Drafting Sprint · DPIA Workshop · Incident Response Tabletop Exercise · Security & Compliance Training Program · Vendor Risk Assessment Sprint · Mock Audit / Pre-Certification Assessment · **Compliance-as-a-Service retainer** — continuous monitoring between audits

WHAT WE ASSESS

The 10 modules

01 Regulatory Scoping & Framework Mapping

Which regulations, standards and certifications apply to your industry, geography and business model?

- ISO 27001, SOC 2, GDPR, NIS2, DORA, HIPAA/HITECH, PCI DSS, EU AI Act, iGaming licences
- Jurisdictional overlap and conflicts
- Regulatory change monitoring
- Certification vs. self-attestation

You get: a regulatory applicability matrix with scope and priority for each framework.

Legal partner interprets applicability

02 Governance, Risk & Policy Management

Is there a real governance structure, risk method and policy set behind your compliance claims?

- Risk methodology and risk register
- Roles and responsibilities (RACI, DPO/CISO mandate)
- Policy library: InfoSec, Privacy, Acceptable Use, Retention
- Leadership reporting cadence

You get: a governance maturity report with a policy gap list and a risk register template.

Legal partner reviews policies

03 Data Protection & Privacy

How is personal and sensitive data collected, processed, stored and transferred?

- Data mapping and Records of Processing (RoPA)
- DPIAs and PIAs
- Consent and lawful basis
- Retention, deletion and cross-border transfers (SCCs, adequacy)

You get: a data flow map with a privacy gap analysis and a DPIA action plan.

Gart engineers map the technical data flows

04 Access Control & Identity Management

How is access to systems and data granted, authenticated and revoked?

- IAM and least privilege
- MFA coverage and privileged access
- Joiner, mover and leaver process
- Secrets and credential management

You get: an access control assessment with a prioritized hardening checklist.

Cybersecurity partner tests access controls

05 Security Controls & Technical Safeguards

Do your technical controls actually protect infrastructure, applications and data?

- Encryption at rest and in transit
- Network segmentation and firewalling
- Vulnerability and patch management
- Endpoint security and secure SDLC

You get: a technical security posture report with remediation priorities.

Gart engineers implement and harden

06 Third-Party & Vendor Risk Management

How are vendors and subprocessors assessed, contracted and monitored?

- Vendor due-diligence process
- DPAs and subprocessor register
- Review cadence for vendors' SOC 2 / ISO reports
- Concentration and fourth-party risk

You get: a vendor risk register with tiering and a reassessment schedule.

Legal partner on contracts · security partner on vendor scans

07 Business Continuity, Incident Response & DR

Can you detect, respond to and recover from an incident, and notify the right people on time?

- Incident response plan and playbooks
- Breach notification timelines (GDPR 72 hours, other laws)
- BCP / DR plans, RTO and RPO
- Tabletop exercise cadence

You get: an incident readiness report with a notification-obligation matrix and DR gap analysis.

Legal partner on notification duties

08 Audit Evidence, Monitoring & Reporting

Can you produce compliance evidence on demand, not only in audit season?

- Logging and monitoring coverage for control evidence
- Internal control-testing cadence
- Compliance KPI / KRI dashboards
- Audit trail retention

You get: an evidence-readiness report with a control-testing calendar.

Cybersecurity partner on monitoring evidence

09 Employee Awareness & Training

Do your people know their part, and can you prove it?

- Onboarding and annual training coverage
- Phishing and social-engineering simulations
- Policy acknowledgment tracking
- Role-based training for engineering, finance and support

You get: a training maturity scorecard with a program improvement plan.

Security partner runs phishing simulations

10 Certification & Attestation Readiness

How far are you from audit-ready for the exact certification you need?

- Control crosswalk (SOC 2 Trust Services Criteria, ISO 27001 Annex A)
- Evidence collection readiness
- Mock-audit findings
- Auditor selection and timeline

You get: a certification gap analysis with a remediation roadmap and an auditor-readiness checklist.

Legal and security partners support evidence

The five pillars

Every finding is mapped to one of five compliance pillars, so leadership sees which part of the program it puts at risk.

Governance & Risk | **Data Protection & Privacy** | **Security & Access Controls** | **Regulatory & Certification Readiness** | **Continuous Monitoring & Resilience**

WHAT YOU RECEIVE

One report, built for the auditor and the board

Executive summary — overall compliance health, key risks and the most important recommendations

Compliance Health Scorecard — overall score and a maturity score per module: Strong, Needs Improvement or High Risk

Scope & objectives — regulations, jurisdictions, systems and business goals covered

Methodology — modules, evidence, interviews, legal and technical analysis, scoring

Regulatory landscape — which frameworks apply, why, and where they overlap or conflict

Compliance maturity assessment — strengths, weaknesses and score for each module

Key findings & risks — severity, evidence, legal and business impact, recommended action

Domain reviews — governance, privacy, security and access, vendors, incident readiness

Prioritized remediation plan — Critical, High, Medium and Low, with expected impact

30/60/90-day roadmap — what to address now, next and later

Certification readiness summary — gap to certification, auditor readiness and timeline

Appendix — evidence, policy inventory, regulatory citations and scoring criteria

Why Gart

Engineers do the assessment, and build the fixes. Most audits end with a list. Ours end with a team that can implement the controls in your cloud and infrastructure.

Works with your GRC platform. Using Vanta, Drata or Secureframe? We build the controls the platform tracks.

Fixed scope, fast start. The Express Diagnostic gives you a clear picture in 3 days and a fixed-price proposal for what comes next.

Track record. ISO 27001, HIPAA, GDPR and SOC 2 work for SaaS, healthcare, fintech and iGaming companies. Rated 4.9 / 5 on Clutch.

Book your free applicability call

Tell us the framework, the market and the deadline. We will tell you where you stand.

info@gartsolutions.com
gartsolutions.com/services/it-audit-services/compliance-audit/