Research Report

How hot is GRC?

The UK GRC Temperature Report 2026



SURECLOUD®

www.surecloud.com

About this report

In 2026 we've shared that the temperature is rising across new regulations, complex supply chains, shadow tooling and an unprecedented GRC workload. Now we've measured it.

We've just launched our very own GRC Temperature Checker letting organisations explore how hot they're running from the outside-in.

This report shows how we've used this checker ourselves, taking the temperature of over **700** UK organisations using what's publicly available, with the same rules and scoring as our own GRC Temperature Checker at **scan.surecloud.com**

Our message is clear. The pressure on UK GRC is easy to see from the outside. The evidence of readiness is not.

Who is this for

This report is for the people who own GRC across UK organisations: CISOs, CROs and the managers who run the work day to day. It is also for the executives who fund them looking for proof of some of the pressures facing their team.

If you are asked why GRC needs more time, tooling or people, use this report as outside-in evidence.

Find your sector and size, see where your pressure comes from and then run the GRC Temperature Checker on your own organisation.

Key findings

703
UK organisations, read from public information

43°C
median temperature on a 20 to 50°C scale

73%
of the organisations we read run Hot

3.1
IT, cyber and data regulations per organisation

01 **Most organisations we read run hot.** The median reads **43°C** on a 20 to 50°C scale. 73% read Hot. This means they have complex regulatory obligations, large third-party supply chains visible from the web and potential internal complexity.

02 **AI is becoming a compliance necessity, not a question.** 43.8% of the organisations we have scanned publicly use or build AI. Nearly a 1/3 of the total organisations we scanned aligned to AI regulations and standards from the EU AI Act to ISO 42001. The number working internally to match ISO 42001 or NIST AI RMF is even higher.

03 **BUT the proof is rarely on show.** Only 26.5% of homepages show any assurance signal. Of organisations whose customers may ask for ISO 27001, 84.2% don't show certification on their homepage.

04 **Enforceable IT and privacy regulation is stacking up.** The average organisation faces 3.1 IT, cyber and data regulations in force or likely. 26.9% face five or more. Whilst every company scanned faced UK GDPR, a further half also had to make considerations for EU GDPR.

05 **Technology and financial services are the hottest UK sectors.** Technology and SaaS averages 44.5°C and financial services 44°C. They carry the heaviest regulation load: 62.5% and 50% face four or more regulations.

06 **Third-party exposure runs through one tag manager.** 96.1% of the 610 homepages we could read load code from at least one other company, and the median loads five. Google Tag Manager is on 72% of them, and it can add tags without anyone touching the site's code, so the list of suppliers can grow without a change to the site. 3% already load 15 or more, and one loads 32.

07 **London runs hotter than the rest of the UK.** 41.9°C against 40.6°C, with 3.5 regulations per organisation against 2.7. The gap comes from reach, AI and size: 64.4% of London organisations serve the EU, against 44.3% elsewhere.

These findings come from 703 UK organisations. Our readings are indicative, not legal or consultative advice.

01

The GRC temperature is rising

We wanted to measure the pressure on GRC teams from the outside. So we read what each organisation publishes about itself and then we scored it using our own GRC Temperature Checker.

This included:

- Its sector and size
- Active markets it operates in
- Use or building of AI
- Card payment requirements
- The third-party technology on its website
- The vendors it discloses.

The result was a temperature between 20°C and 50°C.



Reading	Share of organisations	What it means
Cool (20–30°C)	5%	Low scores on most of the four factors. These businesses have fewer external drivers though may still face GRC immaturity or pressure from the inside. Here the GRC is contained. The work can sit with a few people alongside their day jobs.
Warm (31–39°C)	22%	Scores on some factors, but fewer than half the available points. These businesses have a growing pressure but there's less public attention on them. GRC reaches across the business and the work needs a named employee and a plan.
Hot (40–50°C)	**73%**	Half the points or more. Sector and size alone can get an organisation there; others add heat through regulation or third parties. These have complex external drivers that force these businesses to consider GRC practices and technology. GRC is persistent, they typically need dedicated teams and specialists to handle the heat.

Median: 43°C. Nearly 3/4 of the organisations we scanned are Hot before we have asked them a single question about their own team.

Why it matters

GRC has often been an overlooked function, a reluctant necessity that is under-resourced or even pushed aside against competing IT, security or enterprise priorities. Today the temperature is rising. Without any insight on businesses' internal people, processes or technology, we can see that UK organisations are facing growing complexity, exposure and obligation that needs to be addressed.

With Verdantix recently reporting that 38% of businesses have frozen their risk budget, organisations are being asked to do more with less against a landscape that can't be ignored.

Verdantix, Hindsight, Oversight, Foresight: Why Half of Risk Leaders Are Still Flying Blind on Third Parties, 2026

What to do next

This week: run your own temperature and note which of the four factors drives it.

This quarter: list the business events that would raise it (a new market, an AI launch, an acquisition) and agree a communication plan for risk owners to be told before they happen.

Sector and size were established by SureCloud based on a projected base pressures and complexity that come with specific industries and company sizes, while regulation and third-parties scores responded directly from scanning results.

This is a public reading and the external temperature is just one part of the puzzle. This report can't see audit pressure, evidence scattered across inboxes or a team that spends its week firefighting. The live Temperature Checker asks additional questions about those factors, so a visitor's own result can differ from this public reading.

02
The hottest industries

Rank	Industry	Mean temperature	Share of "Hot"	IT and Cyber regulations per organisation
1	Technology and SaaS	**44.5°C**	94.4%	4.4
2	Financial services	44°C	90.5%	3.6
3	Manufacturing	41.8°C	82.4%	2.9
4	Public sector	40°C	69.4%	1.3
5	Legal & Professional services	39.1°C	56.4%	2.6
6	Education	39°C	55.3%	2.6
6	Media and entertainment	39°C	63.6%	2.6

Critical national infrastructure is included in the overall figures but isn't shown on its own.

- **The hottest sectors carry the heaviest regulatory load:** 62.5% of technology and SaaS organisations and 50% of financial services firms face 4+ regulations.
- **The coldest sectors still had global compliance obligations:** 69.7% of media and entertainment organisations had a level of IT compliance obligations that came from EU or US law.
- **Law firms ran hottest on size and reach:** 85.1% of the law firms whose size we found have 250 people or more, and 67.3% serve the EU. That reach brings regulation from abroad: the UAE's data protection law applies to 40.8% of them, and Saudi Arabia's to 24.5%.
- **UK public sector is less public about their IT/cyber compliance obligations:** A larger share of public bodies read Hot (75.6% against 72.8%), yet they face far less regulation: 1.3 per organisation against 3.2. Only 6.7% serve the EU. Their heat comes from the sector rating and size: at least 27 of the 45 public bodies we read (60%) have 250 people or more.

Why it matters

As the AI opportunity continues to rise, the appetite for UK investment in new technology partnerships and business opportunities also increases. However just like the financial services which the UK already has a global reputation for, these organisations are full of risk and compliance complexity so it is no surprise both sectors came out the hottest.

With growing supply chains and disparate regional offices, UK organisations who used to be out-of-scope of some of these obligations, continue to face IT, cyber and privacy regulations established not within the nation but also within the EU, Middle East and USA.

Understanding your overlapping control requirements, establishing a set of common controls and taking efficient actions to test them and monitor your adherence is now essential for the modern business.

What to do next

This quarter: list all of your compliance obligations and self-assess your readiness. How many are you prepared to evidence today? Where do controls overlap?

03

Size and revenue: where GRC heats up

Size has a clear pattern with GRC temperature: Fastest in the first 250 people, the bigger the company the more they typically fell in scope of regulations.

People	Mean temperature	Share of "Hot"	Regulations per organisation
1–49	35.5°C	30.4%	2.1
50–249	40.6°C	69%	2.9
250–999	43.3°C	93.7%	2.7
1,000–4,999	44.7°C	98.2%	3.9
5,000–9,999	45°C	97.2%	4.2
10,000+	45.5°C	100%	4.7

Revenue points the same way.

Revenue	Mean temperature	Share of "Hot"	Regulations per organisation
Small-company filing (indicative under £15m)	38.5°C	53.5%	2.7
£15m–£50m	41.4°C	72%	2.9
£50m–£250m	42.9°C	87.5%	3.2

Why it matters

Larger organisations with more people and revenue may have more resources, but they also face larger expectations and obligations. Big UK enterprises can face the largest financial, reputational or operational consequences from risk events, non-compliance or poorly managed incidents. The last 5 years have seen multiple large UK brands suffer from severe impacts because of their large supply chains that have been compromised. As size and revenue increases, so do the potential gaps facing the business. Organisations need better visibility, more frequently into their third-party risks and supply chains and to link those to their broader internal risk and control efforts.

04

Regions: London runs hotter

We also looked at each organisation against its registered address. The spread is narrow, from 39.8°C in the South West and Wales to 41.9°C in London.

Region	Mean temperature	Sample
London	**41.9°C**	309
South East and East	41°C	134
North of England	40.7°C	94
Midlands	40.4°C	51
Scotland and Northern Ireland	40.2°C	40
South West and Wales	39.8°C	51

London against the rest of the UK.

Area	Mean temperature	Share of "Hot"	Regulations per organisation
London	41.9°C	76.7%	3.5
Rest of the UK	40.6°C	68.9%	2.7

Why London runs hotter. Reach, AI and size.

- 64.4% of London organisations serve the EU (44.3% elsewhere).
- 57% use or build AI (34.3% elsewhere).
- 62.3% of those whose size we found have 250 people or more (46.5% elsewhere).

Scotland's organisations reach abroad less: 29.4% operate beyond the UK, and they face 1.9 regulations each.

Why it matters

Today organisational reach drives heat more than geography. Whether a business is based in London or the North East, it still faces EU, US and Middle East obligations if it sells there. Whilst geographies can change concentration or geopolitical risks on a global scale, within the UK location is not a good indicator for exposure.

What to do next

30 days: pull the countries you have customers and data subjects in from your CRM or finance teams, and compare against the markets your compliance standards assumes.

Ongoing: ensure the risks are recorded around customers, data and suppliers, not just offices or geography.

05

Emerging IT, cyber and data regulations

The report focused on IT, cyber and data regulations. “Applies” means the law covers the organisation. “Likely” means it may, depending on details we can’t see from outside. “Coming” laws aren’t yet in force and add nothing to the temperature.

UK GDPR was the baseline: it applies to all UK organisations with the scanner showing 99.6% coverage of organisations sampled.

Regulation	Share in scope	Tier	What puts an organisation in scope
UK GDPR and Data Protection Act 2018	99.6%	Applies	Operates in or serves the UK
EU GDPR	52.3%	Applies	Operates in or serves the EU
US state privacy laws (e.g. California CCPA)	46.9%	Likely	Serves US customers
EU AI Act (Regulation (EU) 2024/1689)	30.4%	Likely	Uses or builds AI and serves the EU
UK NIS Regulations 2018	28.7%	Likely	Works in a UK sector the NIS Regulations cover
UK Cyber Security and Resilience Bill	28.7%	Likely, coming	Works in a UK sector the Bill will cover once it becomes law. Currently unscored
NIS2 Directive (EU) 2022/2555	20.8%	Likely	Works in the EU in a sector NIS2 may cover, with 50 people or more or size unknown

Regulation	Share in scope	Tier	What puts an organisation in scope
UAE Personal Data Protection Law	11.1%	Applies	Operates in the UAE
DORA (Regulation (EU) 2022/2554)	5%	Likely	EU financial services
Saudi Arabia Personal Data Protection Law	4.8%	Applies	Operates in Saudi Arabia
NYDFS Cybersecurity Regulation (23 NYCRR 500)	4.3%	Likely	US financial services
UK Telecommunications (Security) Act 2021	2%	Likely	Works in telecoms or digital infrastructure in the UK

IT frameworks and standards

Framework	Share	Why customers may ask
ISO/IEC 27001	93.2%	Sells to businesses
NIST Cybersecurity Framework (CSF)	46.9%	Operates in the US
SOC 2	46.7%	Sells to US businesses
ISO/IEC 42001 (AI management system)	43.8%	Uses or builds AI
PCI DSS	5.1%	Takes card payments in commercial or financial sectors

What we found:

- **Half answer to two different GDPRs.** EU GDPR applies to 52.3% of the organisations we read, on top of UK GDPR which applies to all that were scanned.
- **AI is becoming a compliance necessity.** 43.8% publicly use or build AI. 69.5% of those also serve the EU, so the EU AI Act may apply to 30.4% of all the organisations we read. Their customers may also ask for ISO/IEC 42001.
- **The Cyber Security and Resilience Bill (CSR) may reach fewer organisations than you'd expect.** Once it becomes law, the Bill only covers specific critical UK sectors only: health, energy, utilities and transport, telecoms and digital infrastructure, and technology. Far smaller in sector scope than the EU equivalent through NIS2. However that is still **28.7% of the organisations we read** vs the 20.8% of NIS2.
  - Within the sample CSR affected:
    - 58.2% of tech organisations;
    - 16.7% of manufacturers;
    - 4.4% of public bodies;
    - 4.3% of financial services firms;
    - none of the law firms.
- **NIS2 may cover more sectors than the UK rules,** including manufacturing, the public sector and education, for organisations working in the EU with 50 people or more (or whose size we couldn't find). Because it needs EU reach, it is likely for fewer of the organisations we read overall: 20.8%, against 28.7% for the UK NIS Regulations. But half of manufacturers (50%) are likely in scope.

- **DORA has low public exposure.** In reality DORA has nearly complete coverage over financial services and banking businesses in the EU however only half of the firms we scanned surfaced as in-scope in their website materials.

06

Who shows their GRC proof

In the private sector many customers ask for proof of certification. We checked how many homepages show it: badges or links for Cyber Essentials, ISO 27001 and SOC 2, their trust centre or a sub-processor list. We assessed 608 homepages.

This is what the homepage shows, not verified certification. An organisation can hold a certificate and not display it, and a badge isn't proof of a current certificate.

Signal shown on the homepage	Share of homepages
NCSC Cyber Essentials (any)	14.1%
NCSC Cyber Essentials Plus	6.7%
ISO/IEC 27001	15.1%
SOC 2	2.1%
Hold a trust centre	6.4%
Sub-processor list	0.8%
Any of these	**26.5%**

The proof gap. Customers may ask 93.2% of the organisations we read for ISO 27001. Of those, 84.2% don't show it on their homepage.

Industry	Cyber Essentials	ISO 27001	SOC 2	Trust centre	Any	ISO 27001 may be asked, not shown
Tech	23.8%	26.7%	5.2%	13.3%	46.7%	73.4%
Financial services	5.3%	10.5%	2.6%	2.6%	13.2%	91.7%
Legal	7.1%	4.8%	0%	0%	11.9%	95%
Manufacturing	7.9%	0%	0%	2.6%	10.5%	100%
Public sector	2.9%	0%	0%	0%	2.9%	–
All other industries	12.1%	12.1%	0.5%	4.2%	20.1%	87.2%

- **Tech shows the most proof:** 46.7% display at least one signal.
- **Two of the most regulated groups show far less:** 13.2% of financial services homepages and 11.9% of law firm homepages show any signal at all.

Why it matters

Whilst SOC 2 has often been a right-to-compete for new US organisations in tech or professional services, the UK has historically not had the same drivers for the likes of Cyber Essentials or ISO 27001 beyond the desire to demonstrate and show best practice. The scanner suggests this is still the case. GRC effort is rising exponentially but UK organisations need to be better at promoting those efforts and proving it to foster trust and confidence.

What to do next

This month: list the current certificates and reports you hold and publish what you can in one findable place.

This quarter: keep an approved answer library for incoming due diligence, and log how many questionnaires arrive and how long they take.

07

The most common third-party web technologies

Almost every homepage we could read loads technology from other companies: analytics, tag managers, fonts, cookie banners, chat. Of **610** homepages, only 3.9% load none. Each of the rest runs code or content from at least one other company in the visitor's browser.

The median homepage loads **5** third-party services. **55.1%** load five or more, enough to reach the scoring's warm threshold. **3%** reach the hot threshold of 15. One loads 32.

#	Technology	Share of homepages
1	Google Tag Manager	72%
2	Google APIs	35.7%
3	Google static content	21%
4	Google services	16.1%
5	LinkedIn	14.9%
6	jsDelivr CDN	14.8%
7	HubSpot	13.9%
8	Cloudflare	13.4%
9	Adobe Fonts	11.8%
10	YouTube	9.5%

- **One supplier was found on most homepages. 83.3%** of the homepages we read load at least one Google service. Google Tag Manager alone sits on 72%.
- **Hotter organisations run slightly more third parties.** Hot organisations load a median of 5, warm ones 4 and cool ones 3. Third parties are one of the four factors in the temperature, so part of that gap is built into the score.

Why it matters

Whilst this report focuses mainly on web technologies given their public availability, even this narrow insight still carries multiple implications for GRC teams.

- **A wider attack surface.** Every tag is code from another company, running on your page with your visitors. Each one is a supplier, whether or not procurement ever saw it.
- **Data leaving through the side door.** Tags can send visitor data to third parties. Where a tag manager adds tags after the page loads, the list of who receives that data can change without anyone touching the site's code.
- **Dependence on a single provider.** When one supplier's code runs on most homepages, its availability and its security become part of everyone's risk at once.

What to do next

This week: scan your own site with developer tools or your consent platform and list every third party.

30 days: give each an owner and data category, add them to the supplier register, restrict who can publish to the tag manager, and put tag changes through change control.

08

Email: the open door

We also checked one signal the temperature doesn't score: whether an organisation's domain tells receiving servers what to do with email that fakes it. The control is called DMARC.



DMARC policy	What it asks receiving servers to do with spoofed email	Share
Reject	Reject it	**43%**
Quarantine	Send it to spam	28%
Monitor only	Nothing; report it only	21%
No record	No instruction	8%

Fewer than half reject spoofed email outright. For the 21.3% that only monitor and the 8.3% with no record, the domain's own policy does nothing to stop email that fakes it. Receiving servers may still filter it, but nothing asks them to.

It varies by industry and size.

- Law firms lead: 69.4% reject.
- Then the public sector (57.8%) and financial services (54.3%).
- Tech is at 36%.
- Manufacturing trails at 23.8%, and 31% of manufacturers have no DMARC record at all.
- By size, 79.3% of organisations with 10,000+ people reject spoofed email, against 16.8% of those under 50.

Why it matters

Impersonation is getting easier to do at scale. A convincing email in a supplier's or a client's name no longer takes skill or time. A domain that only monitors, or has no DMARC record, leaves the door open to anyone who wants to use its name. It is one of the few controls that costs little and closes off a whole route of attack.

09

Taking the heat off: SureCloud's view

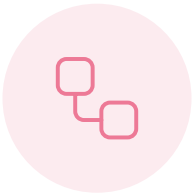
Each of these findings paints a picture of external obligation and each adds work. For many organisations these pressures are stacking up too fast.

GRC does not have a knowledge problem, it has a capacity one. GRC teams know what good looks like but they lack the hours to research, record, chase, evidence, assess and monitor across every framework, every supplier and every risk.

Here are 5 areas SureCloud recommends to change that:



01 **Test once, use everywhere.** The average organisation we read faces 3.1 regulations in force or likely. Customers may ask 93.2% for ISO/IEC 27001, 46.9% for NIST CSF and 46.7% for SOC 2. Much of what they ask for overlaps. You should be able to map a control once and use the same evidence and same tests for every framework that needs it.



02 **Make third-party risk continuous.** The median homepage we read loads five third-party services. 72% run Google Tag Manager, which can add tags without anyone touching the site's code. Point-in-time reviews can't keep up with that. Review suppliers as they change with continual vendor scanning, not once a year.



03 **Get ahead of AI.** 43.8% of the organisations we read use or build AI, and 69.5% of those serve the EU, where the EU AI Act may set duties. Start with an inventory of where AI is used. Then map it to the EU AI Act and to what customers may ask under ISO/IEC 42001.

04 **Close the easy gaps.** Only 42.7% reject spoofed email, and among organisations under 50 people it's 16.8%. Moving DMARC to reject as part of a phased approach of monitoring, quarantining and rejecting is within many teams' reach. So is showing the assurance you already hold: only 26.5% of homepages show any proof of infosec capability.



05 **Know what your customers will ask you to prove.** Of organisations whose customers may ask for ISO 27001, 84.2% don't show it on their homepage. In our view, this is the cheapest gap to narrow: where an organisation already holds a certificate, showing it costs little. A trust centre, which 6.4% of homepages show, answers the question before a buyer asks it.

SureCloud is the platform built to close this gap, helping teams shift to a continuous, automated approach wherever they sit. Gracie® AI extends your reach performing your real GRC tasks through Agents, ensuring they're done to repeatable standard based on your own internal expertise with Skills, and making use of Personas, with 20 years of practitioner knowledge to surface insights and help you act on your data. For once your team leads the programme rather than chases it.

You can do more with less, and do it better.

What's your temperature?

Every organisation in this report was scored with the same rules. Run the GRC Temperature Checker on your own organisation at **scan.surecloud.com**. It asks five questions about your team. Your answers on frameworks and vendors take the place of the regulation and third-party readings, so your result may differ from the figures here.

10
How we did it

The sample. We read 703 UK organisations from a list of UK suppliers, with organisations added in five focus industries: financial services, manufacturing, public sector, legal and critical infrastructure. The sample doesn't represent all UK organisations, so this report speaks about the organisations we read. We only report groups of 30 or more organisations.

What we read. For each organisation: its homepage and the third-party technology it loads, the vendors it discloses, the assurance signals its homepage shows, its DMARC record, and public research on its sector, size, markets, use of AI, card payments, revenue, ownership and registered address.

How we scored it. Each organisation ran through the same rules and scoring as the GRC Temperature Checker. The rules map an organisation's facts to the regulations that apply or are likely to apply. The scoring rates four factors from 0 to 2:

- sector risk, a rating SureCloud sets for each sector. Financial services, insurance, healthcare, energy and utilities, transport and logistics, telecoms, digital infrastructure, technology and SaaS, manufacturing and the public sector are rated 2; other sectors are rated 1;
- size (0 under 50 people, 1 from 50 to 249, 2 from 250 up);
- number of regulations (warm from 2, hot from 4);
- number of third parties (homepage technology plus disclosed vendors; warm from 5, hot from 15).

Temperature = $20 + 30 \times (\text{points} \div \text{maximum points})^{0.6}$. "Coming" laws aren't counted.

The sector rating is part of the scoring by design, and works the same way in the live Temperature Checker. Some regulations, such as the UK NIS Regulations and DORA, also apply by sector, so sectors rated 2 often face more regulation too.

What it couldn't see. This was a public reading. The live Temperature Checker also asks visitors five questions about their own team, and their answers on frameworks and vendors replace the regulation and third-party readings so a visitor's own result can differ from the figures here.

Limits.

- Regulation readings are indicative, not legal advice. "Likely" depends on details we can't see from outside.
- Third-party counts and assurance signals are what the homepage shows: a floor, not verified.
- Where a factor couldn't be found for an organisation, such as its size, its temperature uses the factors we could score.
- No individual organisation is named.

Research ran in November 2026.

For more information on how SureCloud can assist your organization, visit us online at **www.surecloud.com**, or email **sales@surecloud.com**

About SureCloud

SureCloud is the GRC platform that does more, better, with less. One platform covering risk, compliance, audit, third party risk management, business continuity and data privacy, powered by Gracie® AI Agents with Personas and Skills, a virtual GRC team performing the activities the programme needs at scale.

Founded in London in 2006, SureCloud has spent twenty years building GRC expertise into the platform.