SECURE CONTROLS FRAMEWORK

STATE OF THE INDUSTRY SURVEY: GLOBAL CYBERSECURITY PRACTITIONER PERSPECTIVES 2026

con·trol
/kən trol/

A control is the power to influence or direct behaviors and the course of events. That is precisely why the Secure Controls Framework® (SCF) was developed – we want to influence secure practices within organizations so that both cybersecurity and data privacy principles are designed, implemented and managed in an efficient and sustainable manner.

Table of Contents

Executive Summary

This report summarizes the 2026 State of the Industry Survey: Global Cybersecurity Practitioner Perspectives that covered seven (7) sections:

(1) Professional profile;
(2) Laws, Regulations & Frameworks;
(3) Resourcing constraints;
(4) Risk management practices;
(5) Industry challenges and emerging trends;
(6) Industry hype; and
(7) Metaframeworks.

Several themes run through the survey that CISOs and GRC Directors should be aware of:

Compounding Compliance Burdens

The compliance burden keeps compounding rather than consolidating:

- 62% of organizations track four or more (4+) distinct laws, regulations, or frameworks simultaneously;
- Nearly a third face more than ten external audits a year; and
- Only 58% of practitioners feel confident they could withstand an unannounced audit.

Mid-Market Underperformance

Organization size reshapes program health in a counter-intuitive way.

Mid-market organizations (250-4,999 employees) consistently report the weakest executive engagement, staffing, program maturity, GRC-platform satisfaction, third-party risk pressure, and Zero Trust progress of the three size bands; and sitting behind both smaller and much larger peers.

Governance, Risk & Compliance (GRC) Tools Continue To Disappoint

The tools meant to make compliance manageable are themselves a weak link:

- GRC-platform satisfaction is the lowest-rated metric in the entire survey; and
- Close to half of respondents still run governance, risk, and compliance work on spreadsheets or with no dedicated tool at all.

Fractured Risk Management Practices

Risk management practice is more fragmented than mature.

62% of organizations manage four or more (4+) frameworks at once, yet a quarter have no formally defined risk methodology, and pre-production Control Validation Testing (CVT) is ad hoc or absent at 63% of surveyed organizations.

Industry Concerns

Practitioners were candid and skeptical about their own industry:

- "AI-powered" product labeling is the single most distrusted marketing claim (67%), and
- Generative AI for security operations tied with "Zero Trust as a purchasable product" as the most overhyped concept in the field (39% each).

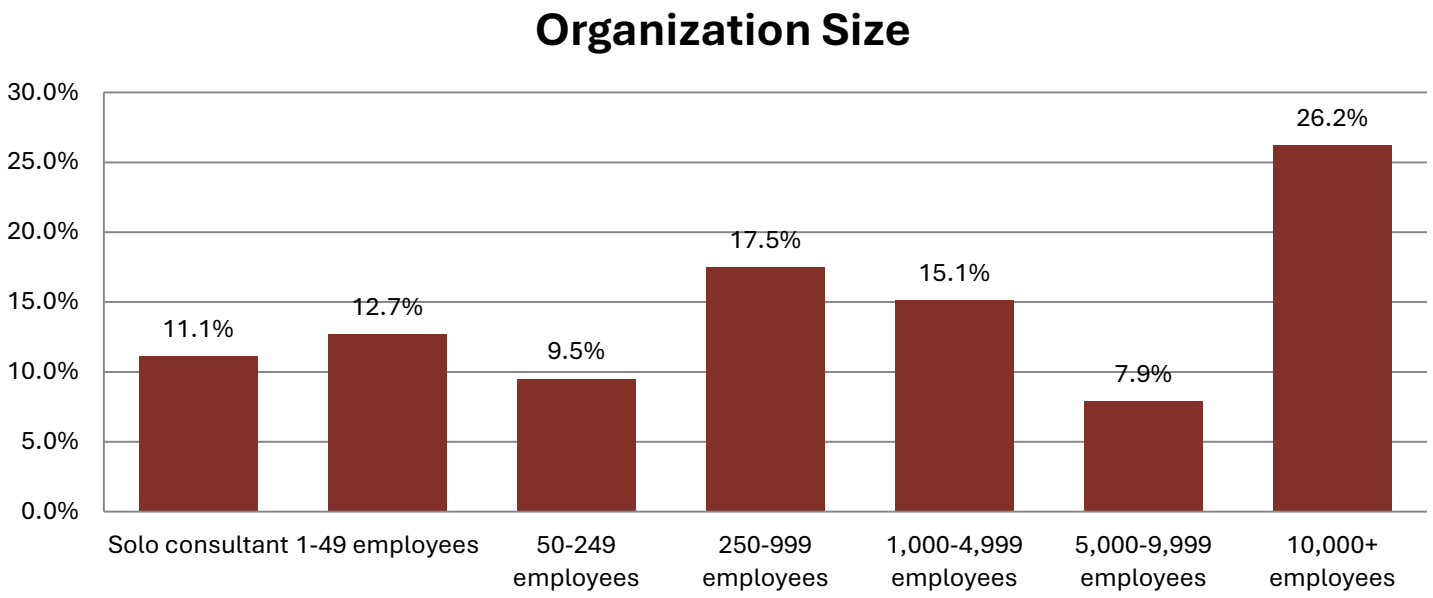
Ungoverned Artificial Intelligence (Gen AI)

Within GRC, generative AI has moved from novelty to daily practice faster than governance has caught up:

- 56% of organizations are actively using AI in compliance, GRC, or security workflows today, but data-privacy risk, employee misuse, and "shadow AI" are each cited as a top concern by more than half of respondents, and
- Only 6% have a formal, externally validated AI governance program.

Professional Profile

In this part of the survey, practitioners were asked to information about their roles and organizations.



Breakdown By Sector

By sector, consulting, advisory, and managed services (30%) and financial services, banking, and insurance (19%) are the two largest groups, followed by technology and software (17%) and healthcare (7%); the remainder is spread across critical infrastructure, government, manufacturing, retail, and other sectors.

Breakdown By Role

By role, CISOs/CSOs/security VPs (20%) and GRC specialists or consultants (20%) make up the largest groups, followed by C-suite executive leadership and compliance analysts or managers (10% each).

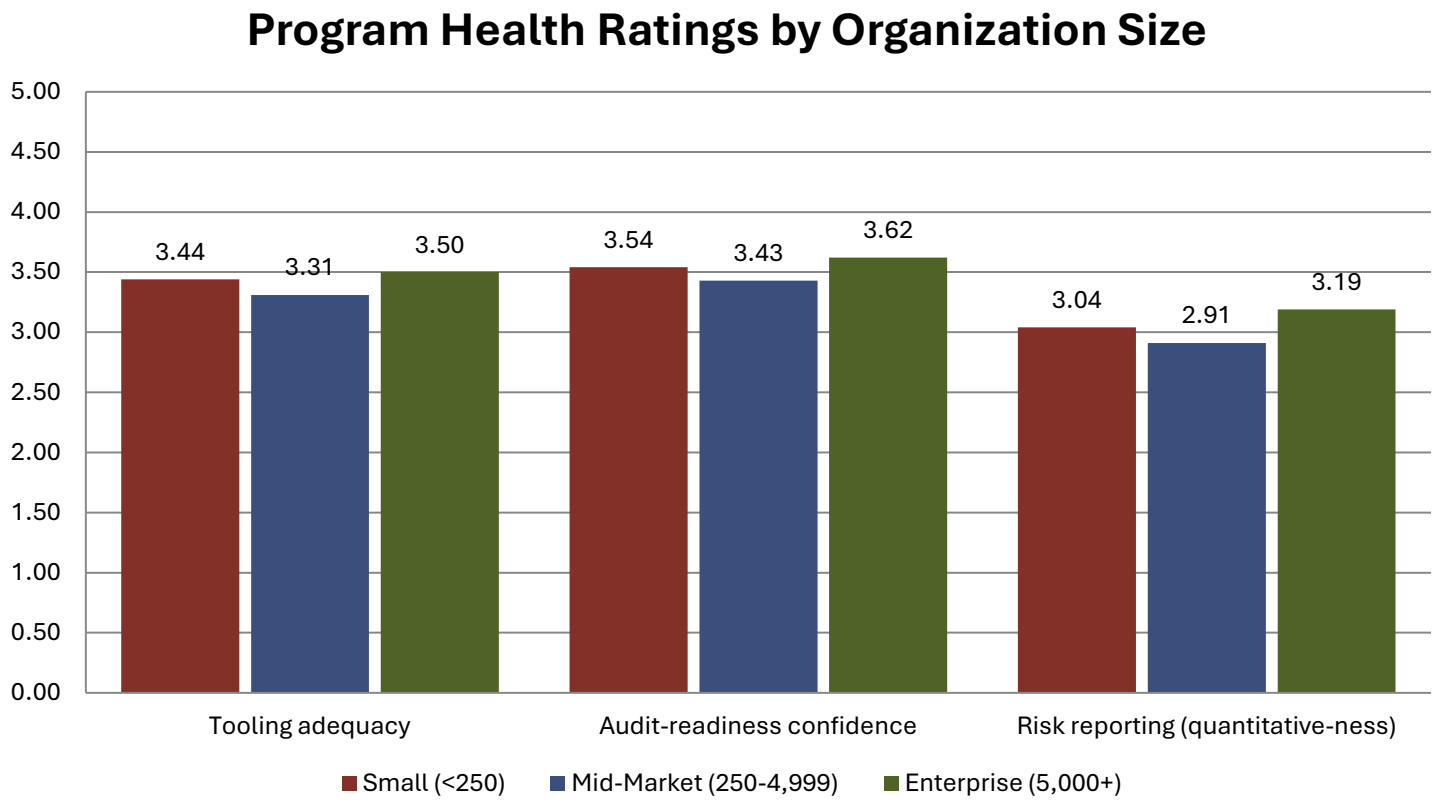
Respondents' work spans a genuinely global footprint, most concentrated in the United States (42%), Western Europe (22%), the United Kingdom (21%), and Central & Eastern Europe (20%), with meaningful representation from every other region tracked.

Laws, Regulations & Frameworks

In this part of the survey, practitioners were asked to describe what shapes their day-to-day compliance work:

- What drives framework adoption;
- How many audits and frameworks they manage;
- Which specific laws and frameworks are in scope; and
- What tools they use to manage it all.

Despite the workload respondents face, audit-readiness confidence has not scaled to match where only 58% of practitioners overall rate themselves a 4 or 5 out of 5 on confidence in surviving an unannounced audit and this figure barely varies by size band (57% small, 57% mid-market, 60% enterprise).



Useful insights:

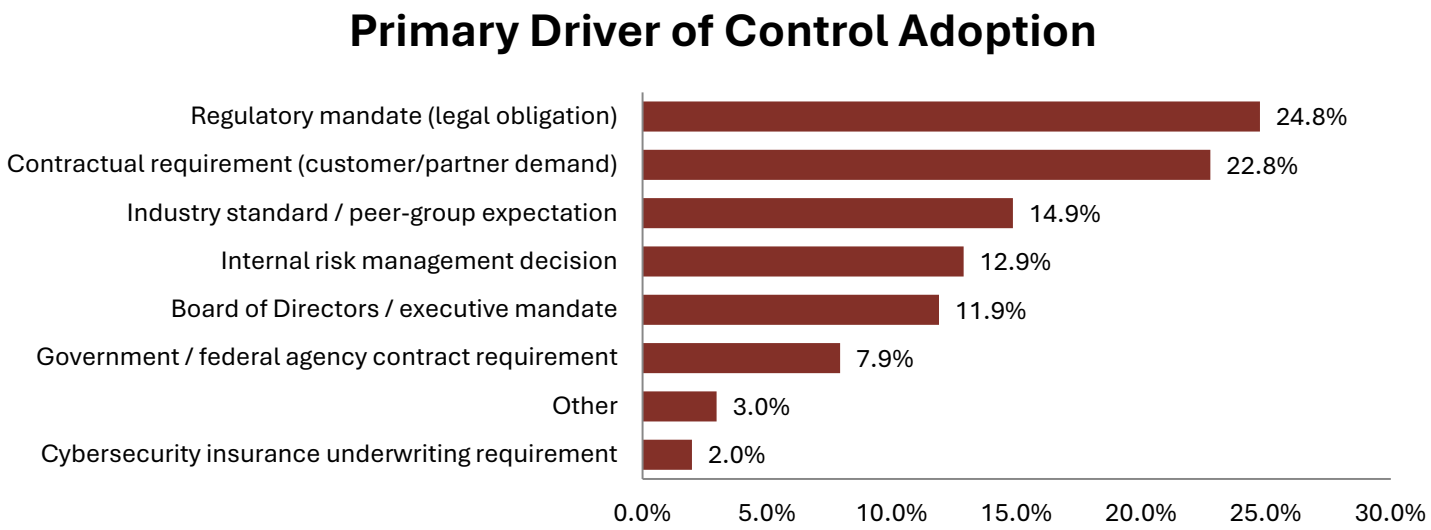
- Organizations facing four times the audit load report almost the same confidence as those facing far less.

GRC Adoption Drivers

Complying with statutory and/or regulatory mandates (e.g., legal obligation in the organization's jurisdiction) was the single most common primary driver of framework or regulation adoption (25%), narrowly ahead of contractual requirements from customers or partners (23%). Industry standard or peer-group expectation (15%) and voluntary internal risk-management decisions (13%) follow, with Board of Directors or executive mandate at 12% and government or federal contract requirements at 8%. Cybersecurity insurance underwriting requirements accounted for only 2%.

Useful insights:

- Mergers, Acquisitions & Divestitures (MA&D) due-diligence was cited by zero respondents as a primary driver.



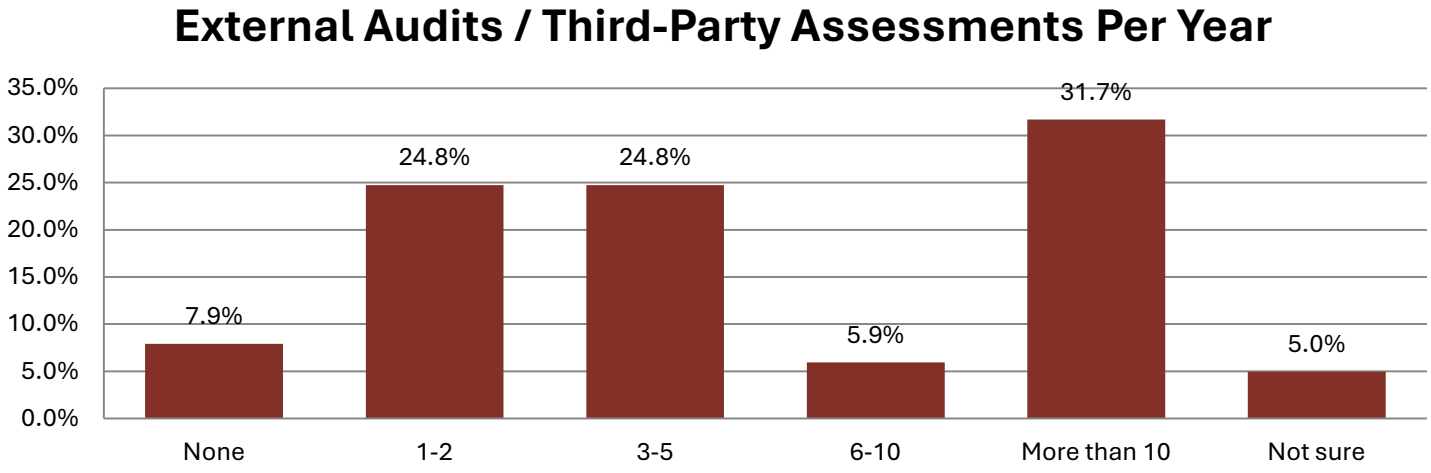
The driver shifts meaningfully by organization size. Contractual requirement is the top driver for small organizations (32%), consistent with smaller firms adopting frameworks because a customer or platform requires it, while regulatory mandate and Board/executive mandate rise steadily with size: regulatory mandate is cited by 14% of small organizations, 23% of mid-market organizations, and 34% of enterprises, and Board/executive mandate rises from 7% (small) to 21% (enterprise).

Useful insights:

- Smaller organizations are pulled into compliance by their customers; and
- Larger organizations are pushed into it by regulators and their own boards.

Audit & Framework Burdens

The overall audit load is heavy where 32% of organizations face more than ten external audits or third-party assessments a year, and only 8% report none at all. Audit frequency scales sharply with size where only 11% of small organizations report more than ten audits a year, compared with 37% of mid-market organizations and 42% of enterprises.

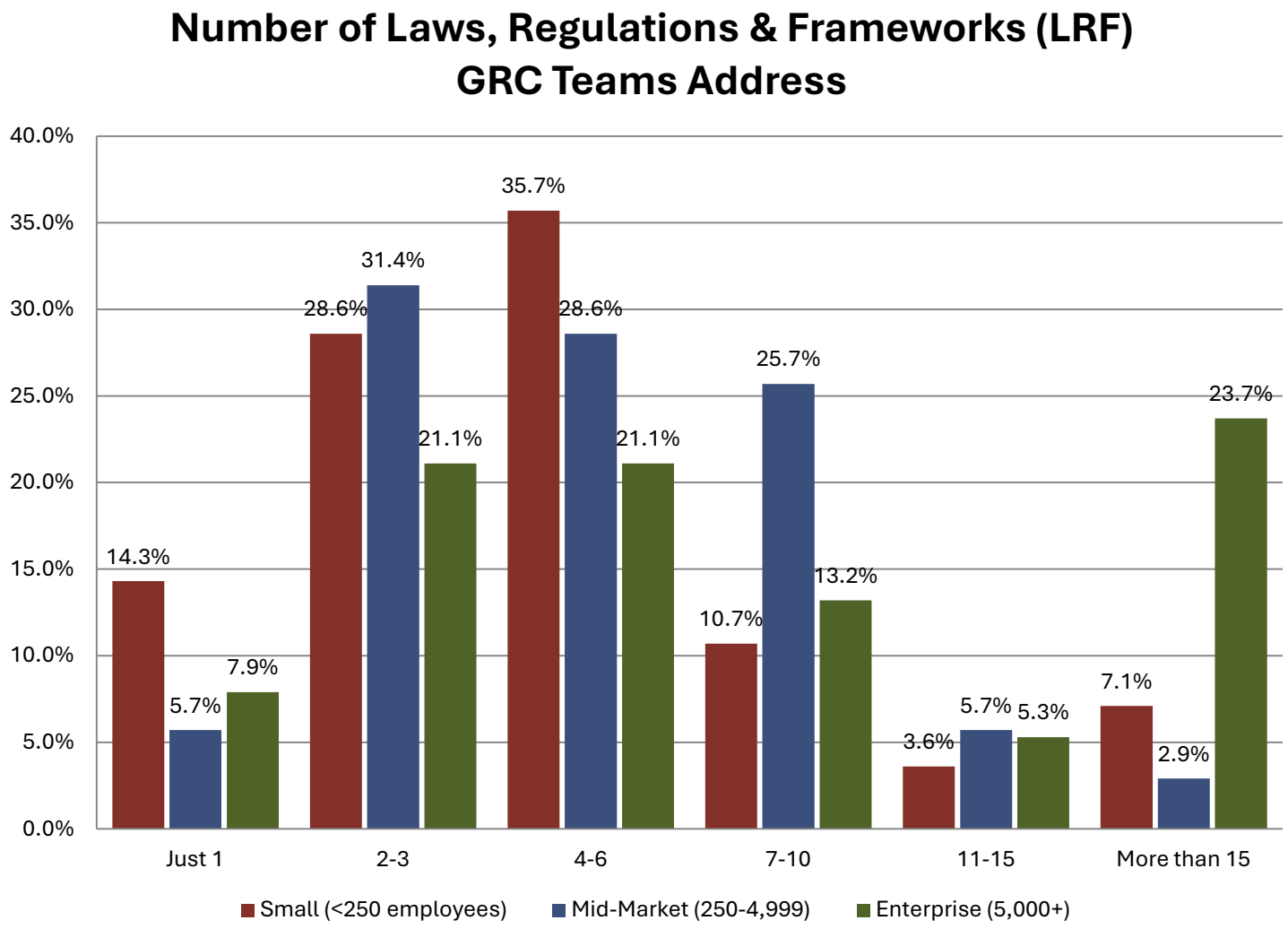


Compliance Obligations

43% of organizations must comply with laws and regulations in multiple countries simultaneously, another 23% operate under one primary jurisdiction that drives a broader compliance program, and 32% operate solely within a single jurisdiction.

Multinational complexity rises sharply with size where only 25% of small organizations report multi-country compliance obligations, compared with 40% of mid-market organizations and 58% of enterprises - unsurprising given that larger organizations are more likely to operate across borders, but a useful baseline for gauging whether a given organization's jurisdictional footprint is typical for its size.

62% of organizations track four or more (4+) distinct laws, regulations, or frameworks simultaneously. Framework count scales sharply with size where enterprises are more than three times as likely as small organizations to manage more than fifteen frameworks at once (24% versus 7%), while small organizations are far more likely to manage a lighter load of two to six frameworks.

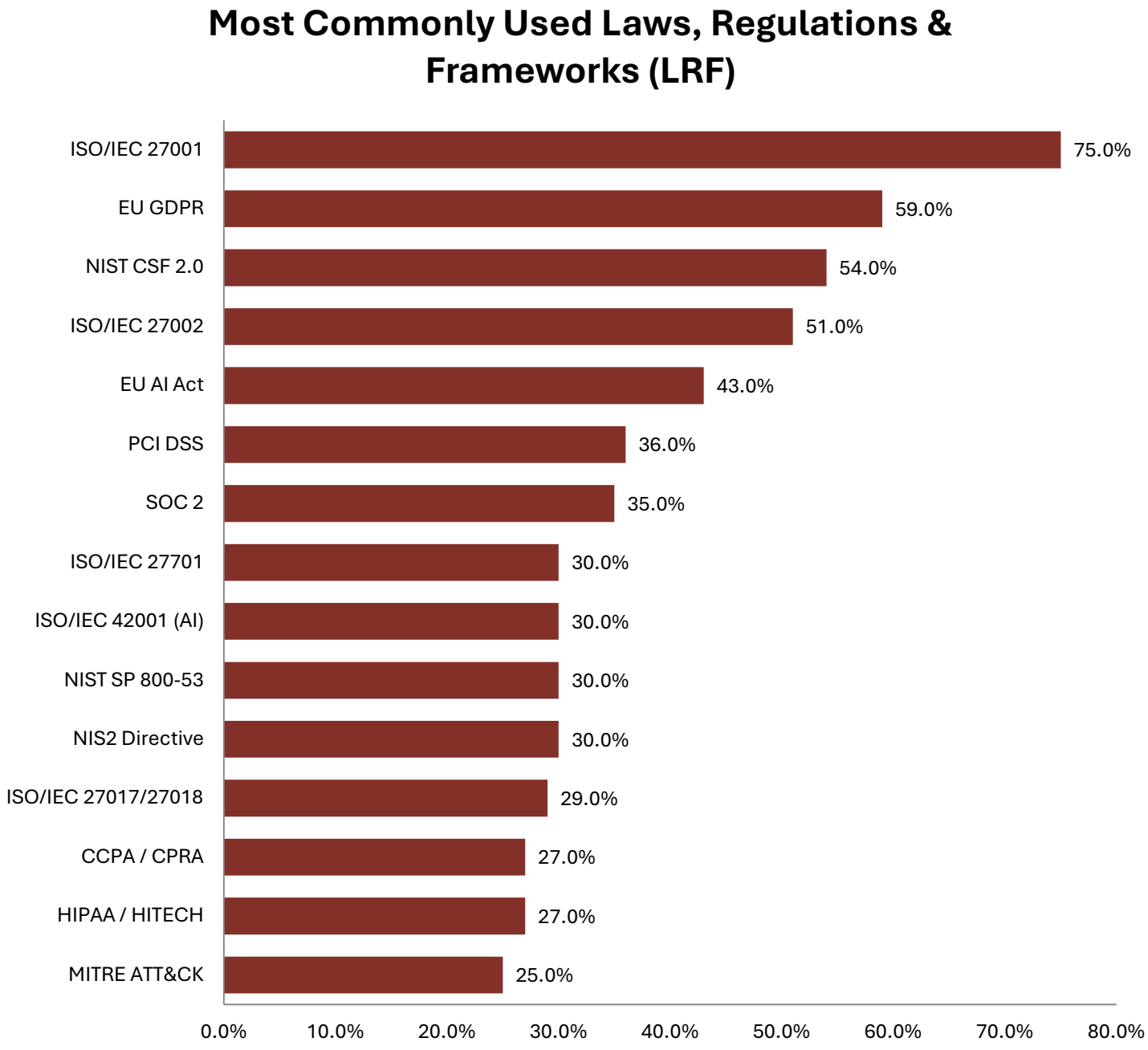


Common Requirements

The set of "common requirements" seen by organizations is expected.

ISO/IEC 27001 is close to universal (75%), followed by EU GDPR (59%), NIST CSF 2.0 (54%), and ISO/IEC 27002 (51%); the EU AI Act already sits at 43% and is ahead of longer-standing standards such as PCI DSS (36%) and SOC 2 (35%).

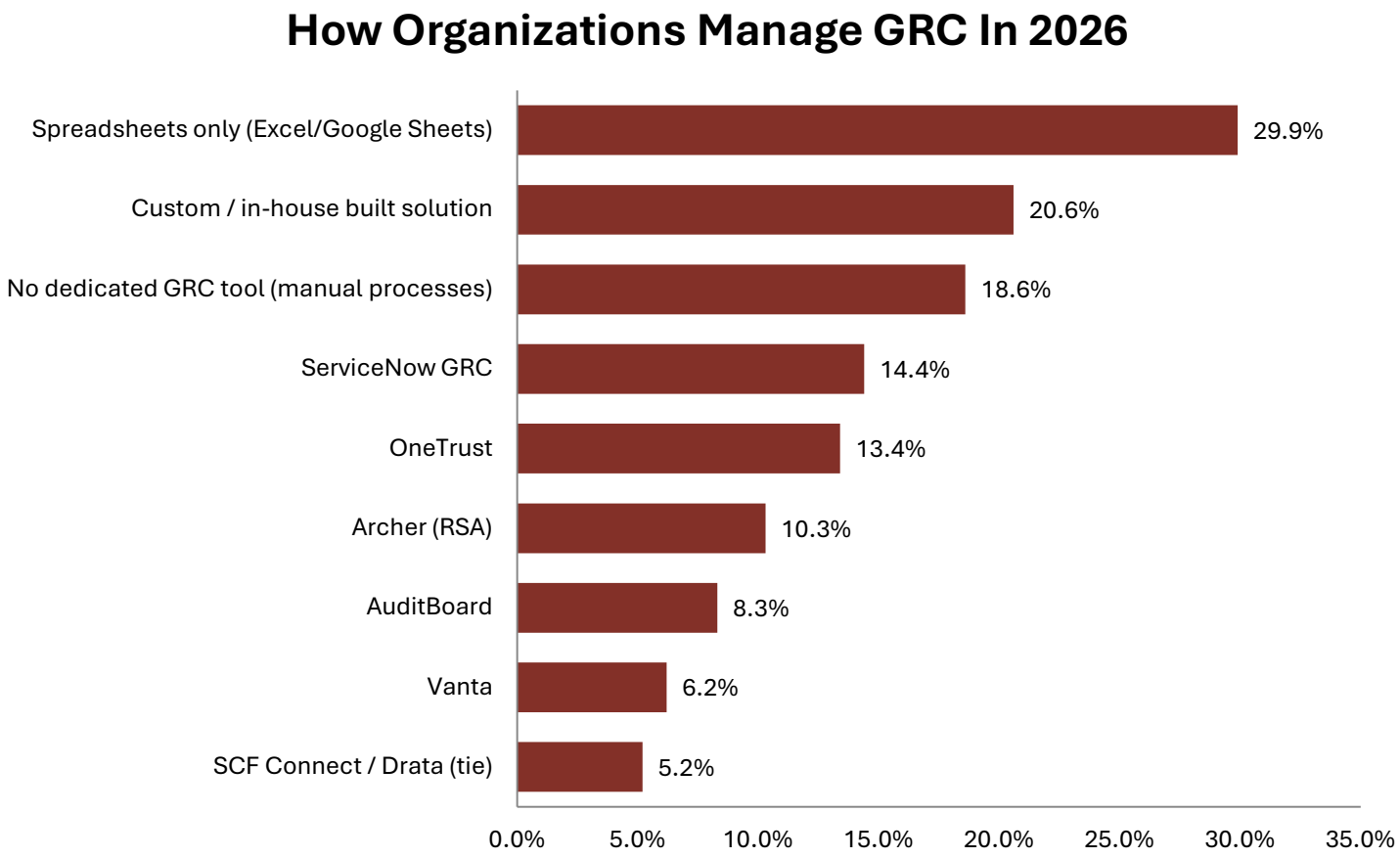
The top fifteen (15) laws, regulations and frameworks tracked by the survey, plus write-in responses:



GRC Tooling

The tooling landscape is fragmented.

Nearly 30% of organizations manage GRC work in spreadsheets alone, and another 19% have no dedicated GRC tool at all - meaning close to half the survey (48%) is running governance, risk, and compliance without purpose-built software. Among named commercial platforms, no single vendor breaks 15% adoption; ServiceNow GRC (14%) and OneTrust (13%) lead a long tail of niche and point solutions, and 21% of organizations have built a custom or in-house solution instead:



Tooling choice varies distinctly by size. Enterprises lean heavily toward named commercial platforms - OneTrust (28%), ServiceNow GRC (26%), and Archer (16%) are each far more common at enterprises than at smaller organizations, where each platform accounts for under 5% - while mid-market organizations report the highest reliance on spreadsheets alone (32%, versus 21% at small organizations and 16% at enterprises), and small organizations report the highest share with no dedicated GRC tool of any kind (21%, versus 12% at enterprises).

Useful insights:

- GRC-platform satisfaction overall averages just 2.85 out of 5, the lowest-rated metric anywhere in this survey; and
- There is a size-based pattern behind that number, where mid-market organizations report the least satisfaction while having the heaviest reliance on spreadsheets.

Resourcing Constraints

In this part of the survey, practitioners were asked to rate, on a 1-5 scale, how well their organization is resourced to address the realities of staying secure, compliant, and resilient (e.g., how seriously executive leadership treats the mission, whether tooling and staffing are adequate, and how mature the overall program is.)

Executive Leadership Seriousness

Overall, executive leadership seriousness averages 3.51 out of 5 (slightly above average).

54% of practitioners rate their leadership a 4 or 5 ("takes it seriously" to "leads by example"), while 18% rate it a 1 or 2 (effectively "lip service"). This is a genuinely mixed picture rather than a uniformly good or bad one, and the average conceals a pronounced dip among mid-market organizations specifically, where only 40% rate leadership a 4 or 5, versus 60-63% at both smaller and larger organizations.

Tooling Adequacy

Practitioners rate the adequacy of their current cybersecurity tooling relative to their organization's actual needs at 3.42 out of 5 on average.

49% rate it a 4 or 5, while 14% rate it a 1 or 2. This is the least polarized of the four resourcing measures, where most organizations sit in the "adequate but not best-in-class" middle of the scale and, unlike the other three resourcing measures, tooling adequacy does not dip sharply for mid-market organizations (3.31 versus 3.44 small and 3.50 enterprise).

Staffing Adequacy

Staffing is the weakest-rated resourcing measure of the four: 2.90 out of 5 overall.

38% of practitioners rated their staffing a 1 or 2 ("severely understaffed," "critical skill gaps") and only 32% rating it a 4 or 5. Staffing adequacy is also where the mid-market dip is most extreme, where mid-market organizations average 2.60, with 54% rating staffing a 1 or 2, compared with 26% at small organizations and 32% at enterprises.

Program Maturity

Asked to describe the overall maturity of their cybersecurity program, practitioners average 3.04 out of 5.

36% describe their program as a 4 or 5 ("advanced" to "world-class, optimized"), while 30% describe it as a 1 or 2 ("informal, ad hoc" to a low level above that). Program maturity again dips at mid-market organizations (2.74 versus 3.30 small and 3.13 enterprise).

Risk Management Practices

In this part of the survey, practitioners were asked how risk management is actually practiced day to day:

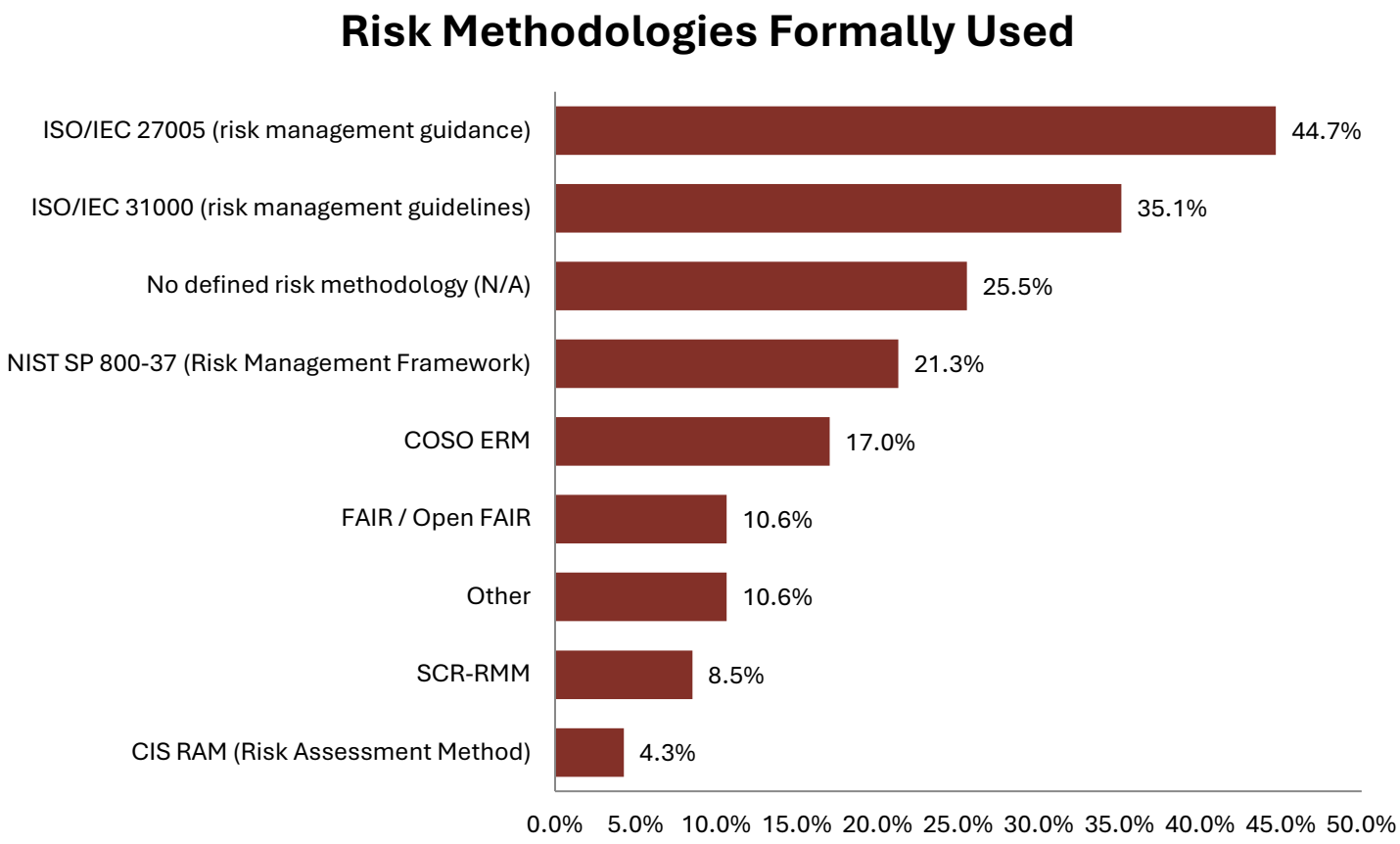
- Which formal methodologies organizations align with;
- Whether materiality criteria are defined;
- How risk is reported to leadership; and
- Whether new technology is validated against security controls before going into production.

Risk Methodology Adoption

A quarter of organizations (26%) do not align with any defined risk methodology at all. Among those that do, ISO/IEC 27005 (45%) and ISO/IEC 31000 (35%) are the two most common formal methodologies, followed by NIST SP 800-37 (21%) and COSO ERM (17%); FAIR/Open FAIR (11%) and the SCF's own Security, Compliance & Resilience Risk Management Model (9%) are used by a smaller minority.

Formal methodology use rises with organization size in a specific way:

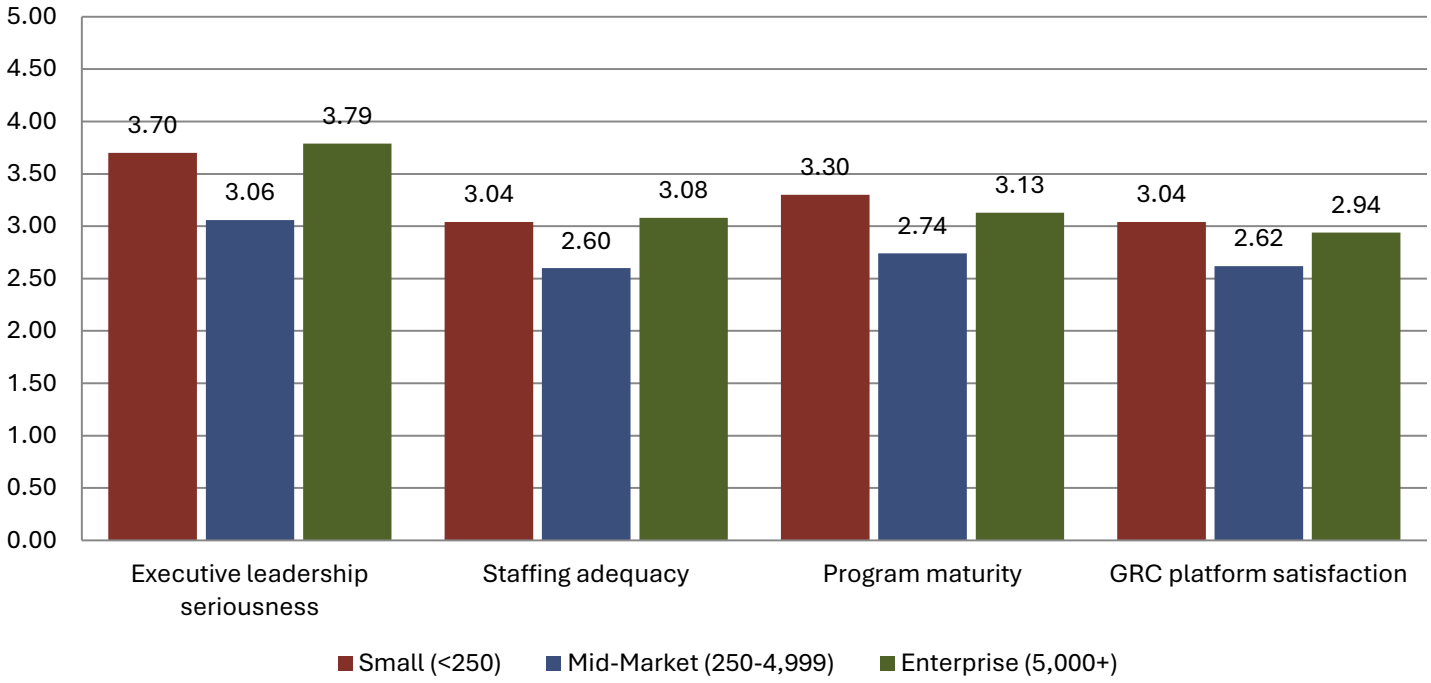
- COSO ERM usage climbs sharply from 2% at small organizations to 12% at mid-market and 23% at enterprises; and
- ISO/IEC 27005 climbs similarly (26% small, 32% mid-market, 42% enterprise).



Useful insights:

- Selecting “no defined methodology” was most common at mid-market organizations specifically (24%, versus 17% at both small organizations and enterprises); and
- This is one of several places in this survey where mid-market organizations report a gap that neither smaller nor larger peers share.

The Mid-Market Dip: Average Ratings by Organization Size



Materiality Criteria Definitions

Just under half of organizations (47%) have defined materiality criteria to frame cybersecurity risk-management decisions, 38% do not, and 14% are unsure. This is one of the few measures in this survey that does not vary meaningfully by size band (48% small, 46% mid-market, 49% enterprise have defined criteria). This suggests materiality-criteria adoption is closer to a genuinely industry-wide coin flip than a size-driven outcome.

How Risk is Reported to Leadership

Asked to place their risk-reporting approach on a scale from purely qualitative (1) to fully quantitative, financially linked (5), practitioners average 3.05 out of 5 - a genuine middle ground, with 40% clustering at the midpoint (3) alone. Only 32% report a 4 or 5 (meaningfully quantitative), while 28% report a 1 or 2 (largely qualitative).

Enterprises report the most quantitative risk reporting of the three bands (mean 3.19, with 38% rating a 4 or 5), against 3.04 for small organizations and 2.91 - the lowest of the three - for mid-market organizations.

Validating Controls Before Production

Only 37% of organizations validate all applicable security controls before new technology goes to production; 45% validate only for technology deemed “critical,” and 18% do not validate at all before go-live.

Enterprises are the most rigorous of the three bands by a meaningful margin where only 11% of enterprises report no pre-production validation at all, compared with 16% at small organizations and 26%.

Useful insights:

- Mid-market organizations once again report the weakest practices on this part of the survey.

Industry Challenges & Emerging Trends

In this part of the survey, practitioners were asked about the forces shaping cybersecurity and GRC worldwide:

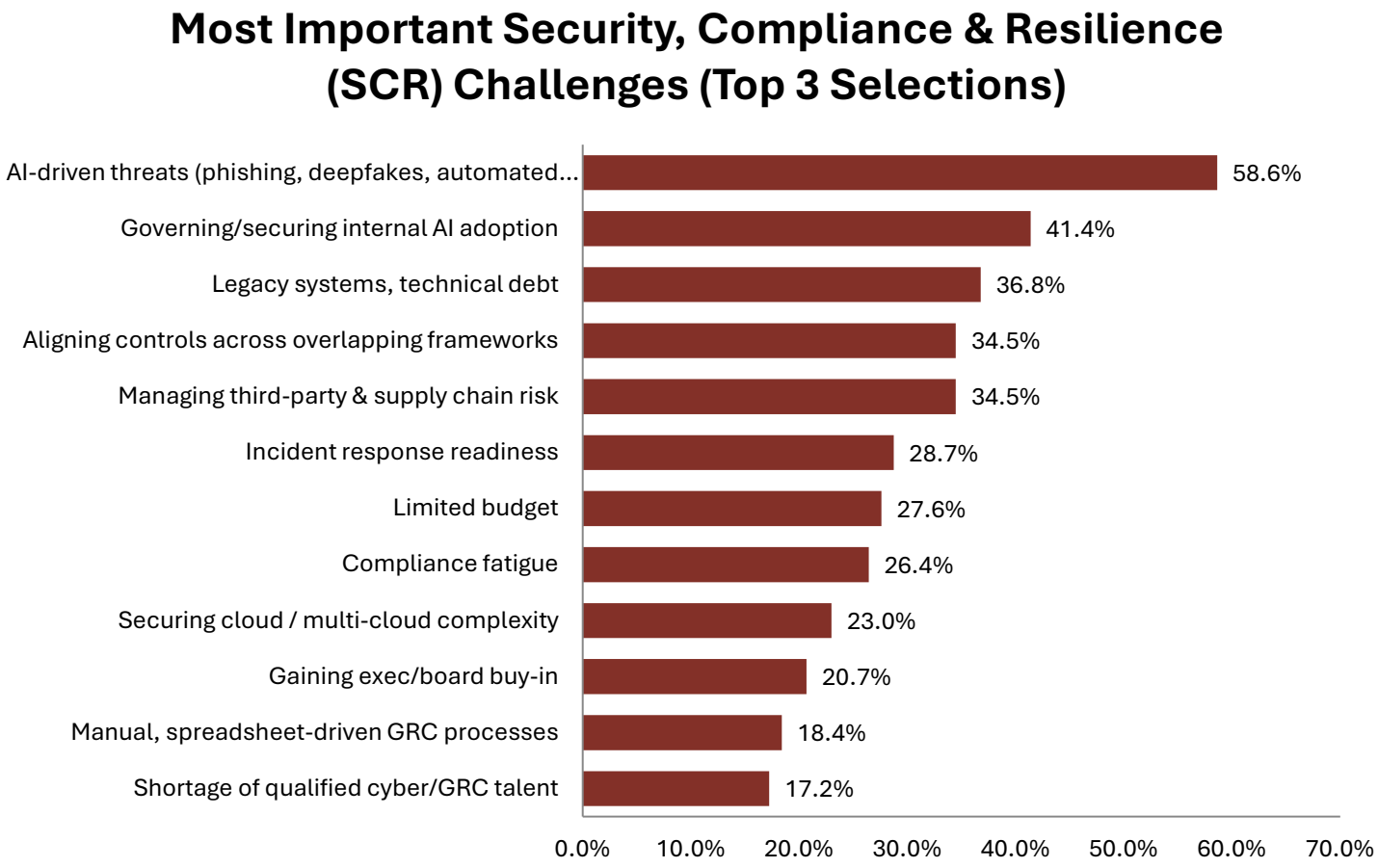
- The top challenges organizations face;
- The state of GRC engineering and automation;
- Generative AI adoption and governance;
- Zero Trust progress; and
- Post-quantum cryptography readiness.

Top Challenges Facing GRC

Asked to select their top three challenges from a list of nineteen, practitioners rank AI-driven threats (e.g., phishing, deepfakes, and automated attacks) as the single most common top-three challenge by a wide margin (59%), followed by governing and securing internal AI adoption (41%) and legacy systems and technical debt (37%).

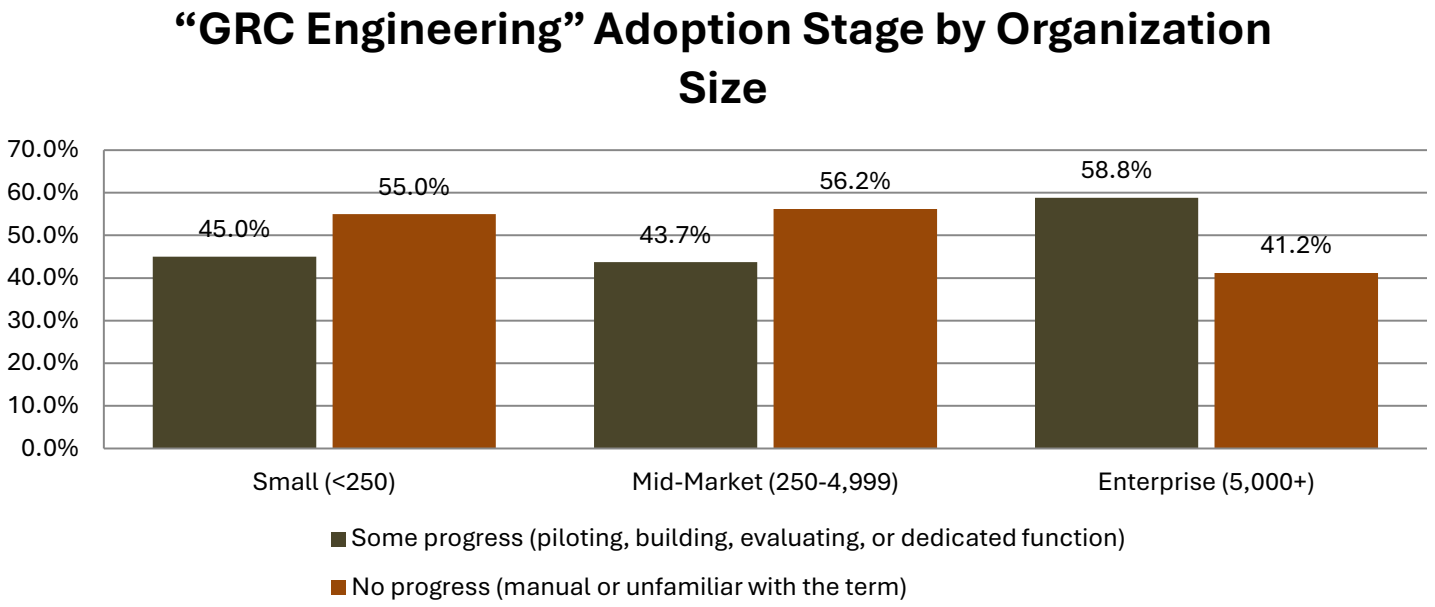
Aligning security controls across overlapping frameworks and managing third-party and supply-chain risk are tied for fourth (34% each), ahead of incident-response readiness (29%), limited budget (28%), and compliance fatigue (26%). Notably, the top two challenges are both AI-related, meaning AI now dominates the top-of-mind challenge list for practitioners in a way no other single issue does.

The challenge list also diverges meaningfully by organization size, and mid-market organizations report the highest rate of several specific pressures, where AI-driven threats are cited by 54% of mid-market respondents versus roughly 34% at both smaller and larger organizations; managing third-party and supply-chain risk is cited by 42% of mid-market respondents versus 17% (small) and 14% (enterprise); and incident-response readiness is cited by 34% of mid-market respondents versus just 7% of enterprise respondents. This pattern of mid-market organizations citing more top-three challenges across more categories than either smaller or larger peers is consistent with the broader mid-market squeeze examined.

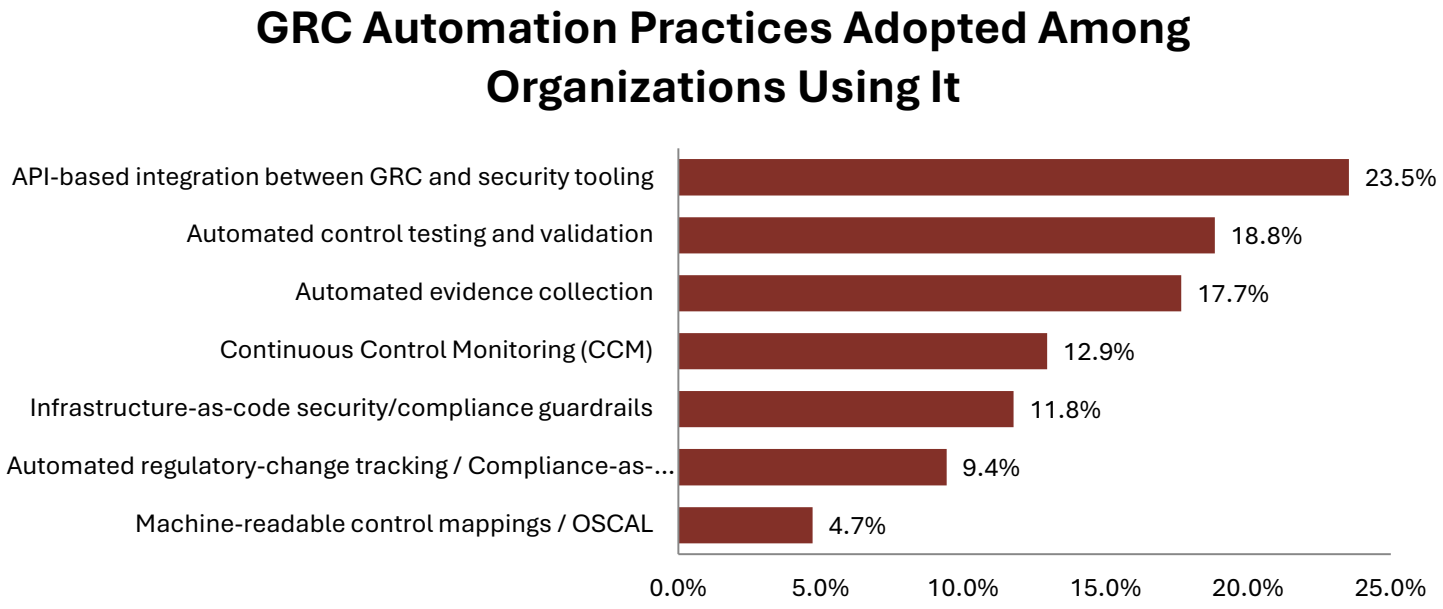


GRC Engineering

Asked directly about "GRC engineering" (e.g., the practice of applying software engineering practices such as automation, code, APIs, and continuous monitoring to governance, risk, and compliance) 17% of practitioners say they are not familiar with the term at all, and a further 33% say their GRC processes remain largely manual. Only 7% report a dedicated GRC engineering function with these practices embedded, with the remaining 43% spread across piloting, actively building, or evaluating the concept. Enterprises report the most progress of the three bands (59% at some stage of active adoption, versus 45% small and 44% mid-market).



Asked about specific automation practices rather than the broader concept, the picture is similarly early-stage where 51% of organizations have adopted none of the ten listed automation practices at all. Among organizations that have adopted at least one, API-based integration between GRC and security tooling is the most common (24%), followed by automated control testing and validation (19%) and automated evidence collection (18%); machine-readable control mappings and OSCAL formats remain rare (5%).



Generative AI

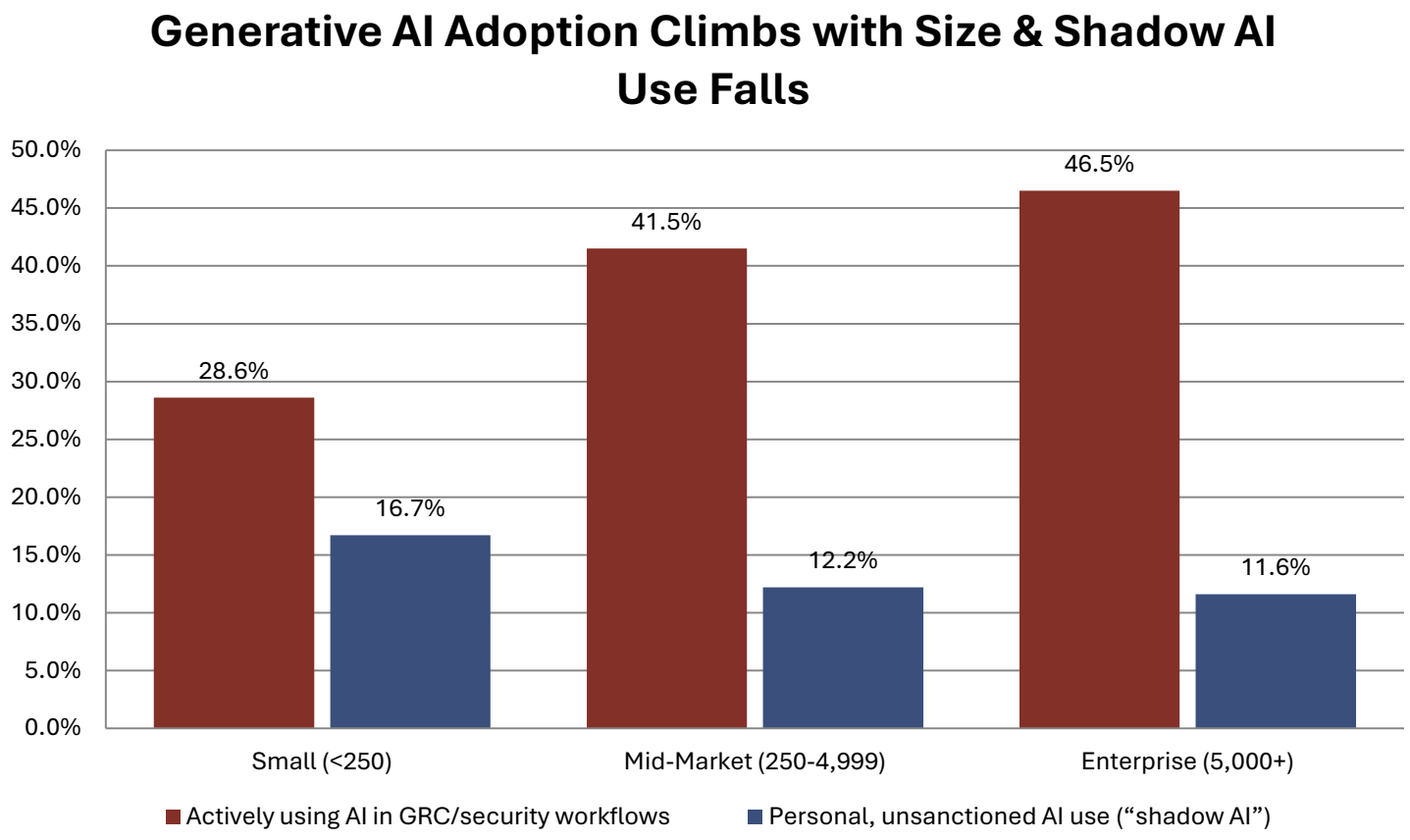
Generative AI has moved past the pilot stage for most of this sample where 56% of organizations report actively using AI tools in compliance, GRC, or security workflows today, and adoption climbs steadily with organization size, from 29% of small organizations to 47% of enterprises.

Governance has not fully caught up with adoption: only 6% of organizations have a formal AI governance program in place that has also been externally validated, though a further 61% report some form of formal or in-progress governance effort under way, and 7% have no current plans for one at all. Shadow AI (e.g., personal use of AI tools without organizational sanction) runs in the opposite direction of formal adoption: it is most common at small organizations (17%) and least common at enterprises (12%), consistent with smaller organizations having less formal AI policy in place to enforce.

Practitioners' concerns about AI are specific and largely about people and process rather than the technology itself: data-privacy risk from AI tools processing sensitive information and employees misusing AI in ways that create security or compliance risk are each cited by 59% of respondents as a top-three concern, ahead of inadequate governance/"shadow AI" (54%), AI hallucinations producing incorrect guidance (45%), and adversaries using AI to accelerate attacks (45%).

Concern about AI also varies by size in a pattern worth flagging where mid-market organizations report the highest rate of concern about data-privacy risk (61%) and employee misuse (59%) of any band, while small organizations report the lowest rate of concern on nearly every listed AI risk - plausibly reflecting less formal AI governance awareness at smaller organizations rather than genuinely lower risk. One respondent's view of agentic AI specifically captures a common practitioner skepticism toward the vendor narrative around AI:

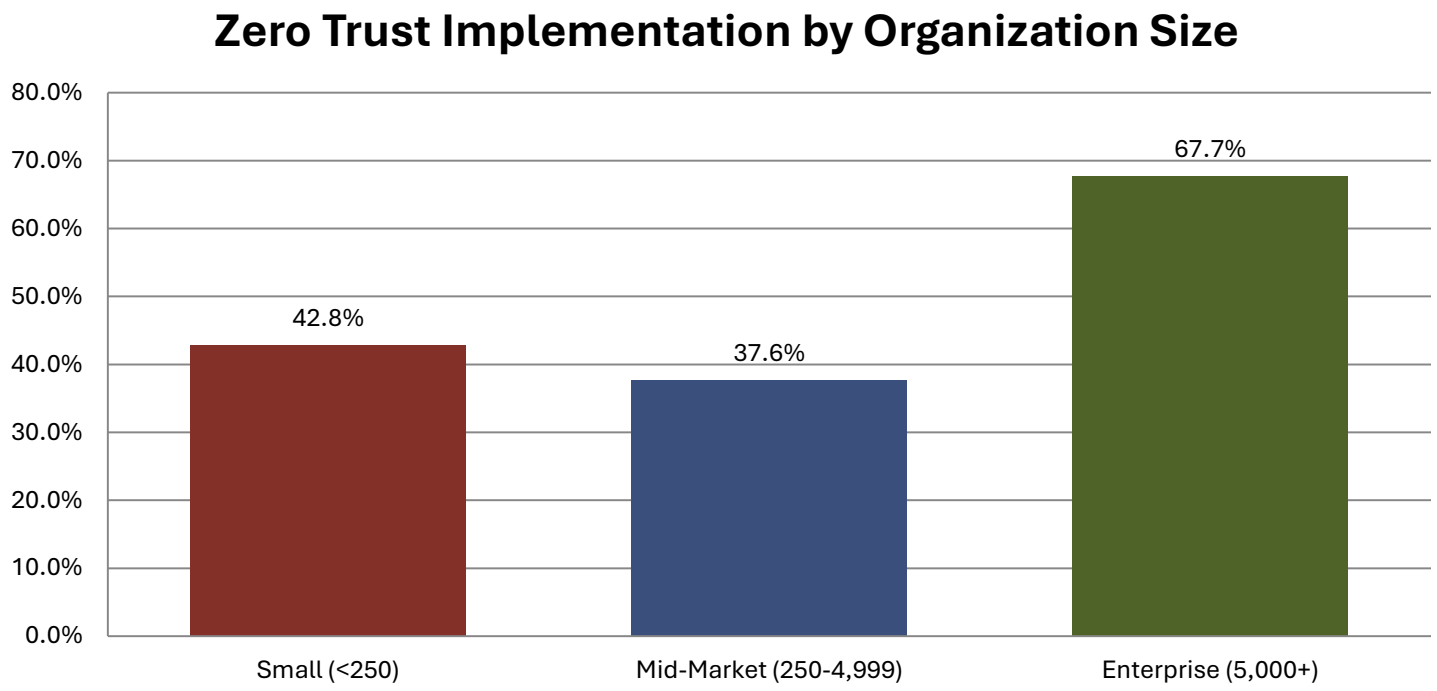
> *"Agentic AI. It's hyped as if agents can do things that other monitoring or NAC cannot, and in practice is a giant risk of unaccountable actions and broad permissions. Human "in" the loop is a joke and can't provide proper attention or oversight."*



Zero Trust Network Architecture (ZTNA)

13% of organizations have fully implemented ZTNA principles across their environment, and a further 37% are actively implementing it with measurable milestones; 11% have a roadmap but have not yet begun, 10% are evaluating it with no formal plan, 14% have discussed it without making it a priority, 7% are not pursuing it, and 7% are not familiar with ZTNA principles at all.

Progress is heavily skewed by organization size: enterprises are far ahead of both other bands, with 68% reporting full or active implementation, compared with 43% at small organizations and just 38% at mid-market organizations.



Post-Quantum Cryptography (PQC)

Concern about quantum-computing risks such as Harvest Now, Decrypt Later (HNDL) is modest overall: 2.76 out of 5 on average, with only 26% rating their concern a 4 or 5 and 40% rating it a 1 or 2. Concrete preparation lags concern further still: only 6% of organizations have an active post-quantum cryptography (PQC) migration program under way, and a further 16% are in early evaluation or planning; 30% have no current plans at all, and 22% say PQC readiness is outside their area of responsibility or knowledge.

A prerequisite step in PQC is inventorying where and how cryptography is used across the organization. Only 7% report a complete cryptographic inventory with a crypto-agility plan, while 33% have no plans to build one.

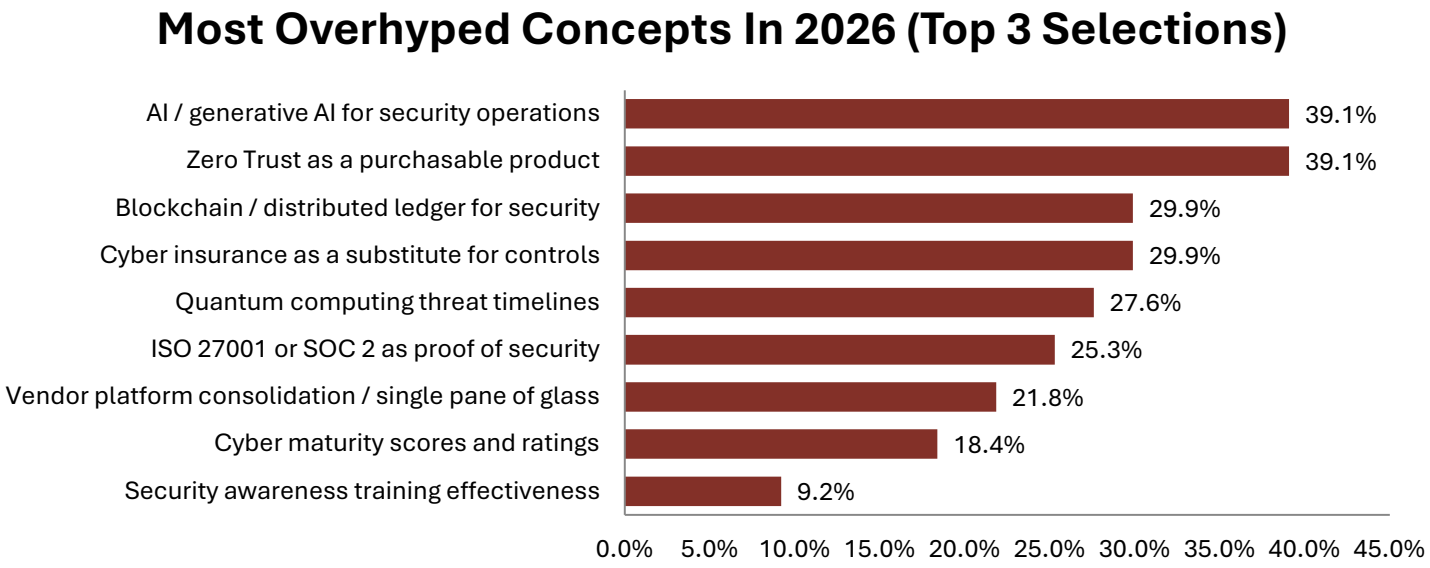
Enterprises again lead where 12% have an active PQC migration program, versus 5% at small organizations and, notably, zero at mid-market organizations - none of the 32 mid-market respondents to this question report an active PQC program. Mid-market organizations also report the lowest quantum concern of the three bands (mean 2.31, versus 2.90 small and 3.09 enterprise), which is consistent with either a genuinely lower risk profile or, more likely given the pattern elsewhere in this report, less bandwidth to think about a threat that has not yet materialized while managing more immediate resourcing gaps.

Industry Hype

In this part of the survey, practitioners were asked to speak candidly about where the cybersecurity and GRC industry is getting ahead of itself - in the survey's own words, “there are no wrong answers here, we want the candid practitioner view.”

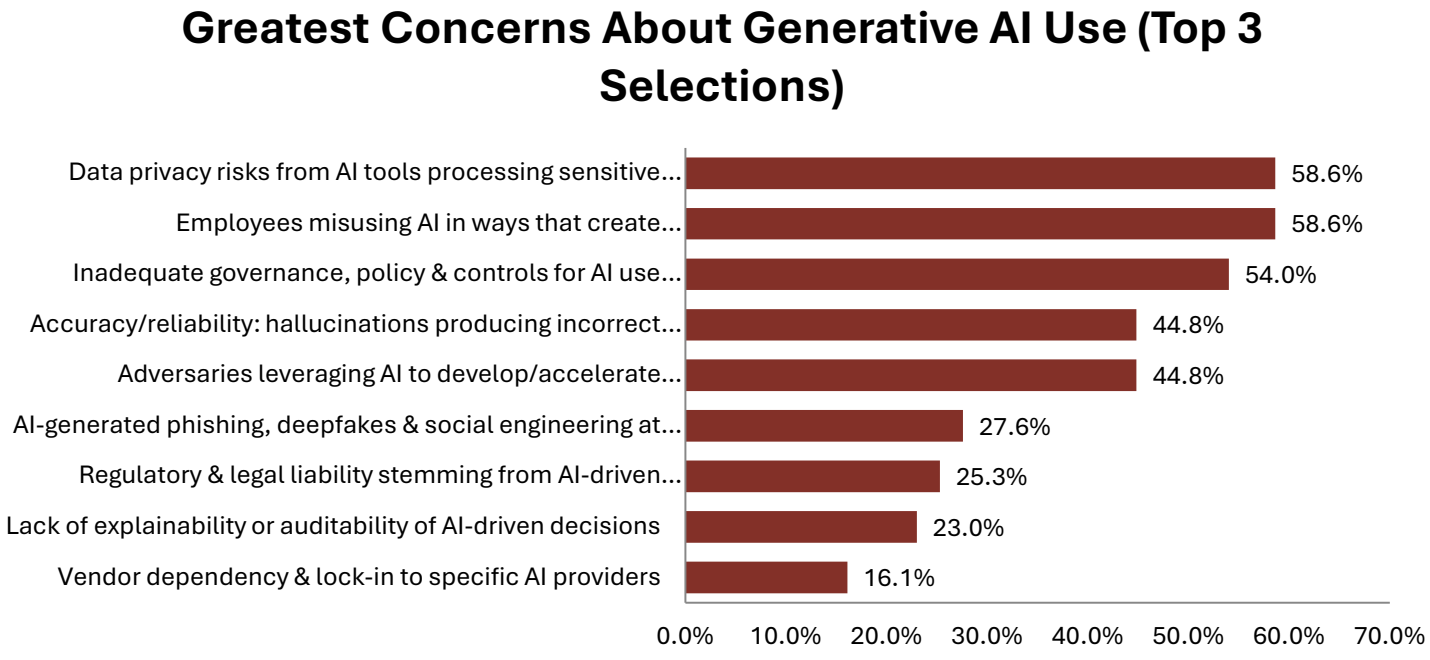
Most Overhyped Concepts

Generative AI for security operations and “Zero Trust as a purchasable product” tie for the single most overhyped concept in the field, each named by 39% of respondents. Blockchain for security and cyber insurance as a substitute for controls tie just behind at 30% each, followed by quantum-computing threat timelines (28%) and ISO 27001 or SOC 2 treated as proof of security (25%). Only 13% of respondents said none of the listed concepts are overhyped.



Most Distrusted Concepts

“AI-powered” or “AI-native” product labeling is the single most distrusted marketing claim, named by 67% of respondents - well ahead of “next-generation” or “revolutionary” marketing (59%) and “military-grade” or “unbreakable” security claims (47%). Certifications treated as proof of competence (44%) and “Zero Trust” used as a buzzword (38%) round out the top five.



Useful insights:

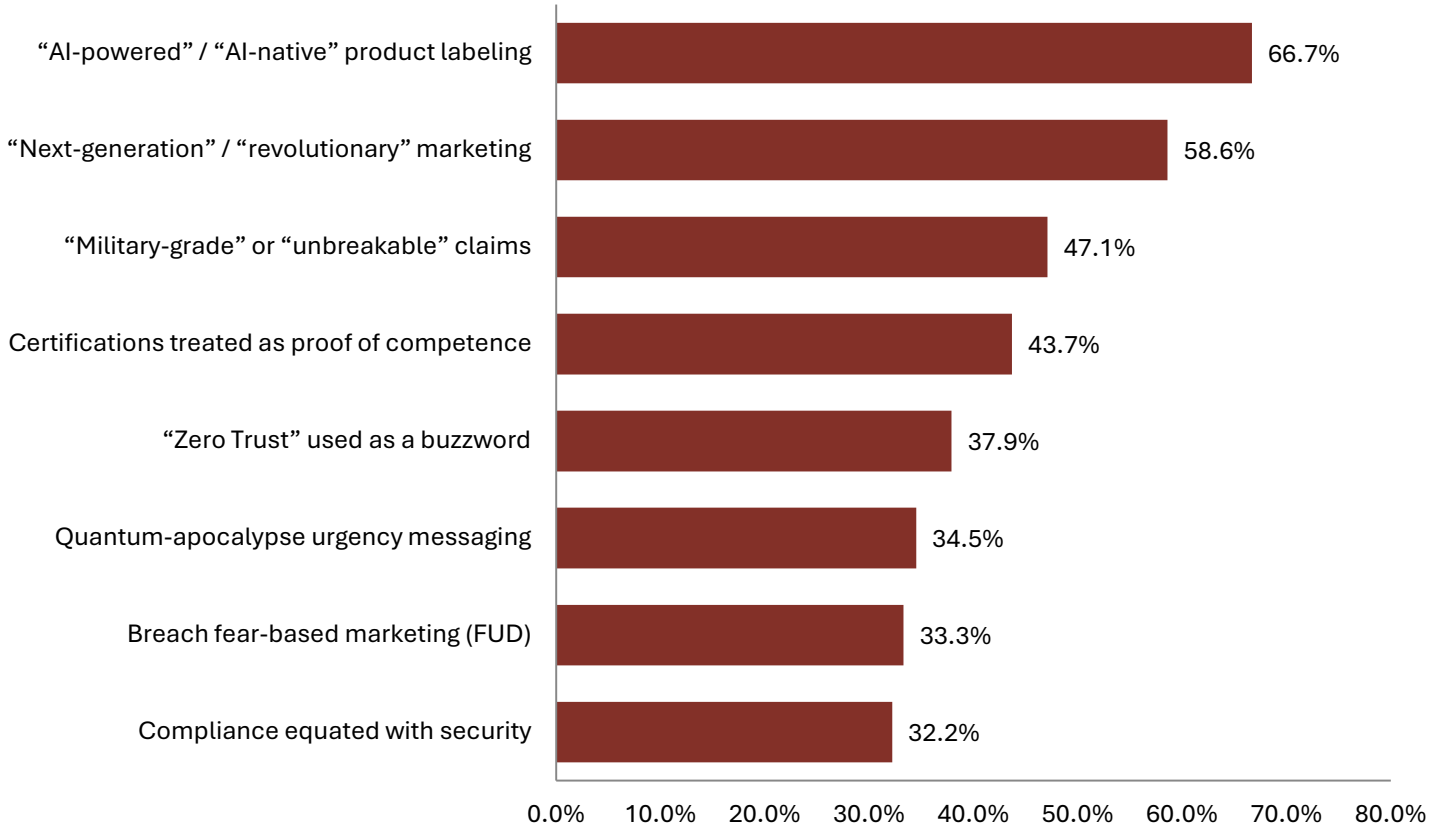
- The same practitioners who report their organizations actively using AI in security and compliance workflows are also the ones most distrustful of AI marketing claims; and
- This is a real distinction between using the underlying technology and buying into vendor positioning around it, not a contradiction.

Given an open-ended chance to name a specific tool, framework, certification, or trend they believe deserves more skepticism, several respondents converged on a similar theme:

> *"The industry should be more skeptical of 'SOC 2 certified' being used as shorthand for secure. A SOC 2 Type 2 report is useful evidence within a defined scope, not a security force field. It should support due diligence, not replace it."*

> *"I don't believe the update to frameworks in relation to the speed of AI is happening. I think we should see updates to the ISO and SOC frameworks in relation to AI usage every year if not every 2 at most."*

Marketing Claims Practitioners Distrust Most



METAFRAMEWORKS

In this part of the survey, practitioners were asked which metaframework(s) organizations use, why, what capabilities matter most, how satisfied users are, and what would make the approach more valuable.

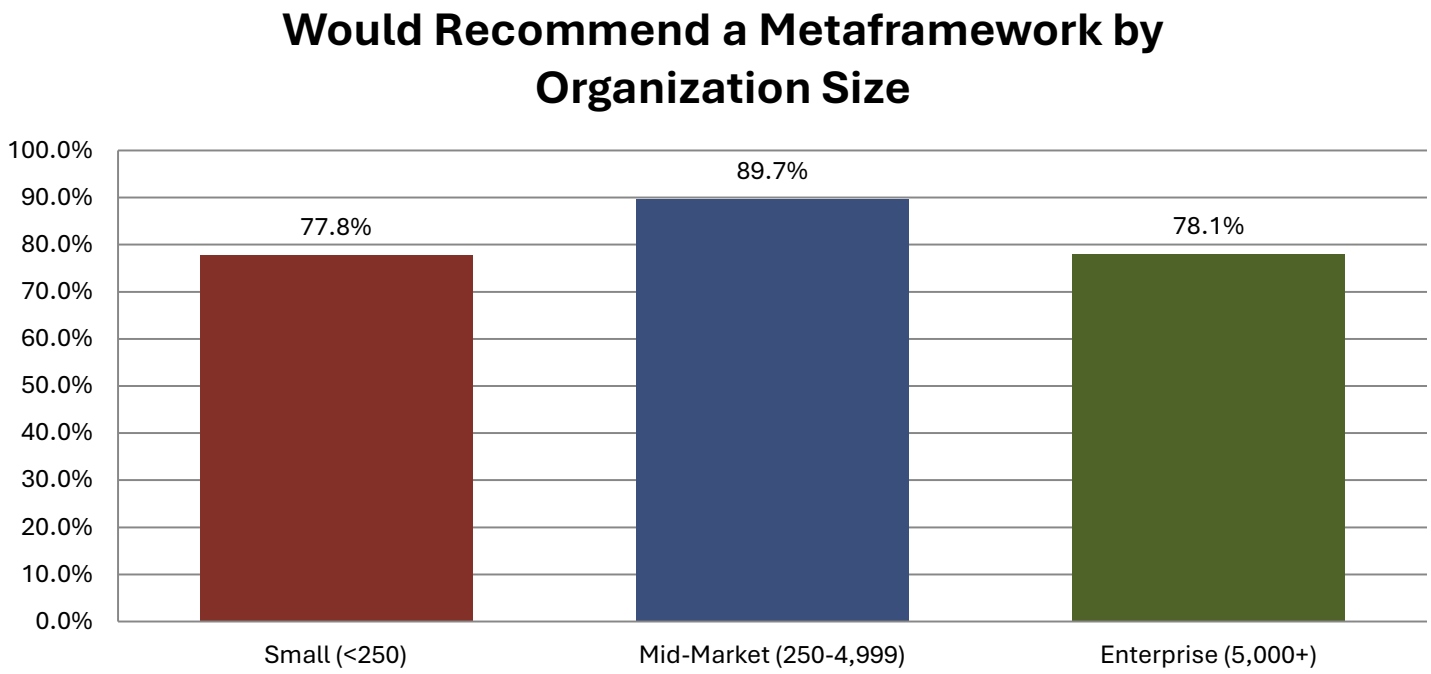
METAFRAMEWORK ADOPTION LANDSCAPE

Among the respondents who answered this question, the Secure Controls Framework (SCF) is the dominant metaframework in use, well ahead of HITRUST CSF and the Unified Compliance Framework. 34% report using no metaframework at all and 8% cite a custom or other approach.

SCF adoption is highest among mid-market organizations (42% of the band use it) and lowest among small organizations (29%), while "no metaframework" climbs steadily with size, from 14% at small organizations to 28% at enterprises.

Useful insights:

- Decreased metaframework use in larger organizations indicates those organizations often have the resources to build and maintain a bespoke, in-house control mapping instead of adopting an off-the-shelf one.



REASONS FOR SELECTING A METAFRAMEWORK

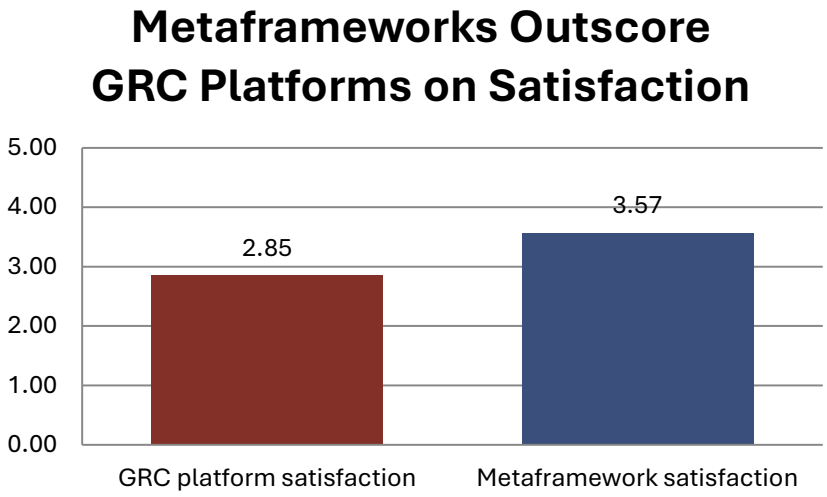
The reason practitioners give for adopting a metaframework is overwhelmingly practical rather than about cost or mandate where 74% cite consolidating many frameworks into a single control set as a primary reason. This consolidation motive is far stronger at mid-market and enterprise organizations than at small organizations, consistent with smaller organizations having a lighter framework load to consolidate in the first place.

Asked which capabilities their metaframework provides, or which they most want from one, control-to-framework crosswalk mappings (72%) and regular updates that track new laws and regulations (66%) top the list by a wide margin, ahead of a capability maturity model (58%), a risk model or risk-assessment method (52%), free or open licensing (49%), and Evidence Request Lists (48%). Machine-readable formats such as OSCAL/JSON remain the least commonly cited capability (28%), consistent with the broader finding that GRC engineering and automation practices are still early-stage across the industry.

Satisfaction & Likelihood To Recommend

Where GRC platforms disappoint, metaframeworks perform noticeably better by comparison. Metaframework satisfaction is meaningfully higher than GRC-platform satisfaction and the gap shows up clearly in willingness to recommend the approach where 82% of respondents would "definitely" or "probably" recommend a metaframework to a colleague, with zero respondents saying they would not.

Recommendation rates by size band add a genuinely surprising wrinkle to the mid-market story that runs through this report where mid-market organizations are the most enthusiastic endorsers of the metaframework approach of the three bands (90% would definitely or probably recommend it), ahead of enterprises (78%) and small organizations (78%) - even though mid-market organizations report the weakest program health on almost every other measure in this survey. A plausible read is that a metaframework is one of the few available force-multipliers at the mid-market resource level, delivering outsized relative value precisely because the underlying program is under strain.



Practitioners most want an interactive, searchable control explorer and direct integration with GRC platforms (37% each), followed by more industry-specific or sector-tailored guidance (36%) and pre-built policy templates tied to controls (35%) - the same integration and usability themes raised about GRC platforms generally.

In their words:

> *"SCF has helped us consolidate overlapping requirements into a more coherent control environment, but the real challenge is operationalizing it. Organizations need clearer implementation guidance, evidence expectations, testing procedures, training, and stronger GRC integrations. The SCF should reduce duplicate work and improve control effectiveness, not simply create one extremely impressive spreadsheet."*

> *"Deduplication and pin-point tailoring appear to be an issue, but this may be a user-education thing. We chose the myriad of frameworks listed above, and ended up with 6,000+ questions to address. When the assessor ran some deduplication, we got the list down to around 650 questions. ERL should be less than or equal to that, which is still a huge uplift."*

> *"My team likes the concept of using a metaframework, however, our process to date has been manual which brings operational/scalability challenges. Because of this we've struggled with scaling the test once/apply to many concept.*