GRACE
From Chaos to Continuous Compliance

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

The GRACE Crosswalk Report:

From SOC 2 to ISO 27001: Which Compliance Requirements Are Already Covered?

letsconnect@ampcuscyber.com

www.ampcuscyber.com

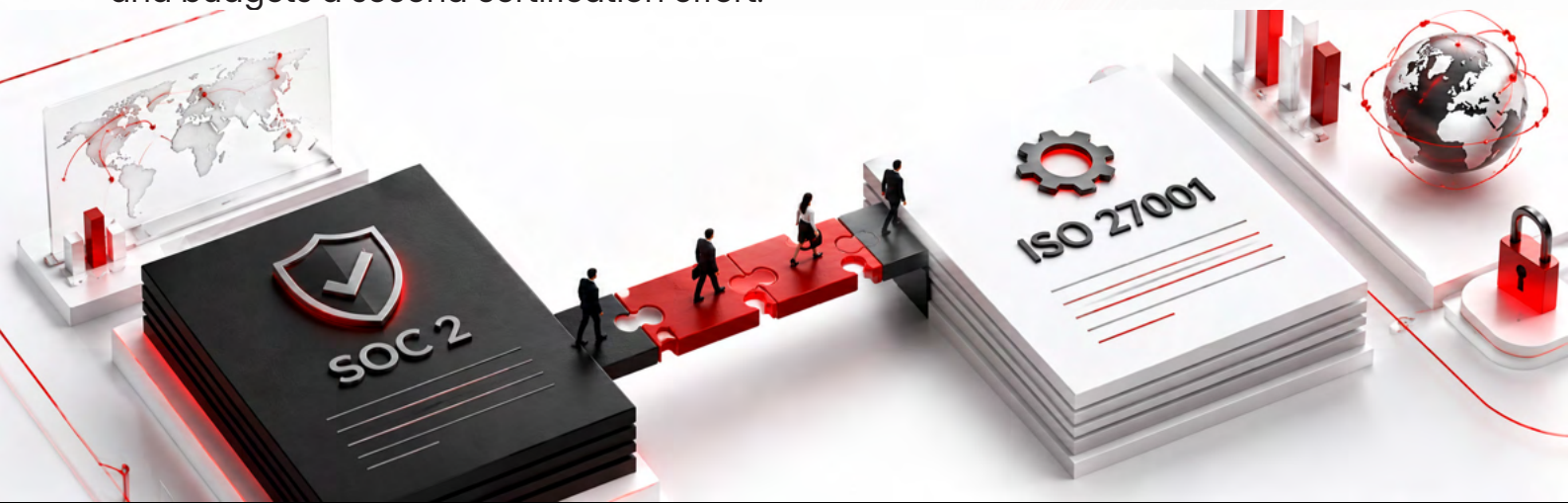
01 Executive Summary:

Security and compliance leaders face a familiar dilemma. Customers in North America ask for a SOC 2 report. Customers in Europe, the Middle East, and Asia ask for ISO 27001 certification. The instinct is to treat these as two separate compliance programs, staffed and budgeted independently. That instinct is costly, because most organizations that already hold a SOC 2 report have, without realizing it, already built a large share of what ISO 27001 requires.

The AICPA, the body that governs SOC 2 through its Trust Services Criteria, has published a formal mapping between those criteria and ISO/IEC 27001, documenting where the two frameworks converge[1,4]. A control-level comparison of the two frameworks, set out in Table 1 of this report, shows that most of the SOC 2 Common Criteria find a direct structural counterpart among ISO 27001:2022's Annex A controls, concentrated in access control, risk assessment, change management, and incident response. That means much of the technical and operational work behind ISO 27001 has often already been designed, implemented, and evidenced during the SOC 2 process.

This report is the GRACE Crosswalk Report. It examines where that overlap genuinely sits, where it does not, and what a security leader needs to build to close the remaining gap. It walks through the structural differences between an attestation (SOC 2) and a management-system certification (ISO 27001), maps the SOC 2 Common Criteria against the four Annex A control themes, and lays out a practical methodology for pursuing both without duplicating the underlying work.

The report also looks at why spreadsheet-based, framework-by-framework compliance management struggles to capture this overlap, and how a control-mapping and continuous-monitoring discipline, the kind a platform like GRACE is built to support, changes the economics of running two frameworks side by side. The intent is not to suggest ISO 27001 is a formality once SOC 2 is achieved. Genuine gaps remain, particularly around the ISMS management system itself. But understanding the size and shape of the overlap changes how a CISO plans, staffs, and budgets a second certification effort.



02 The Current Security Landscape

Enterprise buyers now routinely ask vendors for more than one form of security assurance. A prospect based in the United States may request a SOC 2 Type II report before signing a contract. A prospect headquartered in the European Union or the Gulf may ask for ISO 27001 certification instead, or in addition. Security questionnaires increasingly reference both frameworks by name, and procurement teams treat the absence of as a red flag rather than a minor gap.

Global adoption data reflects this shift. According to the official ISO Survey, the worldwide count of valid ISO/IEC 27001 certificates rose from roughly 48,700 in the 2023 edition to more than 96,700 in the 2024 edition, covering nearly 180,000 certified sites, an increase of close to 100% in a single reporting year[3]. That growth signals that ISO 27001 is no longer framework organizations pursue only when selling into Europe; it is becoming a default expectation in cross-border enterprise procurement.

At the same time, the operational maturity of the programs meant to support this growth is not keeping pace. McKinsey's 2025 Global GRC Benchmarking Survey of corporate leaders found average risk-management maturity scoring only 2.6 out of 4.0 and average compliance maturity scoring 2.9 out of 4.0 across industries, with 42% of respondents saying their IT and GRC systems need improvement and another 15% describing them as absent or lagging entirely[6]. Security leaders are being asked to satisfy more frameworks with governance and tooling that, by their own admission, is not yet built for the job.

The cost of getting this wrong is material. IBM's 2025 Cost of a Data Breach Report puts the global average cost of a breach at 4.44 million US dollars, and the United States average at 10.22 million dollars, with highly regulated industries such as healthcare bearing the highest costs[7]. Compliance frameworks exist to reduce this exposure, but only if the underlying control environment is genuinely operated, not merely documented twice for two different auditors.

03 Understanding the Problem

What Does SOC 2 Evaluates?

SOC 2 is an attestation, not a certification. It is governed by the American Institute of Certified Public Accountants' Trust Services Criteria, first issued in 2017 and updated with revised points of focus in 2022[1]. A licensed CPA firm examines an organization's controls against five possible categories: Security, Availability, Processing Integrity, Confidentiality, and Privacy. Security is mandatory in every SOC 2 report and is evaluated through the nine Common Criteria, CC1 through CC9, covering the control environment, communication, risk assessment, monitoring, control activities, logical and physical access, system operations, change management, and risk mitigation[1,8].

A SOC 2 report describes how controls operated over a defined observation window, typically three to twelve months for a Type II report. It results in a report, not a certificate, and it is generally shared under NDA with specific customers rather than displayed publicly.

What Does ISO 27001 Requires?

ISO/IEC 27001 is an international standard, jointly published by ISO and the IEC, for establishing, implementing, maintaining, and continually improving an Information Security Management System, or ISMS[2]. Certification is issued by an accredited certification body after a two-stage audit and is valid for three years, subject to annual surveillance audits. The 2022 revision of the standard organizes its reference control set, Annex A, into 93 controls across four themes: Organizational, People, Physical, and Technological, consolidated down from 114 controls across 14 domains in the 2013 version[2,5]. Eleven controls are new to the 2022 revision, including threat intelligence, cloud security, and data leakage prevention[5]. Annex A is a reference menu, not a mandatory checklist. Organizations select applicable controls based on a formal risk assessment and document their decisions, including any exclusions, in a Statement of Applicability. Clauses 4 through 10 of the standards, covering context, leadership, planning, support, operation, performance evaluation, and improvement, are mandatory regardless of which Annex A controls apply[2,5].

Why The Two Frameworks Are Structurally Different?

The most important distinction is not in the controls themselves, but in what each framework proves. SOC 2 proves that specific controls operated effectively over a period of time, tested against criteria an organization largely designs itself. ISO 27001 proves that a management system exists, one with defined governance, risk treatment, internal audit, and continual improvement processes, independent of which specific technical controls it selects. This is why an organization can implement nearly every technical safeguard ISO 27001 would require and still fail certification, because the management system wrapper, not just the controls, is what an ISO auditor certifies.

04 Why Traditional Approaches Fall Short

The default path for organizations pursuing both frameworks is to run them as separate projects, often with separate owners, separate evidence repositories, and separate audit timelines. This duplication is rarely intentional. It happens because compliance ownership is often split by framework rather than by control, because policy documents get rewritten in slightly different language for each auditor, and because evidence collected for one audit is not tagged or indexed in a way that makes it discoverable for the next.

A vulnerability scan report gathered to satisfy SOC 2's system operations criteria, for example, may never be linked to the equivalent ISO 27001 technological control unless someone manually makes that connection. McKinsey's benchmarking work points to a structural reason this keeps happening: 42% of surveyed organizations say their IT and GRC systems need improvement, and functions with less senior sponsorship consistently report lower maturity scores across every GRC dimension measured[6]. Under-resourced, fragmented tooling makes it nearly impossible to see, let alone exploit, the overlap between two frameworks.

The result is what practitioners describe as audit fatigue: control owners fielding near-identical evidence requests multiple times a year, security teams re-answering the same questions in different formats, and compliance leads becoming single points of failure because ownership of overlapping controls is unclear. Spreadsheet-based tracking makes this worse. A spreadsheet can document a crosswalk once, but it cannot enforce it, flag when evidence goes stale or automatically route a new piece of evidence to every framework it satisfies. Static mapping documents are a starting point, not an operating model.

The financial and organizational cost compounds over time. Every audit cycle repeats the same manual reconciliation, every new framework added to the roadmap multiplies the tracking burden, and every control owner turnover event risks losing institutional knowledge of which evidence maps were. Traditional, framework-siloed compliance management was built for a world where organizations pursued one certification at a time. Given that a data breach now costs an average of 4.44 million US dollars globally[7], the opportunity cost of a compliance program that cannot demonstrate its controls efficiently is no longer a back-office inconvenience; it is a business risk.

05 The Modern Approach

A crosswalk-driven compliance model starts from a different premise: build one control environment, then map every framework onto it as a different lens, rather than maintaining a separate control set per framework. In practice this means treating SOC 2's Common Criteria and ISO 27001's Annex A themes as two views of a shared control library, connected by a documented crosswalk.

How The Frameworks Line Up?

The table below summarizes how the major SOC 2 Common Criteria domains typically align with ISO 27001:2022 Annex A themes. This is a starting reference, not a substitute for organization-specific mapping. The AICPA publishes an official Trust Services Criteria to ISO 27001 mapping document, which NIST also references as a recognized crosswalk resource for organizations aligning SOC-based assurance work with other frameworks[1,4].

SOC 2 Common Criteria	Primary Focus	Corresponding ISO 27001:2022 Annex A Theme
CC1 – Control Environment	Governance, ethics, board oversight, roles and responsibilities	Organizational controls (A.5)
CC2 – Communication & Information	Internal and external communication of security expectations	Organizational controls (A.5), People controls (A.6)
CC3 – Risk Assessment	Identification and analysis of risk to objectives	Organizational controls (A.5), Clause 6 risk assessment
CC4 – Monitoring Activities	Ongoing evaluation of control performance	Technological controls (A.8), Clause 9 evaluation
CC5 – Control Activities	Policies and procedures supporting management directives	Organizational controls (A.5)
CC6 – Logical & Physical Access	Access provisioning, authentication, physical entry	Physical controls (A.7), Technological controls (A.8)
CC7 – System Operations	Monitoring, vulnerability management, incident detection	Technological controls (A.8)
CC8 – Change Management	Authorized, tested, and documented system changes	Technological controls (A.8)
CC9 – Risk Mitigation	Business continuity, vendor risk, contingency planning	Organizational controls (A.5), Technological controls (A.8)

Table 1. Illustrative crosswalk between SOC 2 Common Criteria and ISO 27001:2022 Annex A themes, built from the structure of the AICPA's published Trust Services Criteria to ISO 27001 mapping 1,2. Treat every crosswalk as a draft; final control-to-control mapping depends on how each organization actually implements and evidences its controls.

Evidence Reuse As The Operating Discipline

Two practices separate organizations that capture the overlap from those that do not. The first is defaulting to the stricter requirement when two frameworks disagree on frequency or depth, for example running quarterly access reviews if ISO 27001's risk treatment calls for it even though SOC 2 would accept an annual cadence, so that a single piece of evidence satisfies both auditors. The second is tagging every piece of evidence at the point of collection with every control it could satisfy, so a vulnerability scan report collected once is discoverable under both its SOC 2 and ISO 27001 references rather than re-requested twice.

Industry trade press coverage of practical control mapping illustrates how granular this reuse can get. A published backup-compliance crosswalk, for instance, maps a single set of backup practices, encryption in transit and at rest, access restriction, tested restores, and retention policies, directly against both SOC 2 criteria such as CC6.6 and CC7.1 and ISO 27001 Annex A controls such as A.8.13 and A.8.24, showing that one well-documented control operation can satisfy both auditors simultaneously[9].

06 Key Challenges Organizations Must Address

The ISMS Is Not Optional, And It Has No SOC 2 Equivalent

The single largest genuine gap between the two frameworks sits in ISO 27001's management system clauses (4 through 10): context of the organization, leadership commitment, planning, support, operation, performance evaluation, internal audit, management review, and continual improvement[2]. SOC 2 has no direct equivalent to these requirements. Organizations should budget this as net-new work rather than assuming it will fall out of existing SOC 2 documentation.

The Statement Of Applicability Forces Explicit Decisions

ISO 27001 requires organizations to formally document which of the 93 Annex A controls apply, and to justify every exclusion, in a Statement of Applicability[2,5]. SOC 2 does not have an equivalent artifact; organizations choose their own control language and typically do not have to justify what they left out. Building a defensible Statement of Applicability from an existing SOC 2 control set requires a genuine risk assessment exercise, not a copy-paste of existing policy documents.

Observation Windows And Audit Formats Differ

SOC 2 Type II evaluates operating effectiveness over a defined historical window. ISO 27001 certification evaluates whether the ISMS is currently operating and improving, verified through Stage 1 and Stage 2 audits and then confirmed annually through surveillance audits over a three-year certification cycle 2. Evidence formats, sampling approaches, and auditor expectations differ enough that a one-time crosswalk document becomes stale quickly unless it is maintained as a living reference.

Ownership And Tooling Gaps

Even organizations that understand the conceptual overlap often lack the operating model to exploit it. McKinsey's benchmarking data shows that GRC functions positioned with less senior sponsorship consistently score lower on maturity across risk and compliance dimensions alike, and that overall resourcing of GRC functions remains modest relative to the scope of work expected of them[6]. Tooling gaps compound this: programs that look sophisticated on paper frequently still run on a patchwork of spreadsheets and manual evidence requests, which cannot enforce the mapping discipline that crosswalk-driven compliance requires.

07 Practical Framework and Recommended Methodology

Organizations that successfully pursue dual compliance without doubling their workload tend to follow a consistent sequence. The steps below describe that sequence at a level any security or compliance leader can adapt to their environment.

Step 1: Align Scope Before Anything Else

Confirm that the systems, data flows, and business units in scope for SOC 2 match the intended ISO 27001 scope statement. Scope misalignment is one of the most common reasons a crosswalk breaks down later, because evidence collected for one boundary does not cleanly map to a different boundary.

Step 2: Build A Single Control Inventory

Consolidate existing SOC 2 controls into one inventory, independent of framework language, organized by function: governance, access, operations, change, incident response, vendor management, and business continuity.

Step 3: Apply The Crosswalk

Map each control in the inventory to its corresponding SOC 2 Common Criterion and ISO 27001 Annex A control, using the AICPA's published mapping as a starting reference and adjusting for how the control is actually implemented in the environment [1,4].

Step 4: Run A Targeted Gap Analysis

Identify which ISO 27001 requirements have no SOC 2 counterpart, focusing first on the ISMS management clauses, the Statement of Applicability, and any Annex A controls outside the organization's existing SOC 2 scope, such as physical security controls if the SOC 2 program was cloud-only[2].

Step 5: Tag Evidence For Reuse, Not Just For One Audit

As evidence is collected, tag it against every control it satisfies across both frameworks, and default to the stricter cadence or depth wherever the two frameworks diverge.

Step 6: Formalize The ISMS And Complete The Statement Of Applicability

Treat this as its own workstream with executive sponsorship, since it is the genuinely new work that a SOC 2-only program has not previously produced.

Step 7: Move To Continuous Monitoring

Replace point-in-time evidence gathering with continuous control monitoring so that evidence freshness, not audit-week scrambling, becomes the default state of the compliance program[10].

08 Measuring Effectiveness

A crosswalk program should be judged against measurable outcomes, not just the existence of a mapping document. The following indicators give security and compliance leaders a way to track whether the overlap is being captured, echoing the maturity dimensions McKinsey uses to benchmark GRC programs globally: technology enablement, resourcing, and the extent to which oversight is embedded rather than bolted on[6].

- **Evidence reuse rate:** the share of evidence artifacts satisfying more than one framework, tracked over successive audit cycles rather than measured once.
- **Time to second-framework readiness:** elapsed time from SOC 2 attestation to ISO 27001 audit-readiness, measured against a baseline of running the programs sequentially and independently.
- **Duplicate control count:** the number of controls still being separately documented, tested, and evidenced for each framework; the goal is to drive this toward zero over successive audit cycles.
- **GRC tooling maturity:** whether the organization's systems can automatically surface which evidence satisfies which framework, the specific gap McKinsey identifies as holding back 42% of surveyed organizations[6].
- **Audit finding recurrence:** whether the same observation appears in both the SOC 2 and ISO 27001 audit cycles, which signals the crosswalk is not translating fixes across frameworks.

None of these metrics require exotic tooling to track, but they do require a system of record that ties evidence to more than one framework at a time, which is precisely where spreadsheet-based tracking tends to fail at scale.

09 Real-World Scenario: A Composite Example

The following scenario is a composite, illustrative example built from patterns commonly described across the compliance industry rather than a specific named engagement. It is included to make the crosswalk methodology concrete.

Consider a mid-market SaaS company that completed its first SOC 2 Type II report roughly a year ago. Enterprise prospects in Europe now require ISO 27001 certification before signing. Facing this request, the compliance lead initially scopes ISO 27001 as an independent project: new policies, a new evidence repository, and a new external auditor relationship, run in parallel with the existing SOC 2 renewal cycle.

Early in scoping, the team builds a control inventory from its existing SOC 2 evidence and applies a crosswalk against ISO 27001:2022 Annex A. They find that access control, change management, vulnerability management, and incident response, control domains that consumed the majority of their original SOC 2 implementation effort, map closely to Annex A's technological and organizational themes and require only minor documentation adjustments rather than new technical work.

The genuine new work concentrates in three areas: building the ISMS management structure required by Clauses 4 through 10, producing a defensible Statement of Applicability that explicitly addresses all 93 Annex A controls, and extending physical security documentation that their cloud-only SOC 2 scope had not required. By identifying this early and resourcing it as its own workstream, rather than discovering it midway through a Stage 1 audit, the team avoids the most common source of ISO 27001 project delay: unbudgeted, late-discovered management-system work.

This pattern, most of the technical control overlap already present, most of the genuine new work concentrated in governance and documentation, is consistent with the structural comparison in Table 1 of this report, even though the specific proportions vary by organization, scope, and existing control maturity.

10 Ampcus Cyber Perspective

Ampcus Cyber works with organizations across the compliance lifecycle, from initial gap assessment through certification and ongoing assurance, including PCI DSS, SOC 2, ISO 27001, HITRUST, and related frameworks delivered through its Compliance Compass service line[11]. Our view, formed through this work, is that the SOC 2 to ISO 27001 question is rarely about whether the frameworks overlap; the AICPA's own published mapping between the Trust Services Criteria and ISO 27001 confirms that overlap exists at a structural level[1,4]. The real question is whether an organization's compliance program is structured to see and reuse that overlap, or whether it is structured around individual audits in a way that hides it.

This is the problem Ampcus Cyber's Synergized Compliance Model is built to address: a unified governance structure that harmonizes overlapping controls, policies, and processes across multiple frameworks into a single compliance ecosystem, rather than managing each framework as an isolated project[12]. Applied to SOC 2 and ISO 27001, this means one control inventory, one evidence repository, and one crosswalk maintained as a living reference rather than a static spreadsheet produced once and left to go stale.

GRACE, part of the Complyx platform, is designed to operationalize this model. GRACE unifies cross-framework control mapping, continuous monitoring, and built-in risk quantification through a single interface, so that evidence collected once can be evaluated against every framework it satisfies rather than re-collected for each audit[10]. Instead of compliance teams manually reconciling SOC 2 and ISO 27001 requirements in parallel spreadsheets, GRACE is built to keep the underlying control environment audit-ready continuously, which is the operating model this report describes as the modern approach.

Ampcus Cyber does not position ISO 27001 as an automatic outcome of SOC 2 compliance. Genuine, organization-specific gaps always exist, and no platform or crosswalk removes the need for a properly scoped risk assessment, a real ISMS, and rigorous internal audit. What Ampcus Cyber aims to change is the starting point: organizations should walk into ISO 27001 scoping already knowing what they have, not rediscovering it control by control during a Stage 1 audit.

11 Implementation Roadmap

The table below sequences the crosswalk methodology into phases with indicative focus areas. Actual timelines depend on organizational size, existing control maturity, and audit firm availability, and should not be read as guaranteed durations.

Phase	Primary Focus	Key Deliverables
Phase 1: Scoping & Inventory	Align SOC 2 and ISO 27001 scope; consolidate controls	Unified control inventory; scope statement
Phase 2: Crosswalk & Gap Analysis	Map controls across frameworks; identify net-new work	Control crosswalk; gap register
Phase 3: ISMS Build-Out	Governance clauses, risk treatment, Statement of Applicability	ISMS documentation; SoA; risk treatment plan
Phase 4: Evidence Reuse & Tagging	Tag existing and new evidence for multi-framework use	Tagged evidence repository; reuse metrics baseline
Phase 5: Internal Audit & Readiness Review	Test the ISMS and control evidence before external audit	Internal audit report; remediation log
Phase 6: Certification & Continuous Monitoring	Stage 1 / Stage 2 audits; move to continuous evidence collection	ISO 27001 certificate; continuous monitoring baseline

Table 2. A phased implementation sequence for organizations moving from SOC 2 attestation to dual SOC 2 and ISO 27001 compliance.

12 Strategic Recommendations

- Treat the crosswalk as a living operating artifact, not a one-time mapping exercise; revisit it at every audit cycle and whenever either standard is revised.
- Assign a single accountable owner for each shared control domain, rather than splitting ownership by framework, to prevent the same control from being documented twice under two different names.
- Budget the ISMS management clauses and the Statement of Applicability as genuinely new work; do not assume they will emerge from existing SOC 2 documentation[2].
- Default to the stricter of the two frameworks' requirements wherever they diverge on frequency or depth, so a single control operation satisfies both auditors.
- Tag evidence at the point of collection against every framework it could satisfy, rather than retroactively reconciling it before each audit.
- Move from point-in-time evidence gathering toward continuous control monitoring, since McKinsey's benchmarking shows GRC technology enablement is the area where organizations most often self-report needing improvement[6].
- Evaluate GRC tooling on its ability to demonstrate a live, control-level crosswalk across frameworks, not just its ability to store separate framework checklists.

13 Conclusion

SOC 2 and ISO 27001 answer different questions. One attests that specific controls operated effectively over a period of time; the other certifies that a management system exists to govern information security on an ongoing basis. But the controls underneath both frameworks draw from the same well of practice: access control, risk assessment, change management, incident response, and vendor oversight. That shared foundation is why the AICPA maintains a formal mapping between the Trust Services Criteria and ISO 27001 in the first place[1,4], and why global adoption of both frameworks continues to climb in parallel, with ISO 27001 certificates worldwide nearly doubling in the most recent reporting year alone[3].

Organizations that recognize this early, and structure their compliance program around a single control environment rather than a stack of independent framework projects, turn a second certification from a rebuild into a mapping exercise. Those that do not end up paying, in time, budget, and team morale, for the same security program twice. The GRACE Crosswalk Report is offered as a starting reference for security and compliance leaders making that decision, and as an invitation to treat framework overlap as an asset to be engineered, not a coincidence to be rediscovered at every audit.

14 Recommended Diagrams and Visuals

- A Venn diagram showing the structural overlap between SOC 2 Common Criteria and ISO 27001 Annex A controls, with labeled examples of shared and framework-specific controls, based on Table 1.
- A side-by-side structural diagram comparing SOC 2's five Trust Services Categories against ISO 27001's four Annex A themes and Clauses 4 to 10.
- A crosswalk matrix visual (expanded version of Table 1) mapping all nine SOC 2 Common Criteria to specific Annex A control families.
- A phased roadmap timeline graphic corresponding to Table 2, showing the six implementation phases and their primary deliverables.
- A line chart of ISO Survey certificate growth (2018 through 2024) to illustrate accelerating global ISO 27001 adoption.
- An infographic summarizing the key statistics highlighted in this report for use in social and email promotion.

15 Key Statistics to Highlight

- The number of valid ISO/IEC 27001 certificates worldwide rose from about 48,700 in the 2023 ISO Survey to more than 96,700 in the 2024 ISO Survey, covering nearly 180,000 sites[3].
- The AICPA publishes an official mapping between the SOC 2 Trust Services Criteria and ISO/IEC 27001, formally documenting the structural overlap between the two frameworks[1,4].
- McKinsey's 2025 Global GRC Benchmarking Survey found average risk-management maturity of 2.6 out of 4.0 and compliance maturity of 2.9 out of 4.0 across industries[6].
- 42% of organizations surveyed by McKinsey say their IT and GRC systems need improvement, and 15% describe them as absent or lagging[6].
- IBM's 2025 Cost of a Data Breach Report puts the global average breach cost at 4.44 million US dollars, and the United States average at 10.22 million dollars[7].
- ISO 27001:2022 consolidated 114 controls across 14 domains into 93 controls across 4 themes, with 11 entirely new controls[2,5].

16 Executive Takeaways

- SOC 2 and ISO 27001 are structurally different (attestation versus management-system certification) but share a substantial, formally documented control overlap.
- The largest genuine gap between the two frameworks is the ISO 27001 ISMS management system itself, which has no SOC 2 counterpart.
- Running SOC 2 and ISO 27001 as separate projects typically means re-documenting the same underlying controls twice, under two different labels.
- A documented, living crosswalk, not a one-time mapping spreadsheet, is what actually captures the overlap over successive audit cycles.
- Evidence tagged for reuse across frameworks, and a default to the stricter framework's requirement, are the two practices that most reduce duplicate work.
- The Statement of Applicability is a distinct ISO 27001 artifact with no SOC 2 equivalent and should be scoped as new work.
- Continuous control monitoring addresses the exact gap McKinsey's global GRC benchmarking identifies as most organizations' weakest point: IT and GRC systems that need improvement.
- Security leaders should evaluate GRC tooling on its ability to show a live, control-level crosswalk across frameworks, not just separate checklists per framework.

17 Ampcus Cyber: Next Steps

If your organization holds SOC 2 attestation and is evaluating ISO 27001, the highest-value first step is a structured crosswalk assessment, not a fresh ISO 27001 project plan. Ampcus Cyber's Compliance Compass team can help map your existing control environment against ISO 27001:2022 Annex A, identify genuine gaps in your ISMS and Statement of Applicability, and sequence the work so technical controls already in place are reused rather than rebuilt[11,12]. For organizations ready to move beyond spreadsheet-based tracking, GRACE provides the continuous, cross-framework control mapping and evidence management needed to sustain dual compliance long after the first certificate is issued[10].

Talk to Ampcus Cyber

Request a SOC 2 to ISO 27001 crosswalk assessment from Ampcus Cyber's Compliance Compass team.

See how GRACE unifies cross-framework mapping, continuous monitoring, and evidence management in one interface.

Visit www.ampcuscyber.com/complyx/grace to book a consultation.

18 References

01 AICPA & CIMA. "Mapping: 2017 Trust Services Criteria to ISO 27001." aicpa-cima.com/resources/download/mapping-2017-trust-services-criteria-to-iso-27001

02 ISO. "ISO/IEC 27001:2022 — Information security management systems." iso.org/standard/27001

03 ISO. "The ISO Survey." iso.org/the-iso-survey.html

04 NIST. "American Institute of Certified Public Accountants (AICPA) 2017 Trust Services Criteria Crosswalk." nist.gov/itl/applied-cybersecurity/privacy-engineering/american-institute-certified-public-accountants-aicpa

05 PECB. "Understanding ISO/IEC 27001:2022 Annex A Controls." pecb.com/en/article/understanding-isoiec-270012022-annex-a-controls

06 McKinsey & Company. "Governance, risk, and compliance: A new lens on best practices." mckinsey.com/capabilities/risk-and-resilience/our-insights/governance-risk-and-compliance-a-new-lens-on-best-practices

07 IBM. "2025 Cost of a Data Breach Report." ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai

08 ISACA. "SOC Reports for Cloud Security and Privacy." ISACA Journal, isaca.org/resources/isaca-journal/issues/2019/volume-6/soc-reports-for-cloud-security-and-privacy

09 Infosecurity Magazine. "Ensuring Backup Compliance with SOC 2 and ISO 27001." infosecurity-magazine.com/blogs/ensuring-backup-compliance-soc2

10 Ampcus Cyber. "GRACE – Compliance Automation & GRC Platform." ampcuscyber.com/complyx/grace

11 Ampcus Cyber. "Intelligent Cybersecurity Delivered" and "Compliance Compass." ampcuscyber.com

12 Ampcus Cyber. "Synergized Compliance Model." ampcuscyber.com/services/compliance-compass/synergized-compliance-model