How to build trust and confidence in technology through assurance reporting

13th annual EY System and Organization Controls (SOC) Reporting Conference Highlights

The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence

Five takeaways

from the 13th annual EY System and Organization Controls (SOC) Reporting Conference

1

Service organizations must adjust to the evolving landscape influenced by AI technologies to strengthen trust and protect data integrity.

2

Robust identity access management (IAM) practices are needed to increase system protection.

3

The American Institute of Certified Public Accountants (AICPA) continues to enhance SOC reporting.

4

Organizations must enhance their cybersecurity strategies to manage increasingly sophisticated risks.

5

ISO certification can complement your SOC strategy to build greater stakeholder confidence.

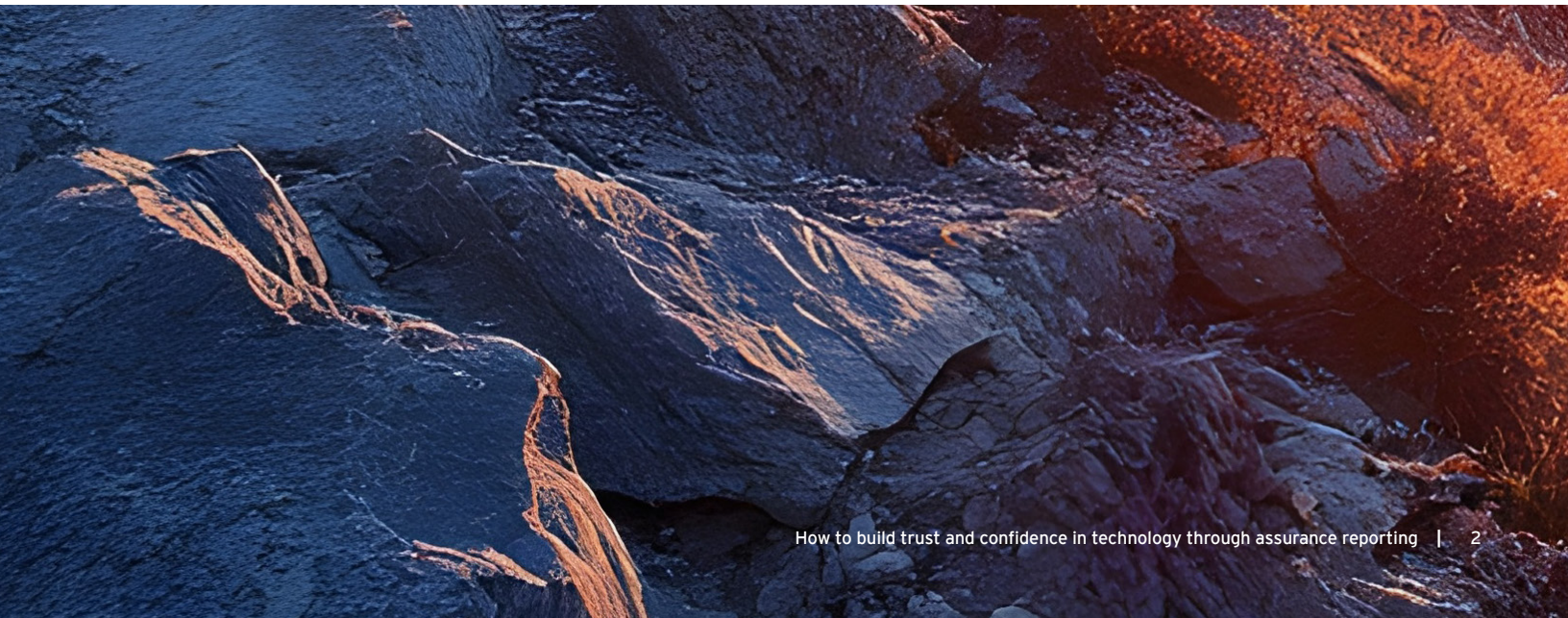
The integration of artificial intelligence (AI), generative AI (GenAI) and agentic AI is transforming how organizations operate, bringing about improved data quality, enhanced detection and more efficient processes. While advanced technology also introduces potential risks, assurance and attestation reports that demonstrate the use, reliability and security of these systems provide stakeholders with confidence in AI-driven processes.

Cybersecurity threats are evolving. Hackers are innovating their methods. Phishing and ransom attacks will continue. Customers' personal data and organizations' intellectual property and operational data are stored in cloud systems, with varying degrees of vulnerability. All this means it is more important than ever to couple attestation reports with robust governance and risk management frameworks to increase stakeholder confidence.

Insights from Trusting the Path Ahead, the 13th annual EY System and Organization Controls (SOC) Reporting Conference, centered on the critical role of transparency in customer relationships and business operations, while also exploring trends and developments in SOC reporting and attestation.

Optimistic about the future, Richard Jackson, EY Global Assurance Leader for AI, emphasized that trust and transparency are foundational to the assurance profession. Jackson represents the EY organization in discussions with external bodies to shape compliance and assurance for AI and the future of audit and attestation. He noted that as organizations adopt AI technologies into their ecosystems, the demand for assurance services will grow.

> "The speed with which that technology will be deployed is heavily predicated on the level of trust and confidence that people have in how it works, the importance and the integrity of what we do has never been more relevant.
>
> **Richard Jackson**
> **EY Global Assurance Leader for AI**
> **Ernst & Young LLP**



1 Service organizations must adjust to the evolving landscape influenced by AI technologies to strengthen trust and protect data integrity.

"Why all of us do what we do is really to help communicate trust and confidence, showing how you're addressing multiple risks through the various types of assurance reports you provide your customers.

Brandon Miller, Partner,
EY Global & Americas SOC/Attestation & Certification Leader
Ernst & Young LLP

As AI technology reshapes how organizations operate, organizations will need to continuously monitor their objectives and performance, and adapt their controls. Leading companies are engaging auditing firms to help them navigate the complexities and governance of AI.

To start, organizations must clearly define how AI is used within their processes and how it impacts their controls, which may be a part of SOC attestations or support financial reporting.

Data quality and a strong governance framework are essential. AI can enhance efficiency by capturing information once and using it multiple times, but that data must be reliable, free from bias and of high quality. Agentic AI systems bring new challenges and additional opportunities. Capable of making decisions and taking actions independently, these systems operate with a high degree of autonomy, reducing human involvement and oversight.

AI governance

Involving risk assessment, inventory management, risk mitigation and other key factors fundamental to SOC reporting

Define Definition of AI	**Map** Inventory of AI; identify system boundaries	**Assess** AI risk tiering; risk assessment	**Develop** Policies, procedures, standards and guidelines
Establish Roles, responsibilities and accountability structures; risk mitigation strategy	**Augment** Third party, cybersecurity and privacy risk management; subservice organization/vendor management	**Implement** AI lifecycle controls; risk mitigation strategy; suitably design control activities	**Monitor** Systems as conditions evolve

2 Strong identity access management (IAM) practices are needed to increase system protection.

Effective IAM through the lifecycle of a user profile helps the organization maintain security of systems and data and supports compliance with SOC reporting expectations. Having a clear understanding of data access is critical information to management and auditors. If something goes wrong, forensic investigators will need to know who had access, what systems were compromised, and the timeline.

However, organizations run into challenges because formal IAM practices are not always implemented effectively or efficiently, observed Scott Rau, Senior Manager, Technology Risk, Ernst & Young LLP. Commonly, we see instances where employees move into new roles, while retaining access and passwords from a previous job function. To prevent users from receiving excessive access to systems and data, some organizations implement a "back-to-birthright" approach. Email and basic access privileges remain, but the user must obtain new permissions for all business applications.

Management must "avoid rubber-stamping access to privileged accounts and role-based privileges," said Sarthak Jain, Senior Manager, Technology Consulting, Ernst & Young LLP. As-needed access can be granted in real time using vaulting tools. Additional approaches to strengthen security include reducing shared and service accounts and using multifactor authentication.

Eddie Foster, Technology Risk, EY US Central SOC Leader, urged organizations to keep open lines of communication between the identity management and human resources teams. IAM automation can assist organizations with timely de-provisioning, provisioning and access review.

An EY survey of over 2,000 SOC reports supporting customers' 2024 and 2025 financial audits found:

52%

of SOC 1 deviations and

40%

of SOC 2 deviations

were logical access related, indicating the need for a heightened focus in this domain

Challenges with identity access management

Access request and approval

- Decentralized administration – requires more oversight to ensure consistency
- New accounts mirror existing accounts – users receive excessive privileges
- Day 1/birthright access doesn't exist or inappropriate – provisioning requires more judgment
- Birthright access excessive or not monitored – users receive excessive/ unnecessary privileges

Enforcement

- Real-time privilege escalation does not exist – users retain more privileges than needed
- Privileged account monitoring doesn't occur – lack of accountability for privileged account usage
- Role-based access is not effective – roles retain excessive privileges or approvers don't understand users' access; too many roles to manage for people in organization

Transfer

- No systematic way to identify and manage transfers
  - Users retain more privileges than needed for new role, potentially impacting segregation of duties

User access reviews (UARs)

- UARs are highly manual – increased PM time to check for completeness/ accuracy and completion or incomplete/delayed reviews
- Multiple access lists needed to identify all users – non-human users (service accounts), privileged users or nested groups are excluded from UARs
- Approvers rubberstamp UARs – Users retain excessive access; Managers don't understand entitlements within roles
- Lookback considerations not defined/ performed – inappropriate access not reviewed for inappropriate activity

De-provisioning

- HR doesn't notify IT of separations – Delayed or no de-provisioning (network and application layer
  - Lifecycle management of non-human user accounts does not occur – Accounts retain access longer than needed
  - Inaccurate contractor management and end dates – Delayed or no de-provisioning; lack of ownership responsibility

3 The American Institute of Certified Public Accountants (AICPA) continues to enhance SOC reporting.

SOC reports instill trust between service organizations and users (i.e., customers) through transparent reporting and examination of business operations and controls. The AICPA produced its latest updates to the 2025 edition of the SOC 1 Guide and is regularly addressing SOC reporting guidelines while also convening other working groups to explore SOC 2 enhancement, cybersecurity, AI practices, sustainability and digital assets as stakeholder expectations continue to evolve.

> “As we think about SOC expectations, your customers and the customers’ auditors continue to ask better questions. Working closely with these stakeholders will be key as we move forward.
>
> **Daryl Box,**
> **EY Americas Technology Risk Leader**
> **Ernst & Young LLP**

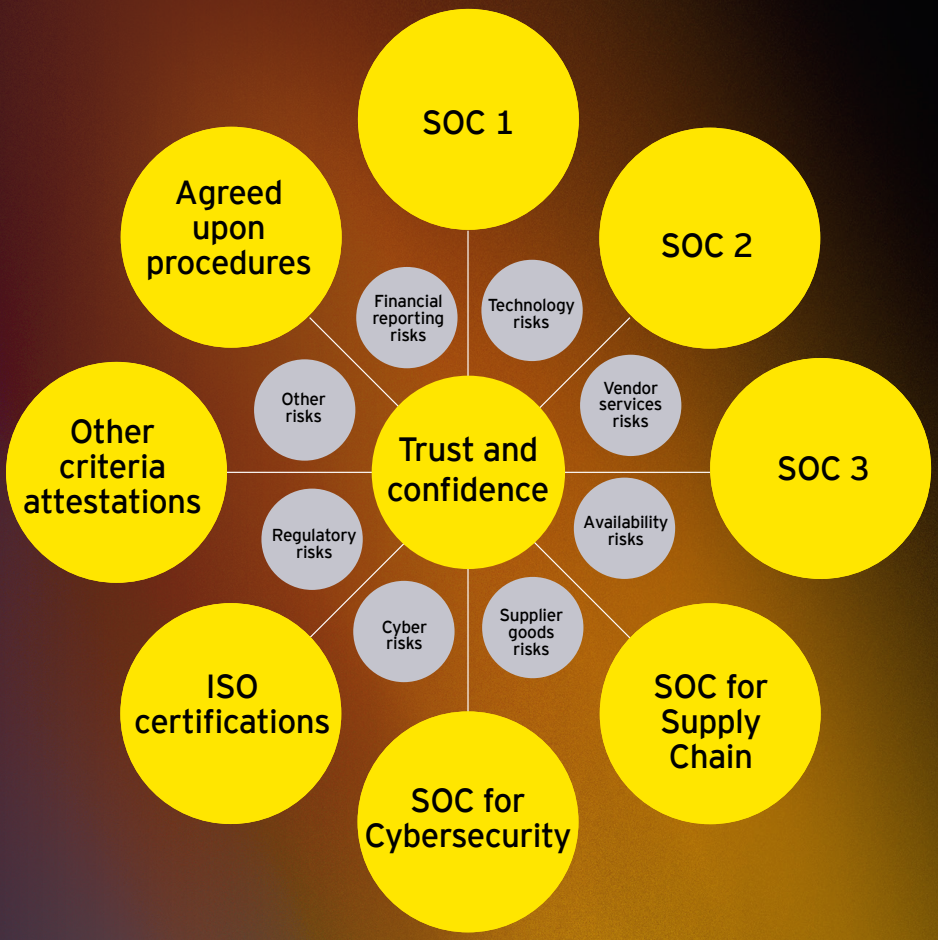
Among the biggest changes for SOC 1 reports within the new SOC 1 Guide has been the focus on whether a service provider meets the definition of a “subservice organization” and their effect on internal controls over financial reporting risks. Software as a Service (SaaS) applications/IT tools and cloud-related systems often warrant consideration as subservicers, rather than vendors in your report.

The AICPA’s focus for SOC 2 reports is to make them consistently of higher quality and more accessible to users, acknowledging that every organization won’t have the same controls. These reports offer customers insights on internal controls designed to meet service commitments and system requirements for security, availability, confidentiality, processing integrity and privacy based on the AICPA Trust Services Criteria (TSC). “Reports should clearly articulate your service offerings, processes and controls, giving the users the right amount of context,” Miller advised.

SOC 2 service commitments and system requirements can include compliance with laws and regulations. In some situations, a process or control framework may be committed to or required by a law or regulation. We are seeing SOC 2 reports used to help evidence compliance with some of the European Union (EU) and US state regulations.

Top organizations are proactive in addressing customers’ compliance questions through their SOC 2 reports and improving their control environments. “These subtle enhancements can really differentiate your reports vs. your peers’ and also build a lot of goodwill,” said Matt Beaulieu, Technology Risk EY US East SOC Leader. “Companies that improve their control environment, address inquiries effectively and respond proactively to concerns will stand out in the market.”

SOC, attestation and certification reports



SOC 1: Reports on internal controls over financial reporting of service organizations to help meet the needs of customers and their financial statement auditors.

SOC 2: Reports that provide current and prospective customers of service organizations information on internal controls implemented to help achieve certain service commitments and system requirements related to security, availability, confidentiality, processing integrity and privacy.

SOC 3: A complementary report to the SOC 2 without the details of the criteria, controls, tests and results of testing that can be more freely distributed.

Other criteria attestations: Using the AICPA's attestation standards, organizations can use available frameworks or define customized criteria that are objective, measurable and relevant and may be most helpful to their customers.

Agreed-upon procedures: Reports that define specific "agreed-upon" procedures allowing for a CPA firm to report results of just those specific procedures to satisfy requests of customers.

ISO certifications: Certification reports based on various standards from the International Organization for Standardization (ISO) that cover areas like quality, information security, privacy, business continuity, environmental areas and artificial intelligence.

A look at EU directives and regulations

GDPR

May 2018

General Data Protection Regulation (GDPR) sets a standard for organizations to follow to protect individuals personal data.

DMA

May 2023

Digital Markets Act (DMA) regulates large digital platforms.

CSRD/ESG

January 2024

Corporate Sustainability Reporting Directive (CSRD)/Environmental, Social, and Governance (ESG) expands sustainability reporting requirements.

DSA

February 2024

Digital Services Act (DSA) governs online intermediaries and platforms.

NIS 2

October 2024

Network and information Security 2 Directive (NIS 2) expands regulatory framework related to cybersecurity.

DORA

January 2025

Digital Operational Resilience Act (DORA) addresses the digital operational resilience needs of financial entities and establishes oversight of service providers.

AIA

February 2025

Artificial Intelligence Act (AIA) follows a risk-based approach (implemented in phases) to confirm that AI systems are safe, ethical and aligned with fundamental rights.

CRA

Effective December 2027

Cyber Resilience Act (CRA) imposes mandatory cybersecurity requirements.

4

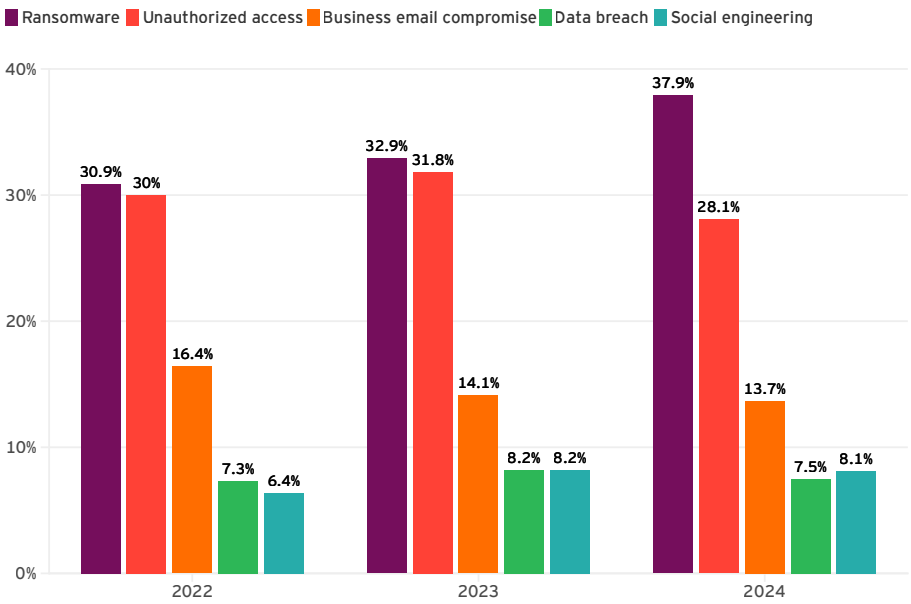
Organizations must enhance their cybersecurity strategies to manage increasingly sophisticated risks.

Cyber risks have implications for SOC reporting not only when something goes wrong, but even when organizations thwart a possible attack.

Sophisticated threat actors have innovated their methods with advanced tools, said Patrick Hynes, Principal, Cyber Threat Management, Ernst & Young LLP. The typical pattern is to find intellectual property and sensitive data and then hold it for extortion. Although all sectors have been pursued, health and life sciences organizations have recently been the most targeted sector. The sensitive nature of data often spurs a response, such as a ransom payout.

In the event of an attack or discovered attempt, organizations must determine the scope of the compromise, which systems were targeted or impacted, and which controls may have failed or need enhancement. The impact on SOC reporting also needs to be assessed.

Top 5 investigations by incident type
2022–2024



Source: EY Shadow investigations

That weakest link is often an employee

38%

of successful simulated attacks began through phishing

Source: EY Red Team analysis of Fortune 500 companies demonstrating the impact of real-world cyber attacks.

A shadow investigation looks back at any compromising factors, such as IP addresses, URLs and malware, the duration of the attacker's presence, and whether the incident reveals any deficiencies in the design or operation of SOC-related controls. It also aims to identify how the issue was found and the corrective actions taken.

Depending on the severity of the incident and what they learn about any design or operating effectiveness gaps, audit firms may need to modify the opinion of their SOC reports, restrict distribution or withdraw previously issued reports. Leaders should also know that any delays in informing customers about incidents can lead to frustration and erode trust.

It is important for auditors to generate awareness about the effects of cyber attacks on SOC reporting and attestation, and the need for audit and compliance teams to be included in cyber response planning and strategy, advised Mo Rusev, Executive Director, Technology Risk, Ernst & Young LLP. "It's so much easier to have that conversation when there is no pressure, rather than during an active event."

Even ransom payments require due diligence, because paying an individual in a sanctioned country can bring further trouble from the US government.

5 ISO certification can complement your SOC strategy to build greater stakeholder confidence.

The International Organization for Standardization (ISO) develops independent, international standards that outline management system frameworks in areas such as quality management, information security, business continuity, ESG, AI and health and safety. These aim for consistency and efficiency across industries, and certifications can bring credibility and predictability into the market. One of the most widely recognized ISO standards is ISO 27001, which focuses on information security management.

Depending on their requirements, customers may request an ISO, a SOC report, or both. The efforts involved in producing them can overlap. By leveraging the synergies between ISO certifications and SOC reporting, organizations can increase efficiency, reduce testing efforts, disruption and audit fatigue, and gain better visibility of risks and controls.

When seeking ISO certification, many organizations just focus on meeting compliance risks, but that mindset does not encapsulate all the benefits of ISO, said Jatin Sehgal, EY Global Leader, EY CertifyPoint B.V.

"That's the wrong approach," Sehgal said. "Do it because you want to reduce the number of incidents. You want to have more information about your controls. You want to [be able to] predict when you're going to have a system failure, or you want to be more efficient. You want to bring more discipline into your operation and have more structure. You want to bring clarity in the marketplace. You want to have better reporting. You want to have control over your supply chain. These are some of the reasons."

> "Do it because you want to reduce the number of incidents, you want to have more information about your controls. You want to predict when you're going to have a system failure, or you want to be more efficient.
>
> **Jatin Sehgal, EY Global Leader, EY CertifyPoint B.V. Ernst & Young LLP**

How to leverage an ISO management system effectively

Address the "why"	Scope, define objectives and target key performance indicators (KPIs)	Drive governance, risk management and compliance (GRC) initiatives through your management system maintenance	Change the technical mindset to a management system mindset

Take action

The 13th Annual EY SOC Reporting Conference highlighted the critical role of assurance and attestation in fostering trust and confidence among customers and stakeholders. SOC programs are increasingly addressing and prioritizing the risks related to AI and cybersecurity. The guidance for SOC 1 reporting continues to progress, necessitating the effective management of customer and auditor expectations. Proactively addressing changes in SOC 2 service commitments and system requirements effectively can lead to strategic advantages. The evolving customer expectations and regulatory environment present opportunities for synergy with SOC and ISO programs. By addressing these areas, organizations can maintain stakeholder confidence and effectively navigate the complexities of modern SOC reporting.

1

Adopt an AI governance framework that includes how AI is used, risk mitigation and regular monitoring, in support of SOC attestation and financial reporting processes.

2

Carefully control, track and monitor who has access to resources and systems to prevent unauthorized access.

3

Enhance training programs focused on cybersecurity, specifically targeting phishing awareness.

4

Develop and implement a clear communication strategy for promptly informing customers, auditors and regulators about incidents, minimizing delays to maintain trust and transparency.

5

Understand customer and regulatory expectations and leverage the synergies between SOC reporting, ISO certifications and additional standards and regulatory frameworks to build greater assurance.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 006227-25Gbl
2506-11965--CS
ED None

ey.com