The past, present and future of service organization control reporting

Key takeaways from EY’s Annual SOCR Client Conference

March 2016
“Study the past if you would define the future.”

— Confucius
Conference overview

On March 1-2, EY hosted the fourth annual Service Organization Control Reporting Client Conference. More than 100 executives representing approximately 40 service organizations met with EY to engage in spirited debate during sessions designed to delve into current market forces affecting service organizations and the impact that related changes have on customer information needs and SOC reporting. This summary highlights the key messages that emerged.

SOCR environment overview: past, present and future

Analyzing the past and present informs how to anticipate future changes in SOC reporting. Throughout the past 50+ years, technology advances and negative market events have been the two key drivers of changes in laws, regulations and professional standards that influence SOC reporting. Six interrelated market forces currently are driving changes in customer needs for risk-based information:

1. Technology advances
2. Increased dependency on service organizations
3. Heightened cybersecurity and other risks
4. Evolving laws and regulations
5. Increased focus on vendor risk management
6. New and modified professional standards

The takeaways

- Technology advances and negative market events drive changes in laws, regulations and professional standards that influence SOC reporting.
- Six market forces are driving significant changes in customer needs for risk-based information.
- The rapid pace of change increases risks, which makes being prepared for future changes more important than ever.

1. What new risks will you need to address?
2. Are you prepared for the next market event?
3. How can you build and maintain customer trust today?
Heightened cybersecurity risks

As the frequency and severity of cyberattacks continue to grow and evolve, various stakeholders (e.g., boards, investors and business partners) are interested in obtaining greater transparency into entities’ ability to effectively protect against and respond to attacks and breaches. Likewise, regulatory requirements and legislative interest relating to cyber risks continue to expand. The auditing profession is developing guidance to enable issuance of attestation reports on the effectiveness of cybersecurity risk management programs to assist organizations in addressing these evolving needs. The goal of these reports will be to improve management’s communication with its stakeholders and enhance stakeholder confidence in the integrity of the cybersecurity information provided. Entities may consider pre-assessments of their existing control environments, especially those cyber-specific focus areas that have not been subject to previous independent assessments. An independent assessment will help to enhance controls and prepare for future reporting.

The takeaways

- Due to the increasing dependency on and interconnectedness among entities and their customers, suppliers, service organizations and business partners, a cybersecurity issue at one entity can negatively affect other entities. This is driving market demand for more risk-based information on cybersecurity.

- To address the market demand for more risk-based information on cybersecurity, the American Institute of Certified Public Accountants (AICPA) is in the early stages of developing practitioner guidance for performing engagements and reporting on the effectiveness of cybersecurity risk management programs.

- Entities should consider their potential cybersecurity reporting needs and consider whether an independent cybersecurity assessment would help them enhance controls and prepare for potential future reporting.

Keep it simple: cybersecurity risks affect logical access and business recovery controls.

Historically, entities implemented controls and expected them to continue to address risks over time. With cybersecurity, the threat landscape is constantly changing, and controls need to constantly evolve to keep up. Increased interconnectivity among entities results in negative security events happening more quickly and causing a more widespread, severe impact. As a result, customers and other stakeholders are looking for more transparency and more confidence that a cybersecurity event at a customer, supplier, service organization or business partner does not become their problem.
The Public Company Accounting Oversight Board (PCAOB) has noted recurring findings in the area of internal controls and specifically failures to test controls over information produced by the entity (IPE). IPE refers to any information created by the entity using IT applications, end-user computing (EUC) tools (e.g., Microsoft Access, Excel), or other means, including manually prepared information. Auditors encounter IPE when it is used by management in the performance of controls that are subject to testing, when it is used as audit evidence for substantive tests, and when it is used as a population from which to select items to test. The concepts related to IPE apply to information produced by service organizations across three layers:

- IPE provided to customers of the service organization
- IPE used by management in the performance of controls performed by the service organization
- IPE used in performance of service auditor procedures

In the first two instances, there is a need to demonstrate that controls over the IPE support customers’ internal control over financial reporting opinions. In the case of IPE used in performance of service auditor procedures, the service auditor should perform direct procedures over the IPE if reliability is not already addressed by controls. Controls addressing the reliability of IPE include input, processing and output controls in addition to IT general controls. To address the PCAOB’s findings, customers of service organizations and their auditors continue to increase their focus on the identification and testing of controls over IPE included in SOC 1 reports and may expect enhancements to management’s description, controls, customer responsibilities or subservice organization responsibilities to gain reasonable assurance that IPE is complete, accurate and timely. Service organizations should continue to challenge the current state of their reports to identify potential gaps related to IPE.

**The takeaways**

- Regulatory changes or areas of emphasis can influence SOC reporting.
- Service organizations should continue to discuss report enhancement opportunities with their service auditor with a focus on IPE including (1) identifying IPE provided to customers and used in performance of controls, (2) identifying risks related to each layer of IPE, and (3) identifying, describing in the SOC report, and testing IPE and IPE-related controls.
- If not already occurring, service organizations should consider establishing a process to actively monitor PCAOB and other regulatory developments to anticipate future customer requests related to requirements that customers are passing through to their service organizations.
Evolving laws and regulation: privacy

Significant changes in regulatory requirements around the world are affecting entities’ obligations related to protecting privacy and personal information. Changes in privacy regulations can have an effect on the commitments that customers pass through to their service organizations, which in turn impacts the “system commitments and requirements” of the service organization that are presented in SOC 2 reports. Privacy changes are magnified in the cloud service model, which has unique SOC 2 considerations. The collection of personal information and the level of access to customer data in the cloud service model are important to defining scope, applicability and responsibility for SOC 2. Service organizations can enable timely updates to SOC 2 reports by tracking global regulatory changes and analyzing the impact of changes on their own privacy obligations and requirements, as well as those of their customers.

The takeaways

- Changes in global regulatory requirements will continue to affect service organizations’ privacy obligations and related SOC 2 reporting, both directly and via passed-through customer obligations. Recent notable regulatory changes include, but are not limited to, EU General Data Protection Regulation (GDPR), EU/US Privacy Shield, EU Model Clauses, and Russian Data Localization Law.

- In response to changing regulatory requirements, service organizations can consider updating executive management and/or the board of directors on relevant requirements, determining budget needs to address changes and performing readiness assessments.

- Entities with current SOC 2 reports covering the privacy principle can anticipate changes in customer reporting needs by evaluating the current system commitments and requirements for updates.

- Entities facing new or increased privacy obligations should consider how SOC 2 reporting can efficiently meet customers’ needs and build trust by providing a consistent vehicle to demonstrate compliance with new and changing regulations.
Regulatory pressure for entities to enhance their vendor risk management programs is increasing. In particular, entities are being challenged to understand the internal control environment and security posture of their service organizations, with greater focus on service organizations’ cybersecurity resiliency and business continuity controls. The Securities Industry and Financial Markets Association (SIFMA) is working with the AICPA, professional services firms and entities across financial services industries to address the difficult challenge of effectively and efficiently responding to requests for information resulting from vendor risk-management programs. As part of this effort, SIFMA is developing a financial services SOC 2+ report to help address the vendor risk-management challenge consistently and efficiently.

The takeaways

- Regulatory expectations continue to increase across financial services industries and are driving an increased demand for service organizations to share information with their customers to satisfy third-party risk-management needs.

- Service organizations should consider evaluating how the financial services SOC 2+ being developed by SIFMA and the AICPA can be used to address the third-party risk challenge and reduce the cost and burden of vendor due diligence and ongoing risk assessments.

Increased regulatory compliance is the new normal.
New and modified professional standards

The AICPA update to the attestation standards is nearing publication and will include several key clarifications and enhancements to existing requirements for SOC reporting. The updated standards are expected to be released in April 2016 and effective for reports dated on or after May 1, 2017. Clarifications address the continued evolution of management responsibilities related to development of the subject matter and corresponding changes to the management assertion. Enhancements include expanded requirements related to subservice organization controls and the service auditor’s procedures performed to evaluate the reliability of reports and data (i.e., IPE). The revised standards also introduce the concepts of misstatement and fraud within the context of SOC reporting, which will affect how service auditors and management think about the service organization’s system description and management assertion.

The takeaways

• The AICPA attestation standards are changing and expected to be released in April 2016 and effective for reports dated on or after May 1, 2017.

• Service organizations should understand the change in standards, perform a gap analysis compared with the current report(s), and develop an action plan with their service auditors to address the gaps.

Regulatory update: new requirements for Singapore banking service providers

One of the more recent financial services regulatory updates focusing on vendor risk management relates to the banking industry in Singapore and service providers related to this industry. Over the past 18 months, guidance released by the Monetary Authority of Singapore (MAS) effectively requires a SOC 1 by requiring material Outsourced Service Providers (OSPs) to commercial banks with operations in Singapore to engage an auditor to report annually on entity level controls, IT general controls and operational controls related to the outsourced services. The Association of Banks in Singapore, in response to the guidance released by the MAS, released a set of 105 specific controls that OSPs should include in the annual service organization control audits. The MAS dictates requirements that the service auditor needs to meet to be an acceptable issuer of the annual audit report. Entities providing services to commercial banks operating in Singapore should work with their service auditors to understand the new requirements, and service organizations who are covered under the new requirements should work with their Singapore-authorized service auditor to plan and execute their reports expeditiously to meet the mandatory deadlines of the end of 2016 for report issuance.
Focus on SOC 2+

Service organizations and their customers have grown increasingly interconnected amid expanding regulatory requirements and heightened cybersecurity risks, boosting the demand for information from service organizations related to internal control. As a result, customers of service organizations have grown more sophisticated in their compliance requirements for existing services and their expectations for new services. In addition to expanding customer compliance requirements, service organizations also face an increasingly complex regulatory environment. These growing compliance requirements have become costly. SOC 2+ reports offer a way to meet many of the compliance needs more efficiently because controls are tested once and the results of that testing are used to report on multiple compliance needs.

The takeaways

- Service organizations face the growing challenges of:
  - Controlling compliance costs
  - Building trust in new services
  - Managing compliance risk for customers
- The “test once, report many” approach of SOC 2+ reports allows service organizations to reduce the cost of compliance and the compliance burden on service delivery team members.
- A SOC 2+ report helps to build trust with existing and prospective customers by demonstrating that compliance with key risk and control frameworks has been engineered into the service offering.

Have you considered:

1. What services have the most requests for compliance reports, or where do you as the service organization have the most need to proactively show potential customers that compliance is in place?
2. What industry sectors and corresponding compliance frameworks are most relevant to your customers or potential customers?
3. What contractual requirements are in place with existing customers, or what terms are potential customers requesting?
4. What questions could a potential report address to eliminate on-site visits and questionnaires from customers?
Executives from three service organizations representing three different sectors, with responsibility to run and support their respective global SOC reporting programs, participated in an interactive panel discussion facilitated by EY on the past, present and future state of SOC reporting. The panelists engaged in a robust dialogue to consider and address the following key questions:

1. What are the biggest challenges and opportunities with your SOC 2/3 program?
2. How are you managing emerging risks and reporting options?
3. How have the drivers of your SOC 2/3 program changed?

The panelists discussed a variety of hot topics and considerations related to these questions, including how to engage and manage multiple internal and external stakeholder requirements, add key risks, understand and capitalize on opportunities with new reporting options, and appropriately leverage ongoing SOC program drivers. The discussion allowed conference attendees to share experiences and learn from one another in traversing the future of SOC reporting.

The takeaways

- Service organizations want to reassure customers that they are taking the appropriate steps with security. They also want to reduce audit fatigue on their technology and other teams.

- There is ever-increasing demand for service organizations to complete assessment questionnaires, accommodate site visits, and answer questions regarding internal controls. Service organizations are increasing the scope of SOC reports (i.e., SOC2+) and performing pre-assessments for previously unaudited products and services to anticipate client demand and reduce ad-hoc compliance requests from customers, internal audit and information risk management groups.

- A leading practice is to obtain customer buy-in on controls in advance. Transparency is needed when a customer moves from one product or service offering to another and the new product is not covered by a SOC report.

- Making the business case for a SOC 2 can be difficult if the cost and time that will be eliminated cannot be specifically identified, but successful implementers have seen that reliance on SOC 2 reports that are aligned to customer needs, combined with customer education, result in a decrease in on-site audits and completion of custom questionnaires.
Customer communications

Customer information needs arise from the risks of the services they have outsourced and from the unique business objectives of each customer. Communication needs also change throughout the customer relationship life cycle; pursue, on-board, maintain, expand services and terminate phases all drive distinct communication needs. The six market forces discussed in the SOCR environment overview: past, present and future section have significantly changed customer information requirements from needing information about financial controls to needing risk-based information across a spectrum of operational, compliance and financial risk areas. Entities that recognize these market forces and successfully transform their communication processes will develop a competitive advantage by building a deeper level of trust with their customers. To drive sustainable benefits at lower costs, entities should evaluate and transform their customer communications processes to operate effectively in today’s fast-paced, rapidly changing environment.

The takeaways

- Six market forces are significantly changing customer information needs.
- There is growing awareness by customers that they can outsource the work but not the risk.
- Service organizations must shift their mindset and communication processes to provide risk-based information as a vital part of the service.
- Entities that recognize the market forces and successfully transform their customer communications processes will develop a competitive advantage by building a deeper level of trust with customers.

Understanding how the market forces impact your customers is critical for building trust and anticipating risk-based information needs.
Technology advances enable outsourcing, and we are in a period of unprecedented technology advances that are disrupting business models and affecting entire entities. The role of IT has progressed from back office automation to the central nervous system of the entity. This has enabled entities’ outsourcing objectives to mature as well from enhancing capabilities/reducing costs to improving quality, strategic partnering and organization optimization. The velocity of change is accelerating, and while it enables new opportunities it also creates new risks that will drive new customer information needs. In the future, transparent, clear risk-based communications will be an important source of competitive advantage.

**The takeaways**

- Information will be an increasingly vital part of the product/service.
- SOC reports will be an important source of trusted, risk-based information.
- SOC reports will expand in size due to increased complexity of processes and supporting technology.
- SOC or similar types of attestation reports will likely evolve to include cybersecurity and/or data integrity.
- Customers will continue to need information beyond SOC reports to manage and oversee their risks.

“Yesterday is gone. Tomorrow has not yet come. We have only today. Let us begin.”

– Mother Teresa
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

Key contacts:

Chris Halterman
Global Service Organization Controls Reporting Leader
+1 515 362 7026
chris.halterman@ey.com

US regional Service Organization Controls Reporting leaders:

Central – Kevin Janes
+1 312 879 5400
kevin.janes@ey.com

Northeast – Brad Routhier
+1 617 585 3421
bradley.routhier@ey.com

Southeast – Courtney Adler
+1 404 817 4957
courtney.adler@ey.com

Southwest – Kris Lonborg
+1 214 969 8688
kris.lonborg@ey.com

West – Chris Tong
+1 408 918 5926
christopher.tong@ey.com

Financial Services – Keith Bispala
+1 612 371 8459
keith.bispala@ey.com