Service Organization Control Reporting

The impact of COVID-19

30 April 2020

As companies adapt to lockdowns and staff working from home, there has been no significant move from regulators to relax requirements around maintaining an effective control environment. This means service organizations should plan to continue to provide Service Organization Control (SOC) reports to their clients. These will come under greater scrutiny, since there is likely to be an expectation that service organizations will have to change control environments to reflect the challenges of COVID-19. User organizations and user auditors may also expect these changes and are more likely to want assurance on control environments from service organizations, which may increase demand for and/or interest in SOC reports.

Executive Summary

To continue to build trust with your clients in these unprecedented times you need to consider the following areas, in conjunction with your service auditor:

▸ Identifying how your service delivery processes and controls have changed

▸ Revising your project plan

▸ Planning for challenges during engagement wrap up

▸ Bridge letters

This applies both to reports that are wrapping up now, and as you start to plan reports which will be delivered later in the year. The sooner you do this, the quicker you can send a positive message to your clients, enhancing their trust in your ability to continue to support them. Our experience is that working successfully with clients through testing times builds ever stronger relationships. which should be your aim.

This paper considers the potential impact on SOC reports arising from COVID-19 restrictions; we will subsequently consider the potential impact on reports of the return to business as usual in a post-COVID-19 world.

EY

Building a better working world

Identifying how your service delivery processes and controls have changed

All SOC standards require that the service organization describes how services were delivered during the reporting period. User organizations will expect to see your SOC report describing how your business as usual (BAU) processes and controls have changed because of COVID-19. If no changes are needed, a statement from management explaining why this is should be included in the report. It is likely that a report that does not identify any changes will lack credibility with user organizations, who are likely seeing significant changes to their own processes and controls. In addition, user auditors are being challenged by regulators to be particularly skeptical during these times – so a report that is silent on the impact of COVID-19 is likely to attract more questions about this from user auditors.

Questions management might ask to assess whether their description needs to be updated include:

- Has there been a significant change in the demand for the entity's services?

- Has the demand for services shifted from one access point to another (e.g., reduced transactions captured at point-of-sale systems and an increase in on-line activity)?

- Has there been a significant change in the resources related to the services?

- Has there been an economic impact resulting in pressure to change controls?

- Implementing working from home policies or restricting access to your facilities

- Reassigning responsibilities between employees and locations

- Addressing the lack of availability of key employees due to illness

- Losing highly knowledgeable and experienced employees (lay-off, furlough, early retirement)

- Changing the performance of controls (e.g., using higher tolerances)

- Falling behind schedule in their own evaluation of the effectiveness of control

- Changing the evidence controls operated (e.g., manual controls may lack hard copies)

- Suspending controls (e.g., cancelling planned penetration testing or disaster recover testing).

- Implementing new controls

- Delaying the implementation of additional processing capacity

- Slowing the implementation of system changes.

- Evaluating changes at subservice organizations and vendors

Management should act now to:

- Document how service delivery changes could affect the risks around service delivery from a controls perspective e.g., if more users are given privileged access to increase resilience, what risk does this create.

- Consider how risks are managed by the controls, including any changes e.g., if privileged access is reviewed annually, does the increased number of people with that access require the review to be done more often, or an additional control added to look, perhaps on a sample basis, what each of the privileged users has done.

- Identify any additional evidence that needs to be retained including of the effective operation of these controls, to be audited by the service auditor at a later date.

This should satisfy the requirement from the standards for management to have done a risk assessment. Management should then document proof that the new controls are working. This can then be the basis for the management assertion that is included in the report.

Revising your project plan

You should work with your service auditor to develop a revised, realistic, project plan to allow you to proactively reassure your clients that:

▶ The scope of the assurance report will be unchanged

▶ When they can expect to receive the SOC report

▶ The report will cover any changes to service delivery that you have made due to COVID-19

You should work with your service auditor to look at how COVID-19 disruption might impact the current plan. Disruption examples include:

▶ The need to do additional work e.g. if there are pre, during, and post-COVID-19 controls, work may be needed on all of these, as opposed to just the one set of control testing that may have been done last year.

▶ If auditors cannot come onsite to do testing: can it be done using screensharing for sample items, do you/ your auditor have the tools to securely transfer other evidence between yourselves, can physical inspections be replaced with video streaming? These are all options, but our experience is that these can introduce delays if these are new.

▶ Resourcing; as staff are furloughed or are sick, when will the remaining staff have time to support the necessary audit testing?

▶ Access to key individuals for sign offs to both approve the project, and to sign off the final report. Can tools like DocuSign be used for online approval instead of hard copy signatures?

Planning for challenges during engagement wrap up

These are likely to revolve around potentially a greater number of deviations and/or access to senior management to discuss these with the service auditor, and to then sign off on the required deliverables as the report moves to being issued. The latter issue should be addressed through the updated project plan, clearly identifying the roles and responsibilities of individuals and required submission dates:

▶ Who will provide the management responses to agreed deviations in the report.

▶ Who will sign off on the report for the service organization.

▶ Who will sign the representation letter and the management assertion, including any changes needed to reflect qualified control objectives/criteria and return these to the service auditor.

The discussion and resolution of deviations is best handled through the service auditor flagging potential deviations as they arise through periodic status update meetings. There should be clear escalation paths within the service organization to agree the response including the management response to be included in the final report.

Bridge letters

Service organizations often produce reports that do not cover all of each client's financial reporting period. A bridge letter is then issued to provide assurance that processes and controls have not significantly changed since the end of the reporting period. If that bridge letter covers the period of COVID-19 disruption, and this environment is not covered by the report, it is unlikely that a bridge that says nothing has changed will be plausible. You should therefore consider:

▶ Describing in the bridge letter how this changed between the end of the reporting period and the date of the bridge letter.

▶ Using the new Agreed Upon Procedures (AUP) standards to ask your service auditor to extend their work and provide a report on how key controls, including new ones in the post-COVID-19 timeframe, have operated.

Summary

These are unprecedented and challenging times. We hope that this short summary has been useful in helping you think about continuing to build trust with your clients, and we stand ready to help you with these issues going forwards. If you have further questions, please do not hesitate to reach out to your local EY contacts.

Local EY contacts

EMEIA	India	UK & Ireland
Dennis Houtekamer	Badrinath P. Midthe	Mark Russell
dennis.houtekamer@nl.ey.com	mp.badrinath@in.ey.com	mrussell@uk.ey.com

Germany, Switzerland and Austria	Financial Services	Central, Eastern and Southeastern Europe and Central Asia
Mathias Feil	Michael Elysee	Milada Zavodova
mathias.feil@de.ey.com	michael.elysee@uk.ey.com	milada.zavodova@cz.ey.com

Western Europe Maghreb	Nordics	Middle East and North Africa
Karen Moutardier	Rune Vanvik	Sudharsan Srinivasan
karen.moutardier@fr.ey.com	rune.vanvik@no.ey.com	sudharsan.srinivasan@ae.ey.com

EY | Assurance | Tax | Transactions | Advisory

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

This news release has been issued by EYGM Limited, a member of the global EY organization that also does not provide any services to clients.

Ernst & Young LLP

ey.com/uk