



Reacting to Covid-19 in internal control over financial reporting

19 March 2020

Helping organisations anticipate internal control over financial reporting challenges

As organisations around the world rapidly enact their crisis recovery plans and focus on ensuring the safety of their people and their assets, business as usual activities risk being interrupted or cancelled.

Financial reporting processes are no exception, however at a time of such exceptional uncertainty there continues to be a need to give investors, regulators and other stakeholders relevant and timely information about operational and financial performance.

While regulators such as the Securities Exchange Commission (“SEC”) and the UK Financial Reporting Council (“FRC”) have been issuing guidance to companies and auditors, at the moment there are currently few relaxations of existing requirements. At this point in time it is difficult to predict if any further financial reporting requirements may be eased if the impact of Covid-19 runs on for many months, and what dispensations may be given in such a future scenario.

The situation is likely to evolve rapidly and so further clarity may be provided in due course. However with a number of organisations having March and April year ends, or interim financial reporting requirements in this period, we have sought to identify some initial areas around internal control over financial reporting that, at this time, are potentially at risk from Covid-19, especially for organisations with SEC reporting obligations and the need to ensure continued compliance with Sarbanes-Oxley.

At this stage, our overall immediate recommendations, focused on maintaining the existing control environment as best as possible, include:

1. **Reassess the financial reporting timetable** and relax timing constraints, where possible, on the operation of key controls. This will likely need to be risk assessed to ensure that all key controls operate prior to financial reporting announcements but potentially some controls may need to operate simultaneously rather than in the traditional step-by-step hierarchy of the financial reporting process.
2. **Formally document where certain decisions have been made** to provide temporary relief, for example changes in timetable or new responsibilities being granted, so that it can be evidenced to external auditors at a later date (via email or other means).
3. Keep in mind that **fraud risks may change** in such a time of crisis, as new opportunities are enabled for both internal and external parties. Incentives for committing fraud, both misappropriation of assets and financial reporting fraud may also be heightened, especially if significant redundancies are likely to be required or employees suffer significant personal financial stress. Misappropriation of physical assets may however, for some organisations, become less likely with more remote working.
4. Ensure early and on-going **discussion with external auditors** to avoid surprises later in the year. Audit approaches are likely going to need to evolve as well.

“Actual effects will depend on many factors beyond the control and knowledge of issuers. However, how issuers plan for that uncertainty and how they choose to respond to events as they unfold can nevertheless be material to an investment decision.”

Jay Clayton
SEC Chairman

The extent to which an organisation will ultimately be impacted is difficult to predict at this relatively early stage of the Covid-19 outbreak. We anticipate that organisations with increased automation and who have significant amounts of technology in their control environment will have different challenges to address to those with a more manual control environment. However neither approach is free from potential pitfalls that may occur in the coming weeks and months.

Changes to the control environment are likely to be needed and, based on the current situation, impacts may be felt around the following key areas:

1. **Scoping and risk assessment conclusions** may need to be revisited to ensure they appropriately respond to the changes in the organisation that have occurred since the Covid-19 outbreak.
2. The **design or implementation of controls** may need to be adjusted to compensate for changes in risk, or contingency plans may need to be put in place for outsourced service providers.
3. Testing activities, both by internal and external parties, may need to **plan for increased levels of remote testing** and greater co-operation between the various testers. There will likely also be increased focus on the quality of documented evidence to support controls operating, in particular management review controls where judgement is used by testers to evaluate the sufficiency of evidence.
4. If an **increased level of deficiencies** results from Covid-19 impacts, plans will need to be put in place to ensure a timely and effective response. This will require careful project management and put increased pressure on those individuals with the best knowledge of internal controls.
5. Typical **communication plans with senior management and board members** may need to be revisited to ensure they are given the information they need to fulfil their responsibilities, on a timely basis.

In order to respond to all of the above, it may be that existing control transformation plans have to be put on hold and extensive prioritisation needed. Project management will be key, especially if there are other significant business needs which have to take priority for some of the critical resources or management focus. Any existing remediation projects will likely have to be reassessed and expectations discussed early with external auditors.

We outline below some potential pitfalls and possible mitigations that organisations may want to consider, focused around these different areas. This is not intended to be a comprehensive list and will vary depending on the facts and circumstances of each organisation. Performing a tailored assessment, going through each of the principles and points of focus in the COSO 2013 framework, will likely need to be performed as a completeness check.

Our separate analyses covering cybersecurity and general accounting and financial reporting requirements are also available. These may be updated frequently so please check the webpages listed below to ensure you get the latest updates.

- Covid-19 homepage at www.deloitte.com/covid-19
- Cyber homepage at www.deloitte.com/cyber
- IFRS in Focus newsletters available from www.iasplus.com
- Heads Up newsletters available from www.deloitte.com/us/audit
- Financial Reporting Alerts on SEC reporting topics through www.dart.deloitte.com (subscribers only)

Contact details of our global Covid-19 team are given on our Covid-19 homepage, see link above. You can also speak with your regular Deloitte contact. Details of how to get in touch with the authors of this document are given at the end and we welcome any questions or feedback you may have. We hope you find it helpful in supporting your contingency planning activities.

Business control implications

Area	Potential pitfalls	Possible mitigations
Management review controls	<p>Breakdown in review-type controls or the inability of individuals to perform control duties (e.g. due to employee illness or the closure of affected offices)</p> <p>Lack of reliable information may affect management's ability to effectively operate controls (e.g., personnel may not be available in offices in affected areas to provide information that is essential to the effective operation of an internal control)</p>	<p>Ensure controls processes and narratives are up to date in the event control owners need to change</p> <p>Ensure any new or temporary control owners have the appropriate authority and competency to perform the control activities</p> <p>Identify other controls that can provide the same assurance but using different information sources</p> <p>Plan to implement new controls that provide additional assurance over the reliability of information (e.g. manual checking back to source documents, such as invoices)</p>
Accounting judgement controls (e.g. bad debt provision, inventory provision, other provisions, impairment of goodwill and other intangible assets, fair value of financial and non-financial assets)	<p>Failure to consider the impact of new uncertainties and market volatility on accounting judgements</p>	<p>Perform a top-down assessment of key accounting judgements to identify where existing controls may need to specifically consider Covid-19 impacts and communicate the results of this to control owners</p> <p>Ensure the financial statements appropriately disclose the sensitivity of those key assumptions</p> <p>Enhance existing controls to ensure appropriate, and documented, consideration of Covid-19</p>
Associate or joint venture accounting controls	<p>Lack of access to timely or reliable financial information from an associate or joint venture</p>	<p>Ensure regular communication with the associate or joint venture to monitor likelihood of knock-on impacts in upcoming financial reporting periods</p> <p>Re-consider the materiality of each associate or joint venture to the consolidated financial statements, to evaluate which need to be in-scope of key controls</p>
Transaction processing controls	<p>Transactions may not be processed on a timely basis due to Covid-19 and as a result backlogs in transaction processing may form (on-shore or off-shore)</p>	<p>Have enhanced monitoring processes and controls to monitor the effectiveness of daily/weekly transaction processing controls</p>
Cash payments controls	<p>Payments may require a dedicated terminal or hardware for the validation of payments</p> <p>Lack of availability to reach individuals to verify transactions / approvals</p> <p>Backup contact details with the bank to verify potentially fraudulent payments are not updated</p> <p>Insufficient dual payment signatories are available to approve payments</p> <p>Changes in reporting / approval lines may not have been communicated to, or acted on, by the bank</p>	<p>Test all processes involving online banking access to determine if they can be operated remotely</p> <p>Review payment approvers listing and risk assess whether expanding it is appropriate (being careful of segregation of duties)</p> <p>Ask bank for additional hardware devices and/or to relax hardware payment controls</p> <p>Speak with bank to discuss emergency contact details and failsafe processes</p>

Business control implications (continued)

Area	Potential pitfalls	Possible mitigations
Automated business controls	<p>If manually triggered and/or monitored they may fail to operate due to personnel being unavailable</p> <p>Failures for other reasons may not be detected on a timely basis if monitoring controls are not operating</p>	<p>Identify which automated business controls are most susceptible to failure, due to Covid-19, or based on historical trends</p> <p>Ensure appropriate compensating controls exist and are operating effectively to mitigate any risks arising from a failure to operate the automated business controls</p>
Outsource service providers	<p>External organisations essential to the control environment may face their own challenges, which could impact on their ability to reliably execute their processes and controls upon which reliance is placed</p>	<p>Speak with outsource service providers on a regular basis to check how they are coping</p> <p>Assess the likelihood of receiving at a future point in time a service organisation report (i.e. SOG-1) that is qualified</p> <p>Assess compensating controls for the outsource service providers deemed to be at most risk and implement new or updated controls if required</p> <p>Ensure contingency planning is in place in case an alternative service provider needed to be used</p>
Insider trader concerns	<p>Employees may have access to non-public information and trading restrictions may need to be imposed, as the potential effects of Covid-19 could constitute material non-public information</p> <p>This risk may be elevated if the financial reporting timetable is extended</p>	<p>Companies should consider how their codes of ethics and insider trading policies address, prevent, and deter trading that is based on material non-public information, including information related to Covid-19</p> <p>Communications to employees may be needed to remind them of their obligations</p>
Programme change	<p>Likely to be similar to the potential pitfalls outlined below under IT control implications</p>	<p>Likely to be similar to the possible mitigations outlined below under IT control implications</p>

IT control implications

Area	Potential pitfalls	Possible mitigations
Key person dependency/ Super User access	<p>Organisations may have contingency or succession plans for senior executives, however, this may not adequately cover IT personnel</p> <p>With increased dependency on IT personnel and infrastructure to support the organisation working remotely, the availability or ability of IT personnel for internal control related matters could be limited</p> <p>Key IT staff with administrative privileges may be unable to perform their duties (for example due to illness) and this may impact on the ability of the organisation to address IT failures, or operate key IT controls</p>	<p>Assess the exposure of current IT capabilities, including outsourced activities, to determine where risk lies</p> <p>Consider cross training of IT staff to support multiple IT activities, subject to segregation of duties considerations</p> <p>Consider using password vaults or other methods to ensure administrative accounts can be used in a secure manner if a key individual is not available</p> <p>Perform a pre-emptive review of IT controls to identify which users and super-users are most critical</p> <p>Consider designing contingency plans for IT personnel, so that key controls can continue to be operated (segregation of duties should be considered as part of this scenario planning)</p>
Outsource service providers	<p>Likely to be similar to the potential pitfalls outlined above under business control implications</p>	<p>Likely to be similar to the possible mitigations outlined above under business control implications</p>
Change management	<p>Individuals try to shortcut the change management process because they believe Covid-19 will result in delays</p> <p>Business personnel are unavailable to approve changes</p> <p>Responsibilities change due to personnel being unavailable and this may result in developers having access to promote changes to a live environment</p> <p>With Covid-19 taking a significant amount of the organisation's focus, inadequate testing of changes may be done before they are allowed to go-live</p> <p>Critical changes may need to be made but the relevant process could be dependent on personnel that may not be available or temporary personnel who are not adequately trained, leading to an error</p>	<p>Communicate with the business in order to reduce the volume of changes requested, to critical items only</p> <p>Ensure monitoring controls over change management continue to operate effectively during the period, to detect any deviations from required testing and approval processes</p> <p>Ensure changes to developer access rights continue to be reviewed and perform mitigating procedures on a timely basis if issues are identified</p> <p>Carefully review existing processes for addressing critical changes to ensure they remain pertinent and ensure only appropriate personnel are given these responsibilities</p> <p>Independently challenge requests marked by the business as being critical to ascertain if this really is the case, or if normal change processes should be followed</p>

IT control implications (continued)

Area	Potential pitfalls	Possible mitigations
Programme change	<p>A project may be delayed due to Covid-19 but there may be a significant need for this to be completed on schedule from an internal control over financial reporting perspective (e.g. remediation of a significant deficiency or material weakness).</p> <p>Key resources may be redeployed resulting in the project being inadequately staffed or having inadequate expertise to execute successfully</p> <p>A dependency on third party vendors or external service partners for the successful delivery of the project may exist, and these third parties could be unable to fulfil their requirements due to Covid-19</p>	<p>Critically consider which projects need to continue and which can be put on hold for the short-term</p> <p>Perform an up-front reassessment of timetables for key projects, to identify revised completion dates and to commence planning for any adverse consequences due to anticipated late delivery</p> <p>Assess resource redeployments from key projects to determine the impact on the project timetable or to determine if additional activities, such as quality assurance, need to be performed in order to ensure the project is completed successfully</p> <p>Ensure contingency planning is in place in case an alternative service provider needs to be used</p>
Interface and batch processing controls	<p>Monitoring of automated interfaces by relevant IT personnel may not occur on a timely basis or may fail to be performed</p> <p>Manual interfaces may not be operated if IT personnel cannot access the system remotely or are unavailable to do so</p>	<p>Ensure there is clear understanding of which interfaces are most critical and identify which have any form of manual dependency to operate</p> <p>Consider designing contingency plans for IT personnel, so that key controls can continue to be operated (segregation of duties should be considered as part of this scenario planning)</p> <p>Identify whether monitoring activities can be spread across a wider population of IT personnel to mitigate risk on a single user or team</p>
Resilience and remote working	<p>Lack of proper infrastructure to support remote working could impact the ability of people to logon to applications and services</p> <p>Remote working facilities may be overwhelmed or operate intermittently</p> <p>Employees may seek to workaround existing security protocols and controls in order to keep the business operating efficiently, which could impact the confidentiality of information and result in the leakage of secure data</p>	<p>Prepare plans for the operation of essential IT controls outside of peak working hours (such as through the use of offshore locations)</p> <p>Ensure appropriate security technologies, such as VPNs, support all critical applications and services, including, at a minimum, those in scope for SOX</p> <p>Communicate with employee to remind them of the existence of training materials, where they can go for support and not to circumvent security protocols</p>

Internal control framework and governance

Area	Potential pitfalls	Possible mitigations
Scoping	<p>Anticipated business performance used to scope the business may end up being significantly different from actual business performance and this may bring different areas into scope at the last minute</p>	<p>Perform up-front scenario analysis on the SOX scoping to identify the likelihood of out of scope components being brought into scope</p> <p>Prepare a short-list of areas that are most at risk and hold contingency planning meetings with those areas to determine their SOX-readiness capability</p>
Risk assessment	<p>Organisations may fail to reassess the risks present in their financial reporting processes and rely on risk assessments performed prior to the Covid-19 outbreak.</p> <p>These may therefore fail to take into account:</p> <ul style="list-style-type: none"> • material changes to the financial results of the business • one or more new risks that are qualitatively significant (e.g. risk of a material volume of credit notes being issued) • pre-existing risks that may be heightened as a result of Covid-19 impacts (e.g. inventory obsolescence, credit risk of customers) 	<p>Perform a top-down risk assessment to identify what may change, or have already changed</p> <p>Seek bottom-up feedback from the business to challenge this re-assessment of risk</p> <p>Document this revised risk assessment and the conclusions reached, based on risk appetite, as to where changes in processes and controls will be needed</p> <p>Communicate the results of this to process and control owners</p> <p>Consider any resulting impact on entity level controls</p>
Monitoring	<p>Existing monitoring activities may fail to cover any newly implemented controls</p>	<p>Ensure consideration is given to monitoring activities as part of the design of any new control activities</p>
Deficiency evaluation and concluding activities	<p>Insufficient personnel, with adequate knowledge and experience, available to evaluate an increased number of deficiencies</p> <p>Deficiencies reported later in the year due to challenges with performing audit activities, resulting in less time for management to mitigate or remediate the issues found</p>	<p>Review the depth and capability of individuals with internal control responsibilities</p> <p>Establish a “quick response” group that is tasked with evaluating deficiencies and making decisions on the best way forwards</p> <p>Consider bringing in short-term project management expertise from elsewhere in the organisation to establish good project management practises and to allow those individuals with internal control experience to focus on identifying and implementing solutions</p>
Communications	<p>Failing to prepare for increased frequency and depth of communications to senior management and board members</p>	<p>Establish accountable owners to summarise overall status and key issues being dealt with, typically one individual for business controls and another individual for IT controls</p>

Testing activities

Area	Potential pitfalls	Possible mitigations
<p>Key person dependency</p>	<p>Organisations may have contingency or succession plans for senior executives, however, this may not adequately cover internal testing personnel</p> <p>Testing personnel from external organisations, both to support internal testing or as part of the external audit, may not be available during the planned testing period</p> <p>Process or control owners in the organisation may not be available during the planned testing period</p>	<p>Perform an up-front review of testing plans and identify ways in which increased flexibility in testing schedules can be obtained</p> <p>Seek alternative sources for testing individuals; this may require delaying assurance activities which are deemed to be less critical</p> <p>Seek ways to align the different testing groups such that the testing impact on the business personnel is minimised</p>
<p>Testing logistics</p>	<p>Protection measures put in place may mean that typical testing approaches are not feasible and remote testing may need to be performed in the majority of cases</p> <p>This is likely to prove most challenging in areas such as:</p> <ul style="list-style-type: none"> • Performing walkthroughs of the end to end process • Performing operating effectiveness testing for management review controls or controls where evidence that has historically been centralised is now decentralised 	<p>Ensure regular communication between all testing parties (testers and those being tested)</p> <p>Agree which technologies will be used to support the testing, in particular communication tools and file sharing platforms, and ensure all testing and business personnel can access these</p> <p>Communicate with control owners to emphasise the importance of retaining high-quality documented evidence to support testing programmes</p> <p>Prepare a contingency plan in case increased levels of remediation testing are required</p>

Authors



Rob Hughes
Partner, Risk Advisory -
US Capital Markets
rohughes@deloitte.co.uk



Charlie Gribben
Partner, Risk Advisory –
Digital Risk
cgribben@deloitte.co.uk



Chris Overd
Director, Risk Advisory –
US Capital Markets
coverd@deloitte.co.uk



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2020 Deloitte LLP. All rights reserved.

Designed and produced by Deloitte Creative CoRe. RITM0428432