OCAG insights: The impact of Covid-19 on your control environment

September 2020

This guidance note has been developed for audit committees and management to assist them when considering the impact of the public health emergency on the entity's control environment as part of their work under the applicable corporate governance requirements.

AI 1

OCAG insights: The impact of Covid-19 on your control environment AI1

September 2020

The onset of the COVID 19 pandemic from early 2020 has significantly impacted on the operation of public business and on the public finances. Public health advice and safety measures have resulted in fundamental and rapid changes to the working and control environment with remote and virtual working becoming the norm for most entities. New activities, reprioritisation of work and pressure to deliver services have also impacted on most entities' operations and staff. This new environment gives rise to a number of challenges for entities in maintaining effective internal controls.

Applicable corporate governance requirements set out the responsibilities for boards, audit committees and management in relation to the system of internal control and for public reporting on controls. The external auditor reviews the entity's statement on internal control in the context of the annual financial audit. Therefore, the external auditor will be interested in understanding how management and audit committees have responded to the challenges and risks faced by the entity in the new environment.

This guidance provides useful information for management and audit committees in considering the impact of the health emergency on the entity's control environment and some issues they may find useful when engaging with the external auditor during the annual audit process.

Audit insights

This guidance is part of a programme of work to identify and share learning opportunities for bodies by providing information on common recurring issues and good practice examples, identified through our financial audit and reporting work.

Risks stemming from changes in systems of control

The *Code of Practice for the Governance of State Bodies*[1] (the Code) published by the Department of Public Expenditure and Reform sets out the elements which underpin an effective system of internal control namely

- an appropriate control environment
- the process to identify business risks and evaluate their financial implications
- the major information and communication systems
- control activities and procedures which address the major risks
- monitoring and oversight procedures for ensuring the effectiveness of controls.

Under the Code, boards are required to review the effectiveness of the system of internal control annually and report on the system in a statement on internal control which accompanies the financial statements. Management and audit committees[2] support the board when it discharges this responsibility.

In the new environment, it is likely that there have been changes to various components of the system of internal control, and it is important for management and audit committees to understand the impact of those changes when assessing the effectiveness of controls.

The control environment

The control environment will likely be different in that nearly all entities have changed the way they operate thereby impacting on their oversight processes and control procedures. These changes may lead to additional risks such as risks of financial errors or fraud. How management have maintained an appropriate tone-at-the-top message is also important as any weaknesses in the control environment (e.g. management override) may have more significant consequences where staff operate in a remote or distributed working environment.

The types of questions which might be raised by audit committees with management include

- What were the key messages from management to staff about financial controls and maintaining compliance with public sector practices?
- What supports were put in place to assist with remote and virtual working (e.g. financial procedures' manual updates, bulletins, specific training)?
- How has management measured and maintained employee engagement (e.g. regular staff surveys, leadership recognition of the difficult working environment, and communications and tips on maintaining discipline and motivation)?

[1] Similar requirements or governance codes may apply in different segments of the public sector such as government departments and third level bodies.

[2] In many entities, the audit committee's role may encompass risk management and be described as the Audit and Risk Committee.

- How well did staff adjust to the new working environment (e.g. ability to cope with technological changes)?
- How has management satisfied itself that the new working environment is effective in preventing and detecting control breakdowns or errors?

Entity risk management

Risk management is a key tool for entities in identifying and addressing significant risks to achieving successful outcomes. It is important that boards and audit committees pay particular attention to risk management in the new environment. Consideration of changes to risks and risk appetite is likely to be more frequent in the new environment as the public health advice and business environment continue to evolve.

There are a wide variety of risk factors and questions that may emerge when considering risk management. Some examples of factors and questions arising from the new environment are set out below.

Significant changes to the business or introduction of new services or schemes

- Has an overall risk assessment been made of the risks facing the entity (including the impact on business-as-usual operations and any new business areas for example new grant schemes)?
- Has an assessment been made of the risks to the adequacy of systems, procedures and capacity (including ICT) to respond to changes in business, new demands or business-as-usual operations?
- Has an assessment been made of whether any new schemes or services are within scope of the entity's legislation and its funding delegation (regularity)?
- Where the entity relies on service providers for key elements of its business, have risks around continuity of supply or changes in their controls been considered?

Significant pressure on management

- Are there any instances of key controls being overridden in order to maintain business-as-usual?
- Are there areas where management may be less vigilant in their oversight and monitoring of the day-to-day business routines due to pressures?

Increased risks of fraud for example due to changes in the control procedures, practices or staff awareness

- Has an assessment been made of the opportunity for increased risk of internal and external fraud (including grant expenditure)?
- Has management reviewed the circumstances of any actual or suspected frauds which have occurred to consider the implications on the system as a whole?

Non-compliance with laws and other requirements for example due to pressure on the entity to deliver or from changes in practices

- Have risks of non-compliance with legal and other public service requirements been assessed?
- Have there been any pressures which could negatively impact on procurement compliance?

Increased legal exposure

- Has there been an assessment of the potential for an increase in litigation or claims?
- Have new services been assessed for potential legal risks such as the creation of unintended obligations or commitments?

Risks to financing and financial reporting

- Has there been an assessment of the impact on forecasts, budgets and cash flow for an appropriate period of time?
- Has an assessment of going concern been made in accordance with the applicable requirements[3]?
- Has sufficient attention been paid to management of costs and value for money in light of changes to services or operations?
- Has the potential for onerous contracts been assessed?
- Are there aspects of financial reporting that may pose a higher risk such as items involving estimation and judgment which could be subject to greater degrees of uncertainty (e.g. discount rates, market values, recoverability of debts)?
- Are there any aspects of annual financial reporting that could prove difficult to complete (e.g. engagement of valuation experts, completion of inventories)?
- Has consideration been given to how significant matters arising may be reported in the Governance Statement, the Statement on Internal Control and the financial statements?

Management will normally set out a number of risk treatment actions arising from the risk identification and assessment process. Progress in implementing or addressing these actions should be monitored by the audit committee or other appropriate forum.

It will also be useful for the audit committee to consider how the internal audit work programme has responded to the changes in risks facing the entity.

[3] The *Code of Practice for the Governance of State Bodies* sets out that boards of State bodies are responsible for preparing financial statements in accordance with relevant accounting standards including the requirement to prepare them on a going concern basis unless it is inappropriate to presume that the entity will continue in existence for the foreseeable future.

While risk management is likely to focus on the potential for negative outcomes there are likely to be opportunities for entities in the new environment for example innovation in the design and delivery of services. Guidance from the Department of Public Expenditure and Reform[4] highlights the importance of considering opportunities when undertaking risk identification and assessment.

Increase in the risk of fraud

The circumstances that many entities find themselves in may have increased the risk of fraud. Entities have had to quickly change the way they operate, including changes to controls, all of which may allow for greater opportunities for fraud.

The heightened fraud risks associated with the pandemic may include the following

- procurement rules and anti-fraud measures may have been downgraded or overridden in response to pressures or other priorities
- organisation-wide controls to prevent and detect fraud and procedural breaches may not have been designed to operate in remote or virtual environments
- cyber-security risks where the quick roll-out of new technology may have exposed networks security to cyber-attack or financial loss
- staff compliance with policies, rules and control requirements may have been weakened. For example, where staff are working remotely, they may become distracted or their actions may be subject to less scrutiny and monitoring. Similarly, pressure on management may reduce the required level of oversight.

Questions that the audit committee may wish to put to management or internal audit in relation to the potential for increased fraud risk might include

- Are there types of remote activities that might pose specific fraud risks (e.g. treasury trading employees, ability to change key supplier or bank details without supervision, staff working unusual patterns to mask bogus transactions)?
- Has robust segregation of duties remained in place (e.g. do processes provide for alternative reviewers and approvers in case key employees are off sick or unable to connect to the ICT network)?
- Are internal audit, fraud investigation and whistle-blowing procedures active and continuing to operate effectively?
- Are activities on remote working devices monitored? For example, how does management monitor staff compliance with sensitive data requirements and acceptable use policies in a remote working environment?
- Is the design of monitoring controls which can identify frauds appropriate for a remote or virtual working environment and are those controls operating?

[4] *Risk Management Guidance for Government Departments and Offices* www.govacc.per.gov.ie

The impact of changes to key control procedures including ICT controls

For most entities in 2020, there have been changes in the way financial transactions are administered with processing occurring remotely and without on-site supervision. It is important to review how those changes in key control procedures have operated in practice to ensure that the revisions have not resulted in an increase in the risk of error or fraud.

Examples of control risk factors which may be a sign that controls (including monitoring and oversight of financial systems) were not easily adaptable to remote or virtual working thereby increasing the susceptibility of financial systems to error or fraud include

- Operations and controls which historically relied on manual processes and where there may be little or reduced ICT capability in the entity to manage the change
- Operation and control changes which were made in haste (e.g. insufficient testing and staff training for the new control procedures)
- Circumstances in which the entity found it difficult to prepare its 2019 accounts or provide information to support the external audit (e.g. difficulties in accessing information, large volume of documentation is required to support transactions, difficulties in responding on a timely basis to routine information).
- A high level of serious control deficiencies identified from previous reviews or audits, or where deficiencies have not been adequately addressed in a timely manner.

The following questions on changes made to specific control activities might be useful for management (including ICT management) and internal audit when considering the types of issues and assurances that might be communicated to the audit committee.

Authorisation and approvals

- How did the changes made to systems and procedures impact on the robustness of the transaction authorisation and approvals process (e.g. to ensure that transactions are only authorised when they represent actual economic events; how/by who is expenditure validated to confirm it is for a valid purpose and that the specified services/goods have been received)?
- Have there been changes in the staff involved in authorising and approving transactions which may have weakened controls (e.g. were different personnel involved who may lack the necessary skills or experience, were there changes made which gave an individual an inappropriate authorisation or approval level)?
- How are the authorisation and approval of transactions recorded in virtual systems (e.g. how are the identities of the authoriser and approver recorded and verified; are there procedures to ensure that a clear record is kept and that authorisations/ approvals cannot be overwritten)?
- Are appropriate safeguards in place and have proper records been kept regarding the use of digital signatures (e.g. authorisation of only those staff who may use digital signatures, process to verify the individual's identity, how access to fobs is securely maintained, how password security is maintained)?

Reconciliations

- Are key reconciliations carried out in a timely manner by persons who are independent of transaction processing?
- Are errors identified by reconciliation processes properly addressed and on a timely basis?

Verifications

- How did the changes in procedures impact on the verification process (e.g. is there a checker/reviewer who verifies the data input on to the financial system, to appropriate source documents or evidence?)
- How did the changes impact on the process for ensuring that only transactions that comply with the entity's policies are entered into?
- Where grants are paid in a remote working environment, how is compliance by the grantee with the grant terms and conditions verified?

Changes to physical access and security controls

- How did the changes impact on the physical access to and security of assets?
- How did the changes impact on the secure retention of documents which evidence transactions?

Segregation of duties

- Were there any changes to roles and responsibilities which may have weakened segregation controls?

It is also important to consider the ICT aspects of any changes in control activities for working in the new environment.

General ICT controls

- Has the necessary infrastructure been provided to staff to work securely from home, including secure connections to the entity's network?
- If changes were made to ICT applications, how did ICT management ensure that there were no negative impacts on the integration with or operation of other applications?
- If changes were made to databases, how did ICT management ensure that there was no unauthorised updates to information in the database?
- If changes were made to the operating system, how did ICT management ensure that user access was appropriate and that no gaps in access security were created?
- How did ICT management ensure that file and network security was maintained?
- Were required patches applied across the network on a timely and consistent basis?

- How were vulnerabilities or intrusions in the ICT environment monitored?

ICT application controls

- Was remote working implemented in such manner that staff had access to all the necessary applications and could perform all the usual key controls (e.g. if access was limited in some way when compared to on-site working, did this negatively impact controls)?
- How did bank and supplier/customer account maintenance operate (e.g. were any changes made which could have given inappropriate access to accounts)?
- Where employees were reassigned roles in a different part of the business, was system/user account access reviewed (e.g. to avoid segregation of duties breaches)?
- Was security configuration changed which may have given staff unauthorised privileges or access at levels which should otherwise have been restricted?
- If upgrades were necessary to programmes or the ICT environment, how did ICT management ensure that the changes were implemented effectively?

Monitoring and oversight

Monitoring of internal controls is an ongoing process which underpins an effective system of control. It encompasses the work of the audit and risk management committee(s), internal audit, management reviews and oversight, other assurance reviews and communications with the external auditor.

In the new environment there are likely to be challenges in how this process operates due to the fundamental and rapid changes to the working and controls environment, pressure on the entity to meet existing or new business needs and the potential for negative impacts on management and staff. Some questions which an audit committee might consider when reviewing how these challenges and pressures have impacted on the entity's controls will include the following

- What has been the impact of the challenges and pressures on the entity's control environment?
- How effective have the risk treatment actions been in mitigating the major risks identified?
- What assurances are there regarding the effectiveness of any changes to the operation of controls?
- What assurances are there in regard to effective operation of network and cyber security controls?
- Were there any significant breaches or deficiencies in controls, including from actual or suspected frauds, and have they been properly addressed? Were such breakdowns assessed with a view to considering whether they may indicate more widespread problems?

- Are there any issues which may materially impact on the financial statements?
- What lessons can be learned on how the entity has managed the challenges of the new environment?
- How might the significant issues and changes to the systems of control be reported in the annual Statement on Internal Control?

Engaging with the external auditor

The external auditor's primary concern is about the risk that the financial statements may be materially misstated whether due to fraud or error. For the purpose of assessing financial audit risks, the auditor will be keen to understand the impact of the pandemic on the entity and its business environment. As part of this process, the auditor will also seek to understand internal controls relevant to the audit, including how changes made by the entity have impacted on the effectiveness of controls. This is in order to design and tailor the procedures to be performed as part of the audit.

The external auditor is also required to review the Statement on Internal Control (SIC) that accompanies the financial statements and which

- describes the various elements of the system of internal control including the fact that a review of the effectiveness of controls has been completed
- confirms compliance with procurement rules
- describes significant internal control issues (if any) or confirmation that no such weaknesses were identified which require disclosure.

It is expected that given the significant changes brought about by the pandemic that the SIC will address how the entity has dealt with the challenges in maintaining effective internal controls.

The external auditor considers whether the disclosures in the SIC are materially consistent with the financial statements and the knowledge obtained from conducting the financial audit. Where the disclosures are misleading or do not meet the requirement of the applicable corporate governance requirements, the auditor will in the first instance bring this to the attention of the entity before considering what further action may be taken.

The external auditor does not provide any assurance on the adequacy of the governance arrangements put in place by the entity, nor does the auditor form an

opinion on the effectiveness of the entity's corporate governance procedures or its risk and control procedures.[5]

The types of procedures and the level of interaction between the external auditor and the entity's management and audit committee will vary according to the complexity, size and risks faced by the entity. Some of the common procedures that the auditor is likely to perform include the following

- enquiring of the directors or senior officials to obtain an understanding of the process defined by the board or management for its review of the effectiveness of internal control
- examining relevant documentation, including management or board minutes and any other material prepared by or for the managers or directors relating to disclosures made in the SIC
- reviewing the evidence to support the disclosures made about procurement
- evaluating whether or not the evidence examined provides sound support for the disclosures made
- requesting those charged with governance to provide written confirmation of oral representations made during the course of the review
- considering whether the information contained in the SIC is consistent with auditor's knowledge obtained during the audit of the financial statements.

In light of the changes brought about by the pandemic, the auditor will be particularly interested in how management and audit committees have responded to the challenges and risks faced by the entity in the new environment. The responses to many of the questions and issues outlined in this guidance will be of interest to the auditor.

Where the auditor identifies significant deficiencies in internal control during the audit these will be communicated to those charged with governance on a timely basis. Significant deficiencies include those which in the opinion of the auditor could lead to a material loss or non-compliance with rules. Consequently, the auditor does not wait until the financial statement audit has been completed before reporting such deficiencies. In this way, management or directors are made aware of the deficiencies that the auditor has identified and are able to take account of them when preparing the SIC.

[5] Further information in relation to the auditor's responsibilities for reviewing the information required to be published by entities under the applicable corporate governance rules is available here