CONTROL NET

WHITEPAPER

How to manage internal controls

www.controlnetapp.com | © 2021

Contents

Introduction 3

What are internal controls? 4

What are the different types of internal controls? 5

Why are internal controls important? 5

How does internal control work? - Introduction to the 'COSO' and '3 lines of defence' models 6

What does the US Sarbanes-Oxley (SOX) stand for? 10

UK SOX - The who, what and when 11

Best practices for managing internal controls post-COVID 13

Improving governance and compliance with internal control software 15

Introduction

Governments and policymakers are constantly looking for ways to improve accountability in achieving an entity's mission and objectives and strengthen financial stability in the economy. One such way is undoubtedly the adoption and implementation of a comprehensive internal control system.

Effectively managing internal controls is critical for an organisation's entire operations and profitability as it allows the management to quickly adapt to changing economic environments, evolving consumer demands, risks and emerging technologies.

In this complete guide, we dive deep into the fundamentals of managing internal controls and risks, looking at the various types of internal controls, how they work, what are the regulatory control-related requirements in the UK and US, and some of the best practices for using internal controls in the post-COVID digital world.



What are internal controls?

Internal controls are the mechanisms, policies, and processes implemented by an organisation to ensure its financial stability and integrity, promote accountability, and protect from financial, strategic and reputational risk.

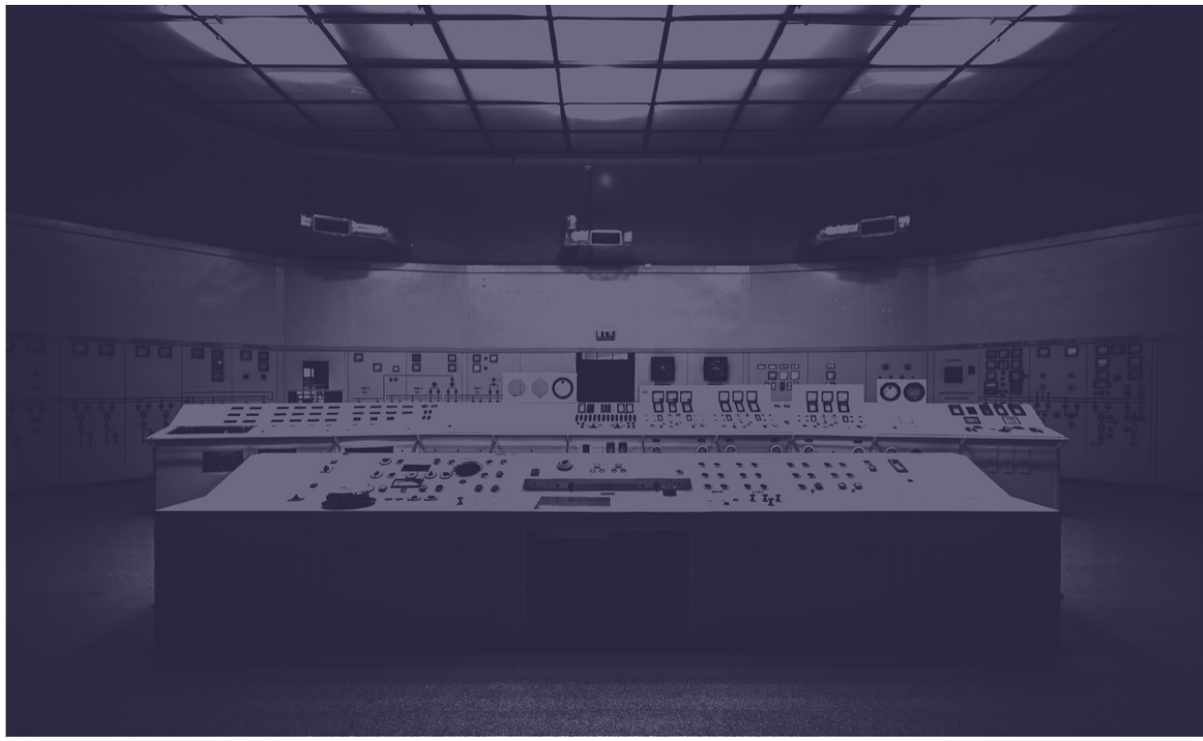
In addition to complying with laws and regulations and preventing fraud, internal controls can help organisations improve their operational efficiency and sustainability.

According to the Turnbull Report 1999, the purpose of any control system should be:

“To provide reasonable assurance that the organisation can meet its objectives”.

The Association of Chartered Certified Accountants (ACCA) identifies the following 5 key objectives of internal controls:

- Efficient conduct of business – Controls should be in place to ensure the smooth and frictionless operations of an organisation and avoid any operational losses and maximise profitability.
- Safeguarding assets – Having a comprehensive system of internal controls can help prevent financial fraud, errors, and misconduct.
- Preventing and detecting fraud and other unlawful acts – Internal controls can minimise the risk of fraud and other unlawful activities.
- Completeness and accuracy of financial records – A failure to keep an effective internal control process and system can lead to inaccurate financial data and records.
- Timely preparation of financial statements – The lack of internal controls can affect and delay the fulfillment of key business regulatory requirements like end-of-year accounts and financial reporting.



What are the different types of internal controls?

Preventative

Preventative controls aim to prevent any fraud or misconduct from occurring and usually involve practices like systematic documentation, authorisation and separation of duties. Some of the most common examples of preventative controls include authorisation of payments and expenses, or limiting individual access to inventory, cash and other tangible assets.

Detective

Detective controls are backup practices and policies that aim to identify events or items that have been missed by the first line of defence. One of the best examples of detective controls are reconciliations and external audit.

Corrective

Corrective controls are activities and measurements taken to rectify any issues that have already occurred and been detected, and prevent them from happening again. An example of a corrective control is deploying a new policy to destroy unnecessary data, to prevent attackers from stealing it.

Manual vs. IT Controls

In terms of execution, controls can also be manually or IT-managed. Manual controls are entirely managed by individuals, whilst IT controls involve implementing an integrated automated system or application.

An example of a manual control is when an authorised employee signs off a document or approves a payment. IT controls, on the other hand, usually form a complex system or application including automated processes like policy management, logical access, change management, and physical security.

Why are internal controls important?

Internal controls are important for any organisation as they help it meet its objectives, whilst remaining compliant with its regulatory, financial and operational obligations.

Internal controls can also help mitigate any internal and external risks, prevent fraud and improve the overall operational efficiency and sustainability of an organisation.

How does internal control work? - Introduction to the 'COSO' and the '3 lines of defence' models

The COSO control management framework

There are many ways to implement internal controls within an organisation, but probably the most popular one is the 5-component control management framework by the US Committee of Sponsoring Organizations of the Treadway Commission (COSO). The COSO framework provides a solid foundation for the effective management of internal controls by following 5 key components:

1) Control environment
This component covers key strategic business fundamentals like a company's leadership team, mission, goals and objectives. It also includes core operational elements like ethics, integrity and corporate social responsibility policies.

The structure of every control environment varies, but it usually includes the board of directors, management team, and HR. Having the right people in the right roles is key to the success of any organisation.

2) Risk assessment
How exposed an organisation is to both internal and external risks. Risk assessment is essential to identifying and tackling a company's threats and weaknesses. Depending on the type of business and industry, the process usually involves examining a company's level of resistibility, efficiency and discovering any potential drawbacks. Risks can range from fraud, cyber-attacks and manual or technical errors to regulatory and financial risks.

3) Control activities
This component covers all policies and procedures an organisation has implemented to ensure its continuity in the case of an emergency. Being proactive and having a robust control system is crucial for achieving both an organisation's short and long-term objectives.

Control activities may be preventive or detective in nature and may be performed at all levels of the organisation.

4) Information and communications
Corporate communications and the level of information shared both internally and externally play an integral part in an organisation's effective task delegation and smooth

operations. A failure in communications can be detrimental to a company's profitability and ROI.

5) Monitoring
Whilst assessing, identifying and rectifying any operational inefficiencies and risks lay the foundations for success, the ongoing monitoring and regular reporting ensures its realisation in the long-term and keeps an organisation on track with its objections and goals.

The COSO internal control framework

5 Components	17 Principles
Control environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk assessment	6. Specifies suitable objectives 7. Identifies and analyses risk 8. Assesses fraud risk 9. Identifies and analyses significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys control activities through policies and procedures
Information and communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

The 3 lines of defence model

The COSO Internal Control Integrated Framework has proven to be an effective way for establishing and managing a comprehensive control environment and mitigating organisational risks, but it fails to outline the relevant roles and actual responsibilities for each component of the COSO model. In order to ensure accountability and avoid any effort duplication and operational costs, organisations should have clear role specifications and task delegations.

The 3 lines of defence model aims to tackle just that. At the core of the model is the idea that "under the oversight and direction of senior management and the board of directors, three separate groups (or lines of defence) within the organization are necessary for effective management of risk and control".

Each group has the following core responsibilities:

1. Own and manage risk and control environment (front-line operating management)
2. Monitor the risk and control environment to support the overall management (risk, control and compliance departments)
3. Provide independent assurance to the board and senior management that risk and controls are managed effectively (internal audit)

Whilst the structure of the 3 responsible groups might differ between organisations, there are a number of critical principles that are equally implicit for each company:

1. The first line of defence lies with the business and process owners who are responsible for managing the risks that can affect the company's operations and prevent it from achieving its objectives. This group is also usually tasked with the development and execution of a comprehensive internal control system.
2. The second line of defence is placed to support the management and its major goal is to make sure that all risks and controls are managed appropriately and effectively. Essentially, this is an oversight function that owns a large aspect of the management of risk within organisations.
3. In contrast to the second line of defence, the third line is usually not a management role and is solely appointed to provide assurance to senior management and the board of an organisation. Its main responsibility is to offer an independent and objective evaluation, reporting and recommendations to the board, and is served by internal auditors.

The 3 lines of defence model

1st line of defence

Management controls

Internal control measures

2nd line of defence

Financial control

Security

Risk management

Quality

Inspection

Compliance

3rd line of defence

Internal audit

What does the US Sarbanes-Oxley (SOX) Act of 2002 stand for?

The Sarbanes-Oxley Act (SOX), also known as the Corporate Responsibility Act, is a US regulatory framework that was implemented in 2002 in response to a series of large corporate frauds in the US capital markets. It introduced a new set of reforms to existing securities law and imposed much stricter penalties on executives and organisations that committed accounting fraud against investors. The main objective of the mandate was, therefore, to increase accountability within boards for more accurate and reliable financial reporting. This also meant tighter and more demanding internal control requirements for organisations.

SOX is all about corporate governance and financial disclosure. So, a large aspect of it is focussed on ensuring the accuracy of financial reporting and facilitating the processing of financial transactions through the so-called internal controls over financial reporting (ICFR). According to Section 404, all publicly traded firms, regardless of size, must include an Internal Controls Report in their year-end financial reporting, whilst all large organisations must also have an external annual audit of their ICFR.

In addition to the strict regulatory requirements, SOX also introduced a protection measure for company whistle-blowers who are willing to provide evidence of fraud, which prohibits companies from retaliating against them.



UK SOX: Who, what and when?

In the UK, the existing requirements for adequate financial reporting and accounting records seem to be consistent with the SOX regime in the US. According to the UK Companies Act, “The board should monitor the company’s risk management and internal control and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report”. However, as there’s currently no formal regulatory framework for the implementation of those requirements, the majority of corporates in the UK tend to be complying with them only notionally.

To tackle this, over the past few years, the UK’s Financial Reporting Council (FRC) has been working on developing a UK equivalent of the US SOX regulation.
Recommendations for the implementation of an internal controls and audit reform were first published by Sir John Kingman in 2018. Following Kingman’s publication, the Institute of Chartered Accountants in England and Wales published the Brydon Report in 2019. The report further reiterated the need for a clear audit regulatory framework “to help establish and maintain deserved confidence in a company, in its directors and in the information for which they have responsibility to report, including the financial statements.”

According to the latest predictions by the UK FRC, a form of UK SOX is expected to be officially launched in 2023/2024. The implementation of the new regime kicked off at the beginning of this year, with the publication of a consultation whitepaper by the UK Department for Business, Energy & Industrial Strategy (BEIS). The whitepaper proposes “a package of measures aimed at improving the UK’s audit, corporate reporting and corporate governance systems”. Below is a brief summary of the key points covered in the report, titled ‘Restoring Trust in Audit and Corporate Governance’:

Who will be affected by the UK SOX regime?

The new UK SOX regime is expected to affect only the largest corporations or all listed entities in the UK.

What is UK SOX all about?

The UK SOX will resemble the US version of the regulation, but it’ll be slightly lighter, or implemented on a more discretionary basis, in relation to external auditing. Similar to the US mandate, UK directors and boards will be responsible for monitoring the company’s risk management and internal control environment. They will also be required to execute an annual review and issue a report on how effective their risk and control management efforts and systems have been.

Besides coming up with a new formal regulatory framework, as part of the new mandate, BEIS is also planning to establish a new Auditing, Reporting & Governance Authority (ARGA) that will replace the existing Financial Reporting Council (FRC). The new regulatory body will continue to serve as a quality assurance audit authority, but it will further take responsibility over the updated Code of Local Audit Practice – the guidelines councils are required to follow – and will need to publish annual reports on the state of local audit.

When is UK SOX going into effect?

The mandate's implementation process started in March 2021, with the release of the Government's consultation whitepaper, 'Restoring Trust in Audit and Corporate Governance'. The consultation will continue until 8 July 2021. There's still no definitive date when the new regulatory framework will go into effect. As mentioned earlier, FRC expect this to happen in 2023/24 at the earliest.



Best practices for managing internal controls post-COVID

The COVID-19 pandemic has shaken up the entire business world whilst impacting almost any industry, organisation and operational function. Internal audit (IA) and controls are not an exception. With remote working becoming the norm, organisations are facing an increasing number of operational risks and challenges, which has put some greater pressure on IA teams to quickly adapt to the new working environment, ensure compliance during the transitional, recovery phase, and provide some direction for the future. Below are some of the best practices and considerations for IA to respond to the new normal.

3 risk factors for organisations post-COVID

Before we look at some of the best practices for IA in the post-COVID environment, we'll briefly outline the 3 key risk factors driving those considerations.

Regulatory compliance

Due to the COVID-19 pandemic, many regulatory authorities have altered various laws and regulations in aim to strengthen the economy and facilitate businesses' recovery. This creates an extra burden for internal auditors who need to constantly keep up to date with any key regulatory changes and ensure the organisation remains compliant at all times.

Fraud

Whilst remote working facilitated business continuity during the pandemic, it also created some new opportunities for fraudsters to exploit any weaknesses in operational controls (e.g., no clear visibility of control breaches, reduced inventory or data control, no clear control managing responsibilities and accountability). KPMG has identified some of the most common control-related frauds:

- Misconduct by employees for personal financial gain
- Manipulation of financial results to comply with covenants
- Bypassing transaction controls, or forging of the necessary approvals
- Non-execution of approved transactions for personal or professional gain
- Processing of fraudulent claims for personal gain, or to benefit a known party

Performance and reporting

Remote working further increased the need for greater management oversight as key responsibilities like monitoring, measuring and reporting on the financial and operational health of the organisation can be easily overlooked.

This brought some more pressure on the IA function, which has the responsibility to ensure the accuracy, completeness and adequacy of reporting in key areas like; Revenue, Liquidity, Cash-flow, Procurement and transactions, Inventory, etc.

To tackle those risks and build a strong and resistant internal control environment, KPMG recommends IA to consider implementing any, if not all, of the below critical areas:

- Adopting a digital sales process and onboarding
- Managing liquidity risk (incl. cash flow forecasting and working capital)
- Ensuring business continuity (remote working setups and policies, digital communications, etc.)
- Increasing governance over remote working and mitigate the risk of cyber fraud and breaches
- Navigating vulnerable customers and facilitating the sales and customer services processes remotely
- Ensuring the effectiveness of financial controls in the new remote environment

Looking at the internal function, in particular, KPMG has also proposed the following 7-step approach for internal auditors to adapt and continue to provide valuable insights and assurance to their organisations in the post-COVID world:

- Define and prioritise the critical controls required to reduce fraud, compliance, and performance and reporting risks
- Identify who has responsibility for monitoring new critical controls arising from the “new normal” (e.g., work-from-home arrangement)
- Assess the impact of changes on internal controls and revisit organisational structure, if required
- Identify and leverage on lessons learnt from the crisis to further improve the internal control system
- Enhance auditors’ capabilities and fill any knowledge gaps
- Identify and evaluate the emerging risks in the aftermath
- Adopt additional technology to increase security and efficiency, and automate business processes



Improving governance and compliance with internal controls software

Adapting to the constantly changing organisational environment is proving to be extremely challenging for IA teams, especially in the new remote-first, post-COVID world. In addition to keeping up with the new government legislations and regulations, industry best practices and economic changes, internal auditors are now also required to be much more proactive and responsible for navigating both external and internal operational risks and controls. Having an efficient process and robust system in place can significantly enhance the role of IA, and help avoid the risk of non-compliance, fraud and/or other operational failures and losses.

What is 'Control and risk management software'?

Control and risk management software solutions can help improve the efficiency of an organisation's entire operation whilst making it more transparent and secure. Nowadays, there are various risk and control products organisations can choose from, but they all tend to offer some or all of the following key functionalities:

- Project management
- Data repository and file management / digital workspaces
- Real-time reporting and notifications
- Planning and scheduling tools

Top 5 benefits of using an internal control and risk software

1) Streamlined operations
By automating the management of internal controls and risks, organisations can create an evidence-based operational environment with appropriate accountability.

2) Simplified and enhanced audit process
Using a control and risk management software reduces the manual burden on IA and allows for greater transparency reducing the risks of non-compliance, financial loss and reputational damage.

3) Reduced costs
Automation means less paper and manual efforts, which can significantly reduce the costs of audit and compliance.

4) Increased transparency and enhanced GRC
Technology allows organisations to create a fully reliable control and risk management process with real-time data storage, access, reporting and notification functionalities.

5) Increased profitability
By streamlining the operations within an organisation, control and risk management software solutions can further boost the profitability and performance of the entire business, and help achieve its short and long-term objectives.

References:

https://www.accaglobal.com/ca/en/student/exam-support-resources/fundamentals-exams-study-resources/f1/technical-articles/internal-controls.html

https://www.coso.org/documents/coso-crowe-coso-internal-control-integrated-framework.pdf

https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2020/12/covid-19-providing-assurance-in-the-new-normal.pdf

https://www.sarbanes-oxley-101.com/

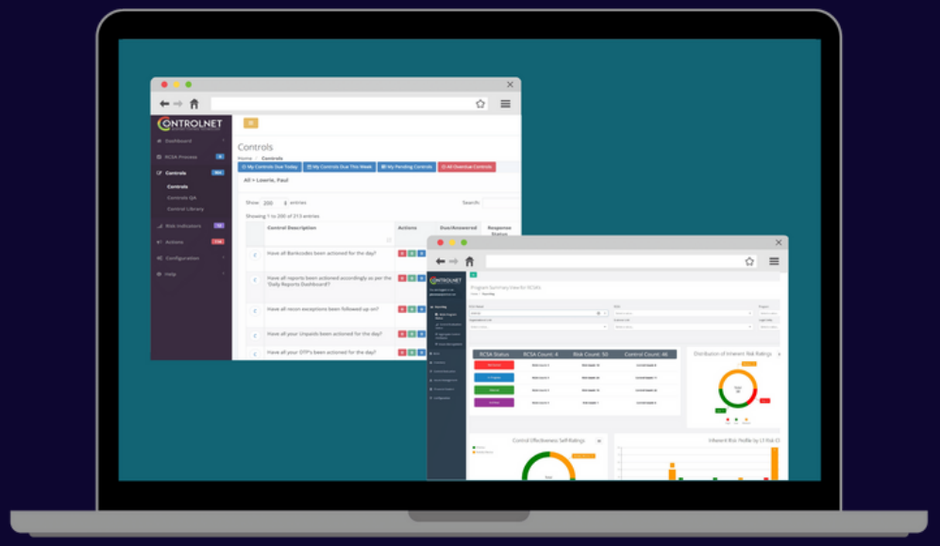
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/970676/restoring-trust-in-audit-and-corporate-governance-command-paper.pdf

https://www.icaew.com/insights/viewpoints-on-the-news/2021/may-2021/arga-powers-strengthened-on-local-government-audit

About ControlNet

ControlNet is an end-to-end control and risk management system that allows organisations to manage their risk and control environments in a cost-effective and secure way, with ease.

By digitising the management of organisational controls and risks, ControlNet eliminates the need to use inefficient, manual and paper-based systems and processes. ControlNet's technology allows organisations to manage the controls and risks across all 3 lines of defence: Business line management, Risk management, and Audit.



Learn more and book a demo at:
WWW.CONTROLNETAPP.COM

Trusted by:

RBC · BR1DG3P01NT3 YOUR SIGNAL IN THE NOISE · FNZ · Delta Capita · RMB · 1762 BREWIN DOLPHIN

© 2021 ControlNet Limited

SUBSCRIBE

CONTROL NET

Digital control and risk management.