Deloitte.

Mission: control in financial services

The emergence of the Chief Controls Officer

Contents

Introduction

The control of non-financial risk is a key priority for the first line of defence, and for the Chief Operating Officers charged with accountability for managing risk. Attention from boards of directors, regulators and auditors has sharpened focus on the topic, while COOs grapple with the associated challenges of compliance with the Senior Managers Regime, complex legacy environments, cost pressures, fragmented assurance approaches and a rapidly evolving threat landscape.

An increasing number of large financial services institutions have recently created the role of Chief Controls Officer (CCO) to address internal control as a topic in its own right. In this publication, we assess this development as a response to these challenges. We consider features of the existing landscape that are driving the development of the role, and assess these in the context of the often-unresolved question of the gap between the first and second lines of defence, as well as other gaps and overlaps in coverage that can emerge in the first line.

In particular, we look at these challenges through the lens of the emerging CCO: what are the qualities a CCO needs to address them, what are the success factors they must deliver, and the potential pitfalls when doing so? Many of these questions do not have a single correct answer, but we believe considering them will be of benefit for anyone in the first line of defence who is charged with accountability for risk and control, whether or not they choose to employ a CCO model.

Tackling these challenges will bring benefits in the form of better control of risk, efficiency of control and of control assurance, consistency of approach, and more transparent, meaningful management information. The imperative to improve is compelling, and there are practical steps that any organisation should consider to achieve that improvement.

Summary

The challenge

1. New challenges in risk and control
There is a renewed focus on risk and control, requiring management to be able to demonstrate how they are confident their risks are well controlled. This comes from:

- The Board
- Regulators and government
- Audit

This is in the context of a challenging landscape for control in the first line driven by multiple factors:

- Complex control environments
- Inconsistent control approaches
- Shareholder expectation
- Cost pressures
- Changing risks
- Auditor rotation

2. Mind the gaps
Effective coordination across the three lines of defence is required to respond. There is a risk of a "gap" between the first and second lines, made more challenging by factors including:

- Structural reform and consolidated service functions
- The extended enterprise, with increased outsourcing
- Regulatory requirements on individual accountability
- New technologies

Typically functional COOs are expected to lead the response. There are separate but linked responses required from:

- Business unit COOs
- Support function COOs

The response

3. The Chief Controls Officer
An increasing number of large financial services institutions are responding by creating the role of Chief Controls Officer, leading a Chief Controls Office function. Regardless of whether this title is formally used, we look at some of the qualities required of individuals charged with responsibility for controls, as Stewards, Strategists, Catalysts and Operators, before going on to look at how such functions can be set up to succeed.

4. Factors for success

Define accountabilities to ensure it is clear which responsibilities for control are delegated, how this delegation operates, and where overall accountability lies.

Establish the mandate, making clear what activities the CCO function is responsible for and what is performed elsewhere, including risk identification and appetite setting, standards setting, assurance, remediation and reporting.

Design the operating model to suit the mandate, taking account of resourcing, reporting lines and organisational structure, centralised or decentralised approaches, and talent, location and sourcing strategies.

Focus on risk to ensure that reporting on risk exposure is not lost in the industry of controls operation, assurance and remediation activities.

Deliver efficient assurance, taking a risk-based approach and making use of a range of assurance techniques – not just periodic testing – as well as considering assurance requirements across the extended enterprise.

The benefits

5. Realising the benefits

- Improved control of risks
- Confidence in control
- Efficiency
- A risk-aware organisation

Mission: control in financial services | The emergence of the Chief Controls Officer

1. New challenges in risk and control

A sharper focus on the control of non-financial risk

Non-financial risk extends beyond the traditional definition of operational risk to encompass a wider range of consequential risk categories, including reputational risks. It is receiving renewed focus from boards, regulators and auditors, increasing the demand for management to be able to demonstrate that risks are well-controlled.

- From the board, control of non-financial risk has become a priority in response to high-profile cultural failures, and a growing awareness that impacts can be reputational as well as financial. Board members, especially non-executive directors, increasingly need to be able to demonstrate that they have a strong grasp of these risks and are confident that they are controlled to within appetite.
- From regulators, the focus comes through a greater emphasis on establishing individual management accountability for the control of risk, and from an increased expectation that compliance with particular regulations can be evidenced. In areas such as financial crime, privacy and risk data reporting it is no longer sufficient to be compliant, but rather management must also be able to demonstrate how they are confident that they are compliant.
- From auditors, external audit rotation is seeing some organisations uncover previously unaddressed control issues, as new auditors arrive with new priorities for the focus of their work. Meanwhile, internal audit functions are beginning to include risk and control culture audits on their annual plan, and some are using this as a proxy for measuring culture overall.

For management in the first line of defence, this focus has put the demonstrable control of non-financial risk firmly back on the agenda.

A challenging landscape

For many firms, the current context of cost pressures, legacy complexity and a changing external landscape combine to make the management response to this requirement a significant challenge.

- Control environments are complex, may be poorly understood, and can be difficult to manage effectively. There is a need to undertake remediation of legacy issues whilst simultaneously responding to business change.
- There is inconsistency, with differing control standards across the framework of risks and existing assurance requirements being met in a fragmented fashion. Silos of assurance activity take place across multiple first line units, each with its own approach and standards.
- There is an increased expectation that controls will not just ensure compliance, but protect shareholder value through the protection of critical assets, margins and reputation.
- Cost pressures drive demand both for more efficient controls and more efficient assurance of controls. There is focus on the return for spend on risk management, and the case to fund strategic or wide-scale change for the control environment can be difficult to make convincingly when compared with ongoing tactical fixes.
- The emergence of new technologies – for example, robotic process automation – and new risk factors, such as increasing use of third parties across the extended enterprise, present challenges for control approaches that were not designed with them in mind.
- The stakeholder audience for risk information is extending, as organisations report on a wider range of metrics for which controls become relevant, including environmental impact, diversity and inclusion, and customer outcomes.

These challenges require robust and well-understood control frameworks, with organised and efficient assurance activities that deliver meaningful and actionable management information. The demand on the first line of defence to meet these requirements has never been greater.

2. Mind the gaps

The first and second lines of defence

The first line of defence is responsible for the primary management of the risks to which the business is exposed, and management in the first line must feel confident that their controls operate effectively to achieve this. Effective risk management for the enterprise as a whole, however, requires coordinated action across all three lines of defence.

In particular, establishing the clear division of accountability and responsibility for risk management and control between the first and second lines of defence is a perennial challenge in many organisations, and is a problem without a "one size fits all" solution. The demarcation between the first two lines, and resources required for each, depends on factors including risk type, organisational culture, risk appetite and the level of maturity of the first line. The appropriate demarcation may vary even within an organisation, depending on differences in these factors.

Where the demarcation becomes unclear, or a gap is allowed to develop between the first two lines of defence, the achievement of the overall objectives for risk management are put at risk. We believe there are market trends currently driving an increase in both the likelihood of, and the threat from, such a gap developing:

- Structural reform, including subsidiarisation and ring-fencing, and the consolidation of central service functions, is increasing the complexity of the relationship between business units and their support functions. If not properly managed this can reduce the level of oversight of risks to the business unit that arise in the support functions.
- The increasing use of outsourcing creates a complex extended enterprise across which risk oversight is required, involving many third parties not under the direct control of the business.
- New regulatory requirements on management accountability – for example the UK Senior Manager Regime – have focused regulators on the governance of risk at the entity-level, and sharpened minds as to how this governance translates into individual, day-to-day executive accountability.
- The changing nature of new risks – for example, the rapid growth of cyber as a risk – demands a concerted response from the lines of defence, with responsibility for areas such as policy setting, control implementation and control assurance clearly defined. This is taking place in a context in which the availability of specialist expertise in these areas is often limited.

The COO as controller of non-financial risk

The Chief Operating Officer of a business unit or support function will typically be assigned first line of defence responsibility for the overall management of non-financial risk. In discharging this, he or she must consider both risks that arise and are controlled within his or her direct management domain (being the business unit or support function), as well as those which arise elsewhere, in a support function or third party supplier.

For the business unit COO, the task is to understand what all relevant risks are – regardless of where the risks arise – and establish comfort that they are controlled within appetite, regardless of where the controls are operated.

Just as the business unit depends upon other functions or suppliers to operate these controls, the COO will depend upon these functions or suppliers to provide timely and robust management information to demonstrate the effective management of risk. Likewise, it may be within the power of the business unit to set appetite for a particular risk, or they may inherit an appetite that is set at the group level. In either instance, they will depend on advice from specialists in the risks concerned.

For the support function COO, the task is similar, in that he or she will need to gain comfort over the control of risks within the function, and the other functions upon which the function depends for services. But the function must also be able to service the demand for the related assurance, management information and expertise from the business units. The COO is less likely to independently set risk appetite for their function, but will be expected to participate in the setting of risk appetite for the group as a whole, particularly in their domain of expertise.

For both, considerable effort and expertise is required to manage risk, assure controls, and produce and consume meaningful information from these activities. The population of controls is likely to be large, may be poorly understood, and there may not be confidence that the controls being operated are the right ones for the risks. The threat of another gap arises: the gap which can exist between the business units and those that serve them. The COOs must work together to design effective cross-functional approaches to risk management, and build control capability within their function to support this.

3. The Chief Controls Officer

Dedicated first line risk and control capability

The need for dedicated risk management resource in the first line of defence is not a new one, and almost all regulated firms have long-established – and widely varying – approaches to meeting this need. Embedded "business risk managers", the "1b line of defence", "risk and control champions": the terms used to describe them are as varied as the models employed. In almost all cases, however, they are providing the first line COO with risk control and assurance support, to assist in discharging the responsibility to manage non-financial risk.

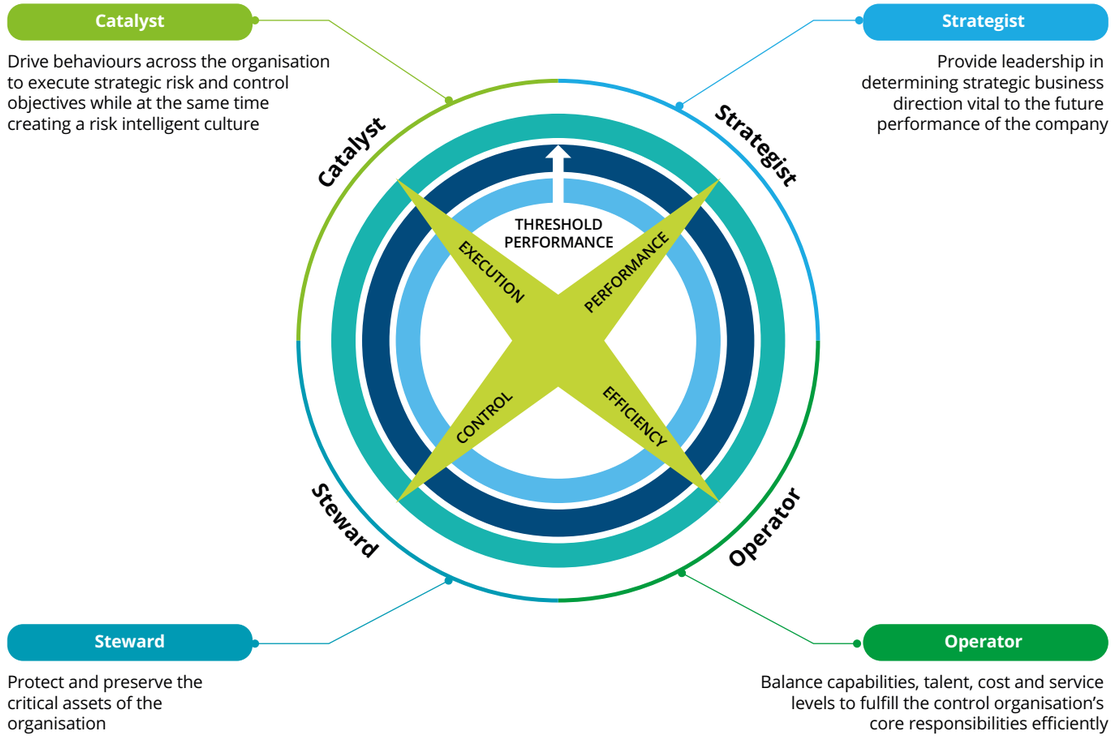
Recently, we have seen the emergence of a new senior role, and supporting function, at a number of large regulated firms: the Chief Controls Officer. CCOs are being appointed to address the challenges described in the sections above, in an attempt both to bridge the gap to the second line of defence, and to close the gaps that exist in the first.

Is this just a relabelling of the long-established first line capability, or something different? Whilst many of the activities performed by the CCO function will be familiar, certain characteristics of the role suggest it is a departure from what has gone before:

- Creation of a senior role – the overall CCO – with oversight for all "1b line of defence" activities.
- Concentration of first line risk and control capability in a single function (be it within a particular business unit or support function, or firm-wide), led by a CCO with primary reporting lines up to the COO; and
- Consolidation of assurance, reporting and stakeholder management capabilities within this function.

The qualities of the CCO

What qualities should a CCO possess to be successful? The Deloitte "four faces" model provides a framework to analyse this question:



From the nature of the role itself, it is clear that all CCOs will be expected to act as:

- Strong stewards, as the overseer of risk on behalf of the COO, and as the caretaker of controls and protector of organisational assets in their business unit or function; and

- Catalysts for risk aware behaviour in the organisation, driving the cultural transformation in which all first line staff act as risk managers and recognise the value of control.

The specific mixture of all four qualities is likely to vary, particularly depending on whether the CCO is in a business unit or service function.

Business unit CCOs are likely to emphasise strategist qualities, providing the leadership needed to align risk appetite and the approach to risk management with the overall strategic focus of the business. Further, the business unit CCO needs to be able to export this alignment to the functions that support them.

Service function CCOs may be more likely to emphasise operator qualities as they respond to the logistical challenge of delivering risk management in a vast and complex operational environment that serves many stakeholders. This is not to say the service function CCO will not also need to be a strategist: particularly in larger functions such as Technology, where essentially they are the CCO of a major technology business serving many clients in its own right.

For a new CCO – or anyone taking on an equivalent role in the first line of defence – early assessment of the qualities they believe they will need in their specific circumstances, and early focus on the practical steps they will need to take to emphasise these, will help to set them up for success.

4. Factors for success – and pitfalls to avoid

Clarity of purpose of the CCO function – from its early design onwards – will enable it to succeed. In this section we analyse some of the factors that should be considered in this design, and the pitfalls to avoid. Whether or not your organisation is formally building a CCO function, considerations will be useful for anyone with first line of defence risk management responsibility.

Define accountabilities

Assuming that the business unit or function COO has overall accountability for the respective control environment, it should be clear which of these responsibilities have been delegated to the CCO, and which responsibilities remain with, or have been delegated to, others in the first line of defence.

This consideration is key, not least as clear definition mirrored in practical implementation will give significant comfort to regulators when assessing the effectiveness of risk oversight arrangements.

Pitfalls	Practical responses
Accountability for risk and control in the first line is unclear, and the CCO role creates confusion in the first line as to where the accountability lies, and who is responsible for the day-to-day execution.	The firm's Responsibilities Map and the Job Descriptions for individuals should be drafted to align with the reality of the operating model, and in a way that avoids overlaps or gaps in the allocation of responsibility. Adequate communication should be employed to ensure that each first line manager is aware of their accountability and responsibilities under the model. Assessment of individual management performance should take account of these factors to identify and correct defects in the discharge of the roles.

Establish the mandate

The need for clear accountabilities naturally extends to establishing the mandate of the CCO function. Depending on the model to be employed, it should be clear how the accountabilities translate into activities to be performed by the CCO function, and, just as importantly, what is performed elsewhere. It should be clear whether the function is primarily responsible for, or else what role it plays in performing activities, including:

- Horizon scanning and identification of new risks;

- The setting of risk appetite for the business unit or function and the alignment of this to the organisation's appetite for non-financial risk;

- Measurement of risk;

- Definition and implementation of controls in response to identified risks;

- Standards setting for particular risk types and the provision of expertise to support the first line;

- Assurance over control effectiveness, whether through testing or other means;

- Reporting on risk and control effectiveness, including aggregation across the organisation and across risk types; and

- Remediation of control weaknesses.

Pitfalls	Practical responses
The CCO function does not clearly define the activities it is responsible for, leading to poor understanding in the first line as to how risk and control is to be managed in practice, and a gap to second line expectations.	Clear definition of CCO function activities and how these interact with other risk and control activities for which the first line is responsible. Close and continuous engagement with the second line of defence to ensure responsibilities are clear.
The CCO function takes on a mandate it cannot deliver due to conflicts.	Articulation of the CCO function as primarily a management and assurance function, with responsibility for control design, implementation, operation and remediation remaining elsewhere in the first line, avoids the potential for self-review by the CCO function.

Design the operating model to suit the mandate

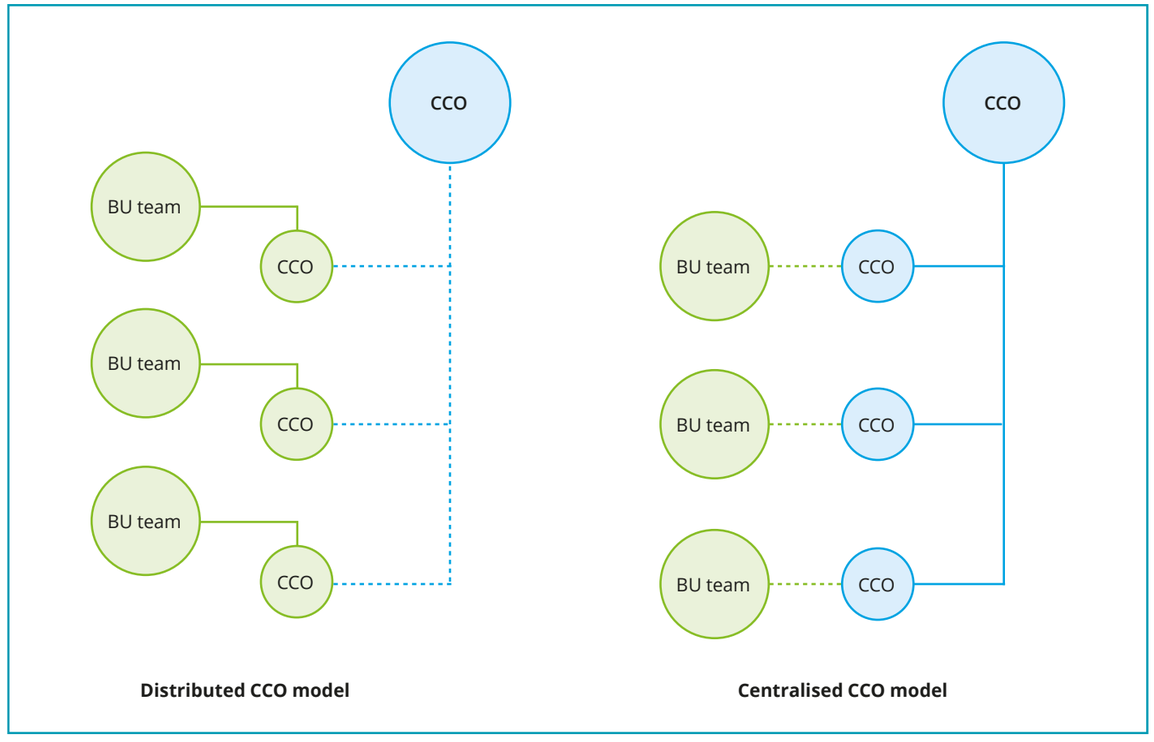
With a clear purpose established, the operating model of the CCO function should be designed to deliver these. Key design questions include:

Resourcing

Is the CCO function adequately resourced – both in scale and expertise – to deliver its mandate? A thin-layer CCO function may be effective if focused on aggregation and reporting of risk and control information generated elsewhere in the first line. A CCO function responsible for standard setting and control assurance will conversely be much more resource-intensive, but may deliver these capabilities with greater efficiency than if they are left distributed across the first line.

Reporting lines

Is the primary reporting line of CCO resources up to the CCO in a centralised model, or to the local business areas and teams they support in a distributed model?



The appropriate model will depend on the specific circumstances, but each comes with advantages and disadvantages:

Model	Advantages	Potential disadvantages
Distributed	Close integration with local business areas delivers a CCO service most tailored to their requirements, demonstrating value to the business.	Likely to be more expensive to implement, and lead to a lower level of consistency. It will also make it harder for the CCO to drive change effectively.
Centralised	Easier to achieve a high level of consistency in approach, standards and methodology, supporting consistent reporting and straightforward aggregation. The model also lends itself to more straightforward sourcing strategies.	Value to the business is less immediately apparent, and resource is concentrated in a single cost pool which is then an easier target for reductions.

Talent, location and sourcing strategy

Setting the talent strategy for a CCO function depends in part on its mandate: will the CCO function have specialists in individual risk areas capable of undertaking detailed assurance activities? Or will it offer highly commoditised services with a lower price point? If the former, a further talent challenge may arise, as care must be taken to design career pathways that attract highly skilled individuals to the function.

Likewise, the operating model should consider location and sourcing strategies to be employed in the function, dependent upon the mandate. Onshore resource co-located with the business units can more easily provide challenge and demonstrate benefit, but at a higher cost. External sourcing may be used to either supplement the core capability of the function as required – for example in a particular specialist risk area – or in a more wholesale fashion, for example by outsourcing all controls testing activities as a managed service.

Pitfalls	Practical responses
The CCO function is not resourced to deliver on its mandate, either in scale or expertise.	Development of a business case for the function that clearly articulates the non-financial benefits, and quantifies the financial benefits from the consolidation of currently fragmented assurance activities, and the automation of assurance processes. Definition of expertise requirements to meet the mandate, with a clear strategy to source.
The CCO function is unable to attract and retain sufficient numbers of qualified, motivated resources.	Definition and implementation of career pathways for CCO resources that allow for development and growth, potentially including rotation in and out of first line delivery roles and/or the second and third lines of defence. Identification of highly standardised tasks – for example, standardised test scripts – that can be delivered in a low-skill commoditised fashion or automated.

Focus on risk

A significant pitfall for any first line risk management capability can be an excessive focus on the industry of controls – their operation and related ongoing assurance activities in a complex, process-driven environment – at the expense of properly understanding the level of risk. A successful CCO function will leverage an understanding of control as a tool to better understand risk.

The CCO should therefore remain aware of the emergence of new risks: horizon scanning for both internal and external factors that indicate the risk profile of their business unit or support function is changing, and taking steps to ensure that the controls in place meet these risks. Likewise, the CCO should consider ongoing changes in the regulatory environment that may have relevance to their business unit or support function, and ensure both the controls in place and the assurance activities are designed to achieve compliance with these.

In maintaining this risk awareness the CCO of a business unit may find they focus more on changes in the external risk landscape and potential impact on the business, whereas the CCO of a support function may be more focused on changes in overall organisational risk appetite and the implications of these.

A successful CCO function will leverage an understanding of control as a tool to better understand risk.

The CCO should support continuous improvement of the reporting used in the first line to ensure that it addresses risk, rather than focusing on controls alone. Reporting on the effectiveness of controls and the progress of control remediation efforts can be a vital part of fulfilling the CCO mandate, but this is not a substitute for properly reporting on the level of risk exposure, and whether it is within appetite.

Pitfalls	Practical responses
The CCO function is not able to respond to developments either in the risk landscape or organisational risk appetite.	Ongoing horizon scanning for new risks or regulatory requirements, either within the CCO function itself or by consuming this scanning from elsewhere in the three lines of defence. Periodic refresh of assurance priorities against risk appetite.
Excessive focus by the CCO on the industry of control assurance execution at the expense of understanding the risk.	Explicit linkage of the activities of the CCO function through to the wider risk framework. The management information produced by the CCO function assesses residual risk, rather than focusing exclusively on control effectiveness and control remediation activities.

Deliver efficient assurance

Assurance is likely to be core to the mandate of any CCO function, and needs to be delivered in a way that produces meaningful outputs in an efficient fashion. The potential for centralisation inherent in a CCO function may help to drive efficiency and consistency, but other key considerations to enable this include:

Integrating and rationalising the assurance approach

Many organisations are moving towards a more integrated assurance approach to improve the efficiency of controls assurance. This involves balancing the need to demonstrate embedded control of risk with the need to improve efficiency, and is driven by increased collaboration across the three lines of defence to reduce duplication in testing and assurance activities. Some organisations are taking risk-based, prioritised approaches to determining controls in scope for assessment and the associated level of assurance required, as well as considering work already undertaken in a particular area by the second and third lines of defence.

Moving beyond testing

Often "control assurance" is treated as synonymous with the testing of controls: a periodic cycle of manual test procedures. This can be expensive to deliver, can prioritise checking the box over understanding the risk, and can leave issues unaddressed in the period between test cycles. Efficiencies can be gained by automating part of this testing, but organisations are also considering alternative ways in which management can gain assurance that risks are adequately controlled.

These alternatives include implementing the continuous monitoring of controls through Key Control Indicators (KCIs), or the direct measurement of residual risk through Key Risk Indicators (KRIs). Both have the advantage of providing management information that is closer to real-time, enabling more rapid action to address risks that are out of appetite.

It may also be possible to deploy a reliance approach which removes the need for direct assurance activity by making us of work that has already been performed by the second or third line, or by relying on the work of service auditor reports produced by third party suppliers and service provider.

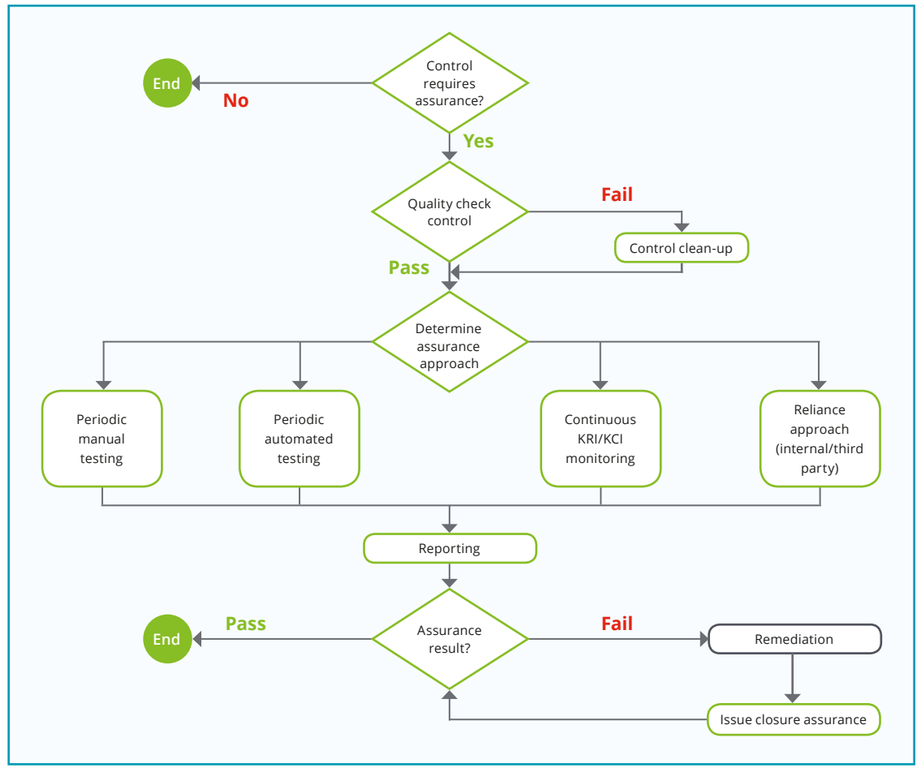
Considering the extended enterprise

The assurance approach must consider risks that arise in the extended enterprise – third party suppliers and service providers – as of equal significance to those that arise internally.

The CCO function can actively contribute to designing this approach, and participating in activities including third party risk assessments, ongoing vendor monitoring, and determining the reliance approach for service auditor reports, or the approach to be taken where such reports are absent.

Many organisations are moving towards a more integrated assurance approach to improve the efficiency of controls assurance.

The diagram summarises a possible controls assurance approach that makes use of each of these factors:



Pitfalls	Practical responses
Excessive focus on the testing of controls as an activity, at the expense of understanding whether the underlying risk is well-controlled.	Deployment of innovative approaches to control assurance – including the integration of reliance approaches across the three lines of defence, automation of testing activities, and continuous monitoring of KRIs or KCIs – to both improve the fundamental understanding of risks and drive efficiencies.
A higher standard of control – and control assurance – is provided for internal controls than those in the extended enterprise.	Comprehensive integration of the approach of the CCO function with the governance structures established for outsourcing and supplier relationships.

Remain flexible

In considering all of the above factors, it is important to recognise that no one model will be appropriate for every organisation, or even for all of the business units and support functions within a given organisation.

The CCO function should be designed to fit the specific needs, maturity and risk appetite of the area it supports, and should be designed with the capacity to change over time as these underlying factors change.

5. Realising the benefits

The challenges we have discussed in this publication are not simple ones to address, but concerted effort and investment to overcome them will deliver significant benefits.

Improved control of risks

The underlying objective of all controls activity is to ensure that the non-financial risks the enterprise is exposed to are controlled to within appetite. Proper focus on these risks, and a coordinated approach to controls activity, will inherently drive improvement in control. This will not only reduce operational losses and the frequency of failures, but is also a positive contributor to the achievement of operational excellence.

Confidence in control

Improved quality, consistency and application of available information about risk allows management to confidently assert that risks are under control and regulatory obligations are being met, and be able to evidence their basis for this assertion. Further, it equips management to direct remediation investment to the areas that are genuinely outside of appetite, maximising the value delivered by this investment.

Efficiency

Focusing controls on a true understanding of risks will help to ensure that the costs associated with control are commensurate to the level of control that is desired. The consolidation and standardisation of assurance and reporting activities will drive efficiencies in these domains.

A risk-aware organisation

The unambiguous statement from management that control of non-financial risk is a priority for an organisation will drive a culture that is more risk aware in its totality. This will encourage the majority people for whom risk and control is not the primary focus of their role to nonetheless think about their day-to-day activities through this lens.

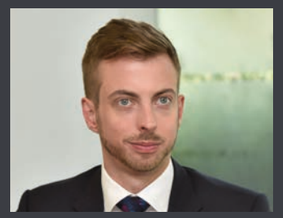
Ultimately, the control of risk becomes a source of competitive advantage for the organisation, and allows management to demonstrate the value that is delivered by investment in control.

Contacts

Jack Pilkington
Partner
Risk Advisory
+44 20 7303 7735
jpilkington@deloitte.co.uk

Stephen Lucas
Partner
Risk Advisory
+44 20 7303 5088
stelucas@deloitte.co.uk

Fiona Walker
Partner
Audit & Assurance
+44 20 7303 7620
fiwalker@deloitte.co.uk



Tom Kohler
Director
Risk Advisory
+44 20 7007 5156
tkohler@deloitte.co.uk

Deloitte.

Designed and produced by The Creative Studio at Deloitte, London. J15656