KPMG

Health Service Executive (HSE)

Review of the Compliance Operating Model

Final Report – Executive Summary Extract

November 2022

Table of Contents

1. Executive Summary

1.1. Introduction

Based on the work of Internal Audit (IA) and the results of the individual internal audit engagements, the 2021 Annual Report of the National Director of Internal Audit provided an overall audit opinion that 'limited assurance' can be provided in respect of governance, risk management and financial control processes[1]. Based on the Internal Audit opinion (which has been maintained since 2019), this means that '*there are weaknesses in the system of governance, risk management and controls which create a significant risk that the system will fail to meet its objectives. Action is required to improve the adequacy and/or effectiveness of the system*'.

As a result, during 2021 the Chief Executive Officer (CEO) and the Executive Management Team (EMT) approved the commencement of a three-year plan intended to improve the HSE's current internal control framework. This controls improvement plan is a key objective for the HSE and is led by the office of the Chief Financial Officer (CFO). This plan focuses on six major work steams. Work stream # 6 focuses on the investment in an enhanced Second Line of Defence (2LOD).

In 2021, following the HSE's Review of its corporate centre, a Governance and Risk Function was established reporting to the Chief Strategy Officer (CSO). This function has responsibility for: the governance and compliance function (the design of which is the subject of this report); enterprise risk; and legal services. Other functions including Protected Disclosures, the National Children First Office and Appeals Service are also part of the broader Governance and Risk function. In addition, in November 2021 a Chief Risk Officer (CRO) was appointed. It is in this context that the Health Service Executive (HSE) appointed KPMG to provide advisory services relating to its current Governance and Compliance (G&C) Framework and Function.

To note, and to avoid confusion with other functions in the HSE, the Governance and Compliance (G&C) Function will be referred to as the Central Compliance Function (CCF) in this report. It is also worth noting that Corporate Governance processes in the HSE are being delivered by the HSE's Board Office and by the Head of Corporate Affairs. The role of the CCF in the future proposed model relating to Governance, will relate to the establishment and maintenance of Compliance related governance structures and activities, and its role on key strategic and operational change fora, to review and challenge the impact of change initiatives on the HSE's Compliance profile.

Our scope and approach are outlined in **Appendix A**. This report summarises our observations and recommendations relative to the current and future state operating model for the HSE's CCF.

1.2. Background and Context

The HSE was established in January 2005 and is responsible for providing health and personal social services to everyone living in Ireland. The HSE is the largest organisation in the State. It has a budget of more than €21 billion, and with over 132,000 Whole Time Equivalent staff members[2] provides a wide range of essential health and social services through acute hospitals and within the community.

[1] HSE Annual Report and Financial Statements 2021
[2] HSE Annual Report and Financial Statements 2021

The HSE provides a range of acute hospital and community services (directly managed or HSE funded), in communities across the country.

The HSE exists within a complex health service ecosystem including agencies funded by the HSE under Section 38 and Section 39 of the Health Act. As separate legal entities, the relationship of these funded agencies with the HSE from a governance and compliance perspective has been considered as part of this review. Similarly, as the HSE itself undergoes structural change with the introduction of Regional Health Areas (RHAs) per the Slaintecare strategy, the governance, risk and compliance activities of the HSE may need to be adapted for this organisational change.

The HSE is committed to fulfilling its compliance obligations in all areas and activities of its operations. It is key that the HSE complies with applicable legal, regulatory, and internal requirements, professional and industry standards. **Robust Compliance Management practices delivers confidence to the HSE Board and Management in the quality and value of services delivered to the public and assists the Board in its oversight of the organisation**. As such, adherence to compliance requirements such as Health Acts, Regulatory Standards (issued by organisations, such as, the Health Information and Quality Authority (HIQA) and Mental Health Commission (MHC)), EU Regulations (e.g. GDPR), Public Policy (e.g. Department of Finance Procurement (DOF) rules, Department of Public Expenditure and Reform (DPER) Code) and Core HSE Policies, Procedures, Protocols, Guidelines (PPPGs) supports the HSE's conformance with good practices and minimum expectations in the delivery of Corporate HSE Processes (Finance, HR, others) and also of Clinical and Care Services.

1.3. Summary scope of work

The scope of this review was to:

1. **Support the development of a Compliance Obligations Register (COR)**. For the HSE to identify and validate the core compliance responsibilities.

2. **Document the current state ("As is") of the HSE Compliance activities and processes.** To understand and map the HSE's core compliance related functions and management processes and identify any gaps.

3. **Develop the HSE Compliance Framework**. To design a compliance framework for the HSE including proposals for the establishment of a Central Compliance Function outlining its mandate and its role vis a vis other governance and compliance functions in the HSE.

4. **Develop the HSE's Four Lines of Defence (4LOD) Assurance Map**. To develop a high-level governance, risk and compliance assurance map across the Four Lines of Defence (4LOD).

5. **Develop the future ("To be") operating model for the Central Compliance Function including high-level implementation and resourcing plan**. To recommend a future operating model and propose a high-level implementation and initial resourcing plan to deliver the recommendations from this review.

Additional scope of services are outlined in **Appendix A**.

1.4. Summary findings and recommendations

1.4.1. Elements of good practice observed

Based on our review, we noted a number of areas of good practice. Some examples include, but are not limited to:

- **The HSE Board through its Audit and Risk Committee (ARC) strongly supports and promotes the importance of robust Compliance management processes**. In particular, we noted that the ARC fully supports the establishment of an impactful, well embedded, influential and value adding Central Compliance Function (CCF).

- **Self-awareness of key issues and willingness to improve.** We noted several improvement initiatives currently underway to help uplift compliance processes and more generally to help uplift the quality of the HSE's control environment. For example, we noted efforts to improve coverage over HR compliance related processes through the establishment of a dedicated HR Pay Compliance Unit. We also noted efforts to improve and automate Quality and Patient Safety (QPS) data management and performance; and we noted efforts from Finance to establish a national data repository and reporting database and tool to support the analysis of key controls.

- **The HSE has established and seeks to improve existing monitoring and assurance mechanisms** such as the National Performance Oversight Group (NPOG), the System of Internal Controls (SIC), and the Performance Accountability Framework (PAF).

- **Although improvements and more mature processes are needed, several teams in the HSE are undertaking some type of compliance related monitoring and assurance activities**. These teams include Finance (and Procurement), the Compliance Unit for Funded Agencies (part of the Operations Function), the Quality and Patient Safety Function (part of the Clinical Function), Human Resources, ICT Management, Capital & Estates, and the Children's Hospital Programme Assurance (both part of Health Care Strategy); and

- **Internal Audit has expanded and provides assurance across both healthcare and non-healthcare activities**. The Healthcare Audit function was amalgamated with the Internal Audit function in 2021. Since then, these audits were formally included as part of the overall HSE 2022 Internal Audit Plan. In 2022, 402 audits are planned to take place: 209 audits across Dublin and Regional Operations; 143 Healthcare Audits; 28 Special Projects & Investigations; and 22 ICT audits.

1.4.2. Summary of key observations on the current operating model and recommendations to improve effectiveness

Notwithstanding the above, we also noted several challenges with the current Compliance operating model at the HSE. Below we have summarised key observations and improvement opportunities noted during our review.

1. Governance and Mandate

Priority: High

The HSE Board (through the ARC), the EMT and the CRO place strong emphasis on uplifting the management, prominence and visibility of Compliance Risks across the HSE. **The establishment of an appropriately resourced CCF** with an organisational mandate, profile and standing is needed to increase effectiveness of compliance activities. Specifically:

- **CRO attendance and reporting at the Board, the ARC and other Board Committees, and at EMT meetings needs to be enhanced.** The CRO attends the Board, the ARC, other Board Committee meetings, and EMT meetings (as needed) to provide risk related updates. However, Compliance related updates are not provided to the Board, ARC, other Board Committees or EMT at an agreed frequency or as part of a standing agenda. Compliance related updates are ad-hoc, and they do not follow a standard or dedicated compliance specific reporting format. This limits the visibility over Compliance matters at these key fora;
- **Compliance related Second Line of Defence (2LOD) Committees / Working Groups need to be expanded.** An EMT led Executive Committee to support the CEO and CRO in relation to the oversight of Risk and Compliance matters is not in place (a common practice at comparable organisations such as other large state bodies in Ireland). Also, the existing forum to discuss risk matters is the Corporate Risk Support Team (CRST) but the remit of this forum does not include Compliance activities;
- **The voice of Compliance at Strategic and Change fora should be established.** Compliance (and the CRO) do not have a formal presence on key fora in place to oversee strategic, operational, or regulatory changes. This means that a Compliance review and challenge role at those forums is largely missing; and
- **The Compliance Mandate and Compliance Framework need to be implemented, and a Compliance related Risk Appetite statement needs to be developed and implemented.** A Compliance Mandate or Framework were not in place and were drafted recently as part of this review. These will be the subject of an implementation plan once the Framework has been adopted. Also, while the HSE Board has approved a Risk Appetite Statement, a specific Compliance Risk Appetite statement has not been developed.

2. Organisation and Location

Priority: High

A formal Three Lines of Defence (3LOD)[3] model including defined roles and responsibilities has been

[3] The 3LOD Model is a recognised Model that distinguishes between three layers of Risk Management and Internal Control. We have considered and applied the model from an HSE perspective. To do so, we considered (1) the context in which the HSE operates; and (2) how the 3LOD model can apply from a Corporate HSE perspective. **The First Line of Defence (1LOD)** is the management layer responsible for oversight of the activities in HSE directly managed and HSE funded services. / **The Second Line of Defence (2LOD)** is responsible for setting Risk and Compliance related policies, and for performing monitoring and assurance activities / the **Third Line of Defence (3LOD) – Internal audit** is responsible for providing independent assurance on the adequacy of the HSE's internal control, risk management and governance systems and activities.

recently documented in the draft Compliance Framework. **The organisational structure of the CCF needs to be established**. Roles and responsibilities aligned to deliver the Framework and a stakeholder management model are needed to enhance effectiveness. In particular:

- **The structure of the CCF needs to be established.** Activities currently performed by 2LOD teams do not align with the recently developed draft Compliance Framework. As such, the organisational structure of the CCF needs to be established, and roles and responsibilities determined to deliver the Framework; and
- **A relationship management framework should be implemented.** This should include specific points of contact for each First Line of Defence (1LOD) function. Once points of contact are established, a consultation process and communications programme on the new mandate and relationship management model should be carried out.

3. Activities and Processes

Priority: High

Compliance related monitoring and assurance activities are undertaken by some 1LOD functions, but activities are immature (for the most part) and improvements are required. Compliance related reporting is undertaken by 1LOD functions though this is fragmented and lacks visibility. In general, key compliance processes need to be developed and others require substantial improvements to enhance, standardise and centralise key compliance activities. Specifically:

- **A 1LOD Maturity Assessment Model needs be developed and implemented to assess the maturity of 1LOD functions performing compliance related monitoring and assurance activities.** Currently 1LOD functions are not required to meet minimum standards to perform compliance related monitoring activities. These activities are for the most part inconsistent and immature. It is critical for the CCF to assess the maturity of 1LOD functions that perform compliance related monitoring and assurance activities to determine: (i) activities where reliance can be placed by the CCF; and (ii) where support is needed from the CCF to mature and develop these activities. This maturity assessment by the CCF, and support to enhance the maturity of the 1LOD functions should form part of the CCF mandate and Compliance Monitoring Plan;
- **A suite of supporting Compliance Policies, tools, and methods to support the implementation of the Compliance Framework needs to be developed.** At a minimum, this includes developing the following Policies and Standards: Compliance Risk Assessment Policy, Compliance Issue Management Policy, Compliance Monitoring and Assurance (CMA) Methodology, and Compliance Training and Awareness Methodology;
- **The Compliance Obligations Register (COR) needs to be finalised and risk assessed.** The HSE COR is under development, owners have not been assigned to each obligation, and controls have not been mapped. In addition, the COR has not been risk assessed or classified by materiality to identify Principal Compliance Obligations to be reported to the ARC and to support the development of the Compliance Monitoring Plan;
- **A risk-based Compliance Monitoring Plan needs to be developed and implemented.** Key sources of information have not been assessed centrally to form a view of the most significant Compliance Risks to the HSE, e.g., the risk assessment of the COR; outcomes from previous monitoring and assurance reviews; compliance breaches; regulatory findings (C&AG, HIQA, MHC, other regulatory bodies); and relevant complaint trends/findings/issues;
- **A centralised issues management process to identify, manage and report on compliance issues**

needs to be established. Currently, (i) there is no centralised process or policy in place to identify, record, classify, remediate, and report on compliance issues; (ii) Issues reported by 1LOD functions do not follow a standard format, are not classified by materiality, and do not follow an agreed governance pathway; and (iii) there is no formal reporting of compliance issues to the CCF, which limits the ability to identify thematic issues and also limits the ability to provide consolidated/aggregated reporting of material compliance issues;

- **Centralised and aggregated reporting needs to be established.** Centralised consolidated compliance related reporting is not in place; there are no clear or agreed upon governance pathways for compliance related updates; and there is no stand-alone aggregate compliance related reporting relative to the HSE Compliance Risk profile for any governance fora including the Board, ARC, other Board Committees or EMT; and
- **A HSE organisation wide Compliance training plan needs to be developed, resourced and delivered.** Although ad-hoc Compliance related training takes place, an HSE organisation wide Compliance training plan has not been developed or delivered.

4. Technology and Data

Priority	Medium

Most Compliance related activities are being primarily managed and tracked through manual processes such as spreadsheets. Although some systems are used to manage specific Compliance activities (such as the data repository and reporting tool being developed by the Finance function), the HSE should consider **implementing an eGRC solution** to support compliance aspects such as COR maintenance; centralising and automating the recording of material Compliance issues; and implementing aggregated/consolidated compliance reporting.

5. People and Skills

Priority	High

As outlined in the Organisation and Location sub-section above**, the structure, roles, and responsibilities of the CCF need to be designed and resourced to deliver the duties and requirements specified in the draft Compliance Framework**. In addition:

- **CCF staffing levels and skills need be established**. The National Director of Governance and Risk is the HSE CRO, who also currently has responsibility for Compliance. A head (dedicated leader) of the new CCF (at Assistant National Director level) has not been appointed, a skills assessment has not been performed, and key activities to inform staffing levels to fulfil the mandate of the CCF have not been carried out, given the mandate has only recently been codified in the draft Compliance Framework. This includes approving the CCF operating model; completing the risk assessment of the COR; and determining the maturity of 1LOD functions; and
- **1LOD Compliance related staffing levels and skills need to be reviewed**. A skills assessment for 1LOD functions that perform compliance related monitoring and assurance activities has not been carried out. 1LOD resourcing and capabilities need to be determined once 1LOD functions formalise their mandate and the compliance related activities they perform, vis-à-vis the COR, are assessed, and activities and processes are assessed against the minimum requirements. See Section 4.3.1 for a summary of the Minimum requirements for 1LOD functions performing compliance related monitoring and assurance activities developed as part of this review.

6. Performance Management

Priority	Medium

Compliance related performance management are provided by different teams as part of Key Performance Indicators (KPIs) included in the National Scorecard. **The current KPIs need to be enhanced.** A suite of Compliance Performance measures that takes into consideration the Compliance Framework (which has been developed as part of this review) has not been developed. As such, key components of the Compliance Framework that may need to be tracked and measured have not been determined, e.g., Training and Compliance Monitoring Plan – completion percentage.

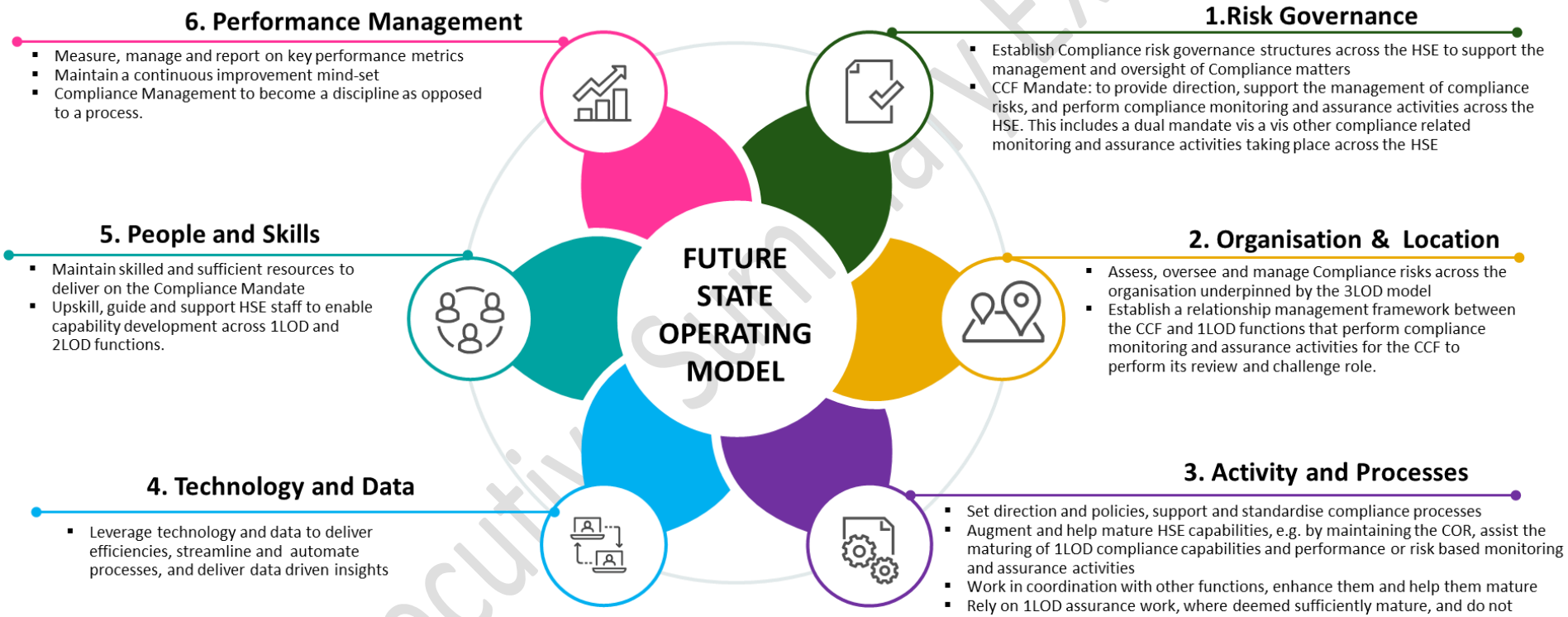
IMPORTANT NOTE: The Compliance Framework and new Central Compliance Function described in this report represents a significant change to the current way in which the HSE manages Compliance across the organisation. As such, the implementation of the Framework (which is aligned with principles of ISO 37301:2021 Compliance Management Systems standard), will require a large-scale programme of change and the assignment of additional dedicated resources (CCF and 1LOD functions) which will need to be continually assessed as Compliance activities mature.

Detailed recommendations to address the improvement opportunities set out above have been outlined in **Section 5**. A roadmap of activities has also been outlined in **Section 7****.**

1.5. Future state operating model - Overview

The Compliance Framework and CCF Future State Operating Model was designed applying key operating principles based on compliance management good practices (see **Section 3** for Second Line of Defence (2LOD) good practices and how these were applied to the CCF). Below, we have outlined key principles applied across each of the six operating lenses.

Figure 1. CCF Future State Operating Model



1.6. Future State Operating Model - Key Benefits

Key benefits from the implementation of the Compliance Framework and CCF Operating Model include, but are not limited to the following:

1	**Greater visibility of compliance risks through improved monitoring and reporting**. Centralised and aggregated independent reporting mechanisms are established for Compliance matters with Compliance updates tailored to the Board, EMT, ARC, other Board Committees, NPOG, the (to be created) ERCC, and the CRCSF in accordance with the guidance and frequency set out in the Compliance Framework. Technology is also leveraged to support the delivery of key Compliance processes such as COR maintenance, performance of risk and compliance reviews, and to support centralised and aggregated reporting.
2	**Enhanced EMT and Board oversight and assurance of compliance across the HSE**. The compliance profile of the HSE is measured against appetite set by the Board, monitored, and discussed regularly at key EMT fora (including dedicated risk and compliance forums (the ERCC and the CRCSF)) and the ARC. Stand-alone Compliance updates are delivered by the CRO to the EMT and ARC, other Board Committees (as relevant) and to the EMT on a quarterly basis. In addition, the CCF has a formal review and challenge role at key strategic and operational change fora to highlight potential compliance or regulatory risks in relation to organisational or strategic change.
3	**A dedicated CCF is in place with sufficient and appropriately skilled resources to provide oversight of compliance obligations and minimise compliance risks by challenging and assuring compliance related activities performed by 1LOD functions**. A Head of Compliance is appointed, and the CCF team structure is established to deliver key duties as outlined in the Compliance Framework. Compliance obligations are managed between the CCF and those 1LOD functions that perform compliance related monitoring and assurance activities, with the CCF supporting the development and maturing of 1LOD activities and challenging them as needed.
4	**Coverage, oversight, monitoring, and assurance of compliance obligations is also enhanced, and the management, escalation and remediation of issues improves**. The maturity of 1LOD functions that perform compliance related risk monitoring and assurance activities is assessed regularly to determine: (i) where reliance can be placed by the CCF on the monitoring and assurance activities performed by 1LOD functions; and (ii) where support is needed to mature the activities performed by 1LOD functions. The CCF itself will also perform assurance of compliance obligations and will implement a risk-based Compliance Monitoring Plan approved by the ARC. A centralised Issues Management process to identify, manage and report on compliance issues is also established.
5	**The Management of HSE Compliance activities and risks improves significantly**, with the CCF setting direction, policies, and methodologies. The delivery of Compliance activities is improved and standardised, reducing fragmentation in the design and management of compliance, while enhancing 1LOD capabilities. A complete listing of compliance obligations (COR) is maintained and is risk assessed on a regular basis to classify each obligation by materiality. Material obligations will be subject to a higher degree of assurance and will be reported to the ARC regularly.

1.7. Quick Wins – within six months

Assuming appropriate sponsorship and resources are assigned to both the implementation programme and the CCF, below we have outlined the main outcomes that are expected to be delivered within the first six (6) months following the establishment of the CCF:

1	**Centralised and aggregated Compliance reporting is implemented at key governance fora**. CRO delivers Compliance related updates to the Board, ARC, other Board Committees, EMT, and the ERCC at an agreed frequency. These updates follow a standard and dedicated Compliance specific reporting format and are tailored to each governance fora. It is recognised that this reporting will mature as the Compliance Framework gets implemented.
2	**A dedicated Risk and Compliance Committee is established chaired by the CRO**. The HSE will have an EMT led Executive Committee (in the form of an Executive Risk and Compliance Committee (ERCC)) to support the CEO and the CRO in relation to the oversight of Risk and Compliance matters. This will uplift the coverage, prominence, and visibility of Risk and Compliance matters at an Executive level.
3	**Formal CRO attendance at every EMT meeting**. This will enable the CRO to have visibility of key strategic, operational and change initiatives that take place across the HSE, and to advise, and perform a review and challenge role as needed at EMT meetings in relation to compliance matters.
4	**Minimum compliance standards are set to assess the maturity of 1LOD functions performing compliance related monitoring and assurance activities are implemented for selected functions and outcomes are reported to the ARC and other relevant fora.** Minimum standards outlined in the Compliance Framework (such as formality of mandate; formality of approach and output; and adequacy of the Governance path followed) are assessed (at a high-level) for at least three functions (e.g., Procurement; the Compliance Unit for Funded Agencies; and HR Pay Compliance Unit). The CCF determines their maturity, identifies improvements needed, supports their development, and reports on outcomes and progress.
5	**Compliance Risk Appetite for the HSE is established and reported**. A Compliance Risk Appetite Statement is implemented including measures, tolerances, and limits. Compliance reporting is expanded to include Compliance Risk profile vs appetite.
6	**A Compliance Obligations Register (COR) is developed, obligations are classified by materiality and reported to the ARC**. A complete listing of compliance obligations is developed, validated by EMT members and with owners assigned for each obligation. Obligations are classified by materiality, with material obligations subject to a higher degree of assurance and with reporting included at ARC compliance updates. This will form the basis for the Compliance risk assessment and Compliance Monitoring Plan development.
7	**A Head of CCF is appointed and a skills and resourcing assessment is performed for 1LOD and 2LOD to deliver the new model**. This includes performing a forward-looking skills and capacity analysis to determine the headcount and skillset needed to fulfil the mandate of the CCF.

For additional guidance, to deliver the above, we expect that, at a minimum, a Head (dedicated leader) of the CCF (at Assistant National Director level) is appointed and is supported by at least 5 WTE's initially to deliver the quick wins above. As an indication, we estimate the CCF will require circa 10 WTE's in addition to the Head of the CCF, to deliver on the foundational elements of the Compliance operating model.