KPMG

Health Service Executive (HSE)

Review of the Compliance Operating Model

Final Report

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.

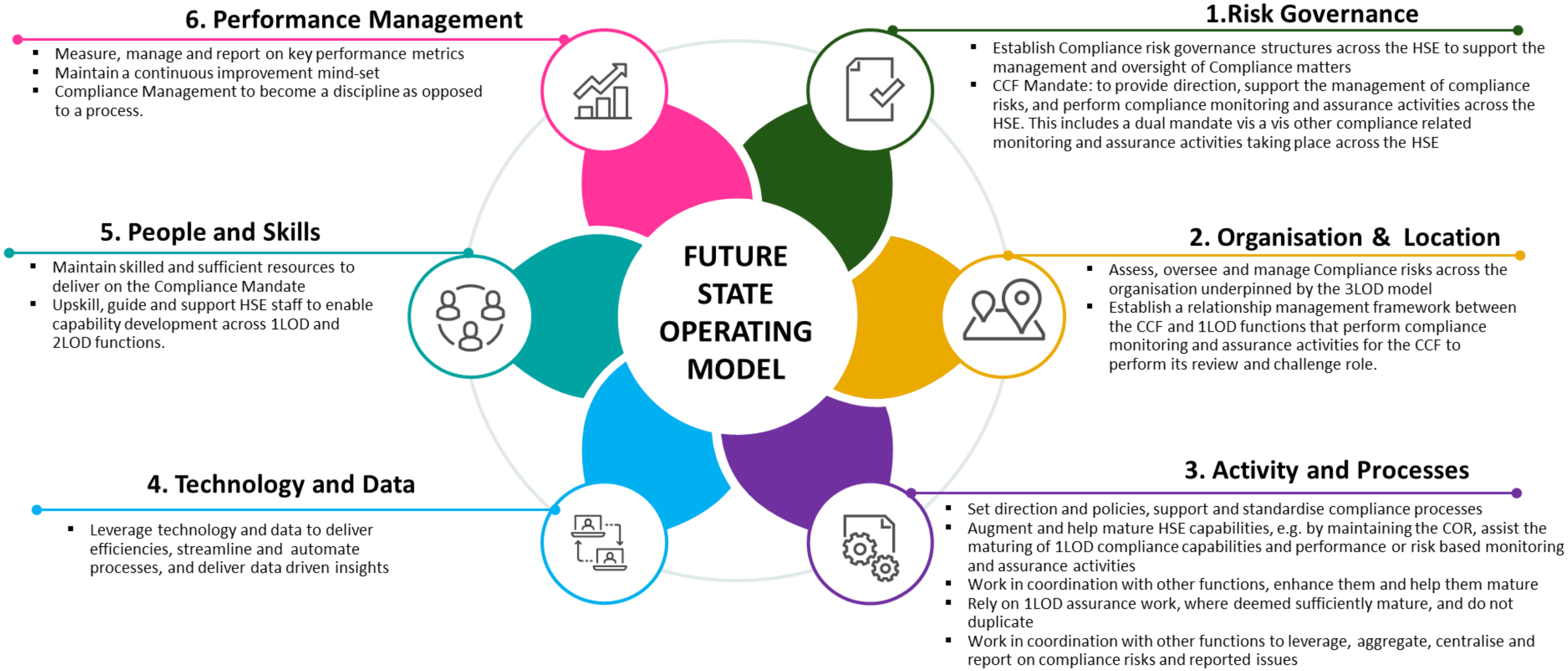
IMPORTANT NOTE: The Compliance Framework and new Central Compliance Function described in this report represents a significant change to the current way in which the HSE manages Compliance across the organisation. As such, the implementation of the Framework (which is aligned with principles of ISO 37301:2021 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



FUTURE STATE OPERATING MODEL

1.Risk Governance

- Establish Compliance risk governance structures across the HSE to support the management and oversight of Compliance matters
- CCF Mandate: to provide direction, support the management of compliance risks, and perform compliance monitoring and assurance activities across the HSE. This includes a dual mandate vis a vis other compliance related monitoring and assurance activities taking place across the HSE

2. Organisation & Location

- Assess, oversee and manage Compliance risks across the organisation underpinned by the 3LOD model
- Establish a relationship management framework between the CCF and 1LOD functions that perform compliance monitoring and assurance activities for the CCF to perform its review and challenge role.

3. Activity and Processes

- Set direction and policies, support and standardise compliance processes
- Augment and help mature HSE capabilities, e.g. by maintaining the COR, assist the maturing of 1LOD compliance capabilities and performance or risk based monitoring and assurance activities
- Work in coordination with other functions, enhance them and help them mature
- Rely on 1LOD assurance work, where deemed sufficiently mature, and do not duplicate
- Work in coordination with other functions to leverage, aggregate, centralise and report on compliance risks and reported issues

4. Technology and Data

- Leverage technology and data to deliver efficiencies, streamline and automate processes, and deliver data driven insights

5. People and Skills

- Maintain skilled and sufficient resources to deliver on the Compliance Mandate
- Upskill, guide and support HSE staff to enable capability development across 1LOD and 2LOD functions.

6. Performance Management

- Measure, manage and report on key performance metrics
- Maintain a continuous improvement mind-set
- Compliance Management to become a discipline as opposed to a process.

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.

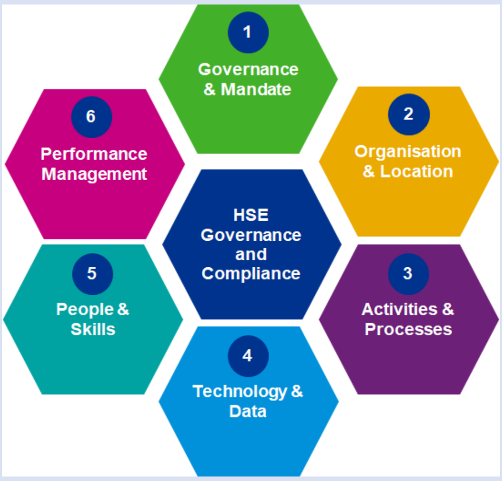
For additional guidance, to deliver the above, we expect that, at a minimum, a Head (dedicated leader) of the CCF (at Assistant National Director level) is appointed and is supported by at least 5 WTE's initially to deliver the quick wins above. As an indication, we estimate the CCF will require circa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

2. Methodology and Approach

2.1. Methodology

We applied KPMG's analysis methodology for Control Function Operating Models which consists of applying the following six lenses:

Figure 2. KPMG's Control Function Operating Model methodology



1. Governance and Mandate	This lens considered the mandate and objectives of the Central Compliance Function, its reporting lines and relationships with the Board, Executive Management, and other key 1LOD and 2LOD fora.
2. Organisation and Location	This lens considered the organisation structure, roles and responsibilities to manage Compliance matters across the HSE. It also considers whether certain activities to support the mandate are centralised or decentralised.
3. Activities and Processes	This lens considered the scope of Compliance activities, processes, policies, procedures, and methodologies. This includes but is not limited to approaches to setting Compliance related Policies; identifying key Compliance Obligations ('Universe') and controls in place meet the obligations; conducting Compliance Risk Assessments (CRAs); providing training and awareness; carrying out Compliance testing, monitoring and assurance, setting out approach to issues management and providing aggregated Compliance reporting.
4. Technology and Data	This lens considered the availability and use of technology-based tools, and the potential to make greater use of Data Analytics.
5. People and skills	This lens considered the quantity of resources in the Central Compliance Function (and those available in a decentralised model) and the skillsets and experience of those resources.
6. Performance management	This lens considered the performance review and assessment structures in place within the Central Compliance Function and the KPI's to support the achievement of the Functions objectives.

2.2. Approach

Informed by our experience in delivering similar Compliance Function Operating Model reviews both locally and internationally, our team applied our Control Function Operating Model methodology to propose recommendations relative to the HSE Central Compliance Function Future Operating Model and implementation roadmap. In undertaking our review, we:

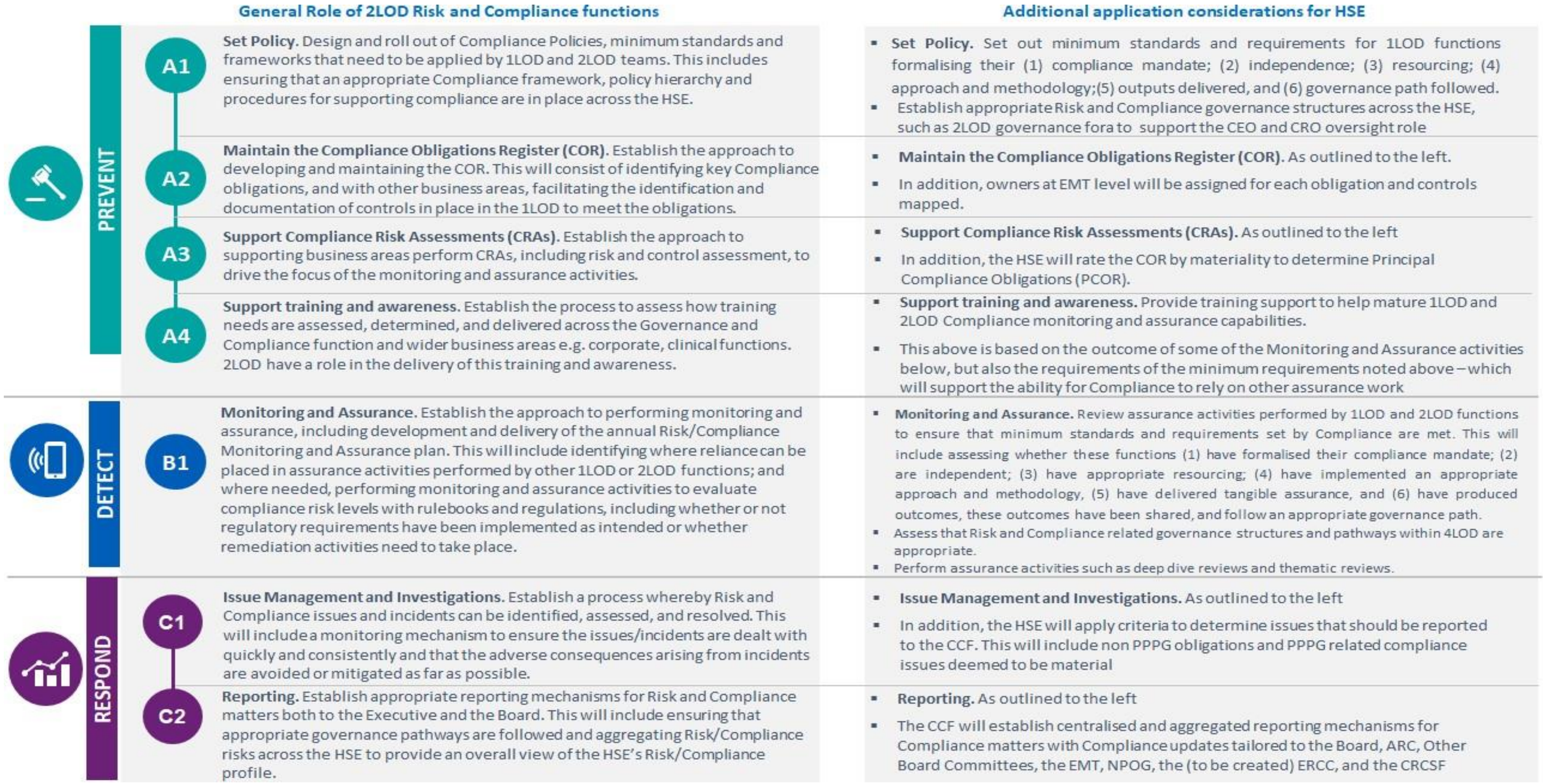
- Performed a desktop review of Compliance documentation (see **Appendix H** for details), including but not limited to Compliance governance fora, frameworks, and policies;
- Conducted stakeholder interviews (see **Appendix B** for details) and assessed the Compliance processes against KPMG's views of good practice; and,
- Applied our Control Function Operating Model methodology across the six lenses outlined below to (i) Identify and map core CCF management processes to determine current ("As Is") Operating Model); (ii) Design a high-level Future state ("To Be") Operating Model for the CCF and management processes; and (iii) Identify improvement opportunities and draft recommendations.

Additional details relative to the approach followed are outlined in **Appendix A**.

3. Good Practice Considerations

Good practices from Risk and Compliance Functions of comparable organisations were considered and factored in to design the Future State of the HSE's Central Compliance Function. Details are outlined below.

Figure 3. General Role of 2LOD Risk and Compliance Functions and Applicability to the HSE.



		General Role of 2LOD Risk and Compliance functions	Additional application considerations for HSE
PREVENT	A1	**Set Policy.** Design and roll out of Compliance Policies, minimum standards and frameworks that need to be applied by 1LOD and 2LOD teams. This includes ensuring that an appropriate Compliance framework, policy hierarchy and procedures for supporting compliance are in place across the HSE.	▪ **Set Policy.** Set out minimum standards and requirements for 1LOD functions formalising their (1) compliance mandate; (2) independence; (3) resourcing; (4) approach and methodology;(5) outputs delivered, and (6) governance path followed. ▪ Establish appropriate Risk and Compliance governance structures across the HSE, such as 2LOD governance fora to support the CEO and CRO oversight role
	A2	**Maintain the Compliance Obligations Register (COR).** Establish the approach to developing and maintaining the COR. This will consist of identifying key Compliance obligations, and with other business areas, facilitating the identification and documentation of controls in place in the 1LOD to meet the obligations.	▪ **Maintain the Compliance Obligations Register (COR).** As outlined to the left. ▪ In addition, owners at EMT level will be assigned for each obligation and controls mapped.
	A3	**Support Compliance Risk Assessments (CRAs).** Establish the approach to supporting business areas perform CRAs, including risk and control assessment, to drive the focus of the monitoring and assurance activities.	▪ **Support Compliance Risk Assessments (CRAs).** As outlined to the left ▪ In addition, the HSE will rate the COR by materiality to determine Principal Compliance Obligations (PCOR).
	A4	**Support training and awareness.** Establish the process to assess how training needs are assessed, determined, and delivered across the Governance and Compliance function and wider business areas e.g. corporate, clinical functions. 2LOD have a role in the delivery of this training and awareness.	▪ **Support training and awareness.** Provide training support to help mature 1LOD and 2LOD Compliance monitoring and assurance capabilities. ▪ This above is based on the outcome of some of the Monitoring and Assurance activities below, but also the requirements of the minimum requirements noted above – which will support the ability for Compliance to rely on other assurance work
DETECT	B1	**Monitoring and Assurance.** Establish the approach to performing monitoring and assurance, including development and delivery of the annual Risk/Compliance Monitoring and Assurance plan. This will include identifying where reliance can be placed in assurance activities performed by other 1LOD or 2LOD functions; and where needed, performing monitoring and assurance activities to evaluate compliance risk levels with rulebooks and regulations, including whether or not regulatory requirements have been implemented as intended or whether remediation activities need to take place.	▪ **Monitoring and Assurance.** Review assurance activities performed by 1LOD and 2LOD functions to ensure that minimum standards and requirements set by Compliance are met. This will include assessing whether these functions (1) have formalised their compliance mandate; (2) are independent; (3) have appropriate resourcing; (4) have implemented an appropriate approach and methodology, (5) have delivered tangible assurance, and (6) have produced outcomes, these outcomes have been shared, and follow an appropriate governance path. ▪ Assess that Risk and Compliance related governance structures and pathways within 4LOD are appropriate. ▪ Perform assurance activities such as deep dive reviews and thematic reviews.
RESPOND	C1	**Issue Management and Investigations.** Establish a process whereby Risk and Compliance issues and incidents can be identified, assessed, and resolved. This will include a monitoring mechanism to ensure the issues/incidents are dealt with quickly and consistently and that the adverse consequences arising from incidents are avoided or mitigated as far as possible.	▪ **Issue Management and Investigations.** As outlined to the left ▪ In addition, the HSE will apply criteria to determine issues that should be reported to the CCF. This will include non PPPG obligations and PPPG related compliance issues deemed to be material
	C2	**Reporting.** Establish appropriate reporting mechanisms for Risk and Compliance matters both to the Executive and the Board. This will include ensuring that appropriate governance pathways are followed and aggregating Risk/Compliance risks across the HSE to provide an overall view of the HSE's Risk/Compliance profile.	▪ **Reporting.** As outlined to the left ▪ The CCF will establish centralised and aggregated reporting mechanisms for Compliance matters with Compliance updates tailored to the Board, ARC, Other Board Committees, the EMT, NPOG, the (to be created) ERCC, and the CRCSF

4. Current State ('As Is') Overview

4.1 Governance and Mandate

4.1.1. Board and Committees

The HSE Board (the 'Board') is required to satisfy itself that appropriate systems, procedures, and practices are in place, including for Compliance Risk Management[4]. As such, the HSE Board has ultimate responsibility for the governance of all risk-taking activity in the HSE including Compliance Risk. The Board's oversight of Risks, including Compliance Risk matters, is mainly supported by the Audit and Risk Committee (ARC), to which it delegates a number of risk and compliance related responsibilities. The ARC works in coordination with other Board Committees to oversee Risk and Compliance matters.

4.1.2. EMT and Compliance related 1LOD and 2LOD Governance

The 1LOD is responsible for owning and managing Compliance Risks across the HSE. The HSE Chief Executive Officer (CEO) is ultimately accountable for managing Compliance Risk and is advised and supported on the management of Compliance Risk matters by the Executive Management Team[5] (EMT) and by the National Performance Oversight Group (NPOG). These fora are supported by a range of executive meetings such as Hospital Groups (HGs) and Community Health Operations (CHOs) service meetings and other functional meetings which escalate issues (as needed) to the EMT and NPOG as appropriate.

From a 2LOD perspective, the CEO is advised on Risk matters by the CRO supported by the Corporate Risk Register Support Team (CRST) which is a forum chaired by the Chief Risk Officer (CRO). The CRST is a senior cross-functional support team mandated by the EMT to support and co-ordinate the identification, assessment, mitigation and reporting of corporate risks. The remit of the CRST does not include Compliance Risks.

4.1.3. CRO standing and reporting to the Board, ARC and other Board and 1LOD Committees

The CRO reports into the Chief Strategy Officer (CSO). The CRO attends monthly ARC meetings, and also attends Board meetings as needed. Compliance related reporting may take place as part of broader updates provided by the relevant EMT member and at times by the CRO via the Corporate Risk Register (CRR) Report (see additional details in **Section 4.5 – People and Skills**). The CRO is a member of NPOG and attends specific parts of EMT meetings.

4.1.4 Compliance Mandate, Framework and Risk Appetite

The Framework to manage Compliance across the HSE has been recently documented (as part of this review) and is in draft form pending approval by the ARC and the EMT. This Compliance Framework outlines specific compliance related duties for each of the above governance fora.

In addition, we note that the HSE Risk Appetite Statement 2021 / 2022 includes coverage of 12 risk areas and outlines tolerances and target risk appetite levels. However, this does not currently include Compliance Risk though we understand this is being considered as part of the review of the Risk Appetite Statement.

[4] As defined in section 3.5 of the 2021 HSE Governance Code.

[5] According to section 3.16 of the HSE Code of Governance the EMT comprises such members as may be nominated by the Chief Executive Officer from time to time

4.2 Organisation and Location

A formal Three Lines of Defence (3LOD) model including defined roles and responsibilities has been recently documented in the drat Compliance Framework. Notwithstanding this, the way in which the HSE currently manages Compliance, can be described by applying 3LOD concepts in accordance with the features outlined below.

4.2.1 First Line of Defence (1LOD)

The Executive Management Team (EMT), led by the CEO is responsible for executive decision making in the HSE. EMT members, as key senior members of 1LOD functions, are responsible for ensuring compliance with applicable HSE obligations as part of the delivery of HSE activities and strategies. As part of this, the HSE follows a decentralised model whereby multiple 1LOD functions perform compliance related monitoring and assurance activities, which we note require maturing. For example, Finance has a leading role in the System of Internal Control (SIC) process, and Procurement performs monitoring activities relative to contract compliance.

4.2.2 Second Line of Defence (2LOD)

The CRO supports the oversight of Compliance Risks across the HSE. The Central Compliance Function (CCF) under the CRO's remit is under development. This Function is currently made up of the former Health and Business Service (HBS) Standards and Compliance team, which is responsible for monitoring compliance and supporting compliance for HBS Functions. The HBS Standards and Compliance team is the only 2LOD team that performs compliance related activities and has 8 staff composed as follows: the Head of the function, 4 WTEs dedicated to Protected Disclosures; 2 WTEs that provide administrative support; and 1 WTE that performs Compliance related activities. This means that only 1 WTE and the Head of the Function support compliance for shared services functions in the HSE such as Procurement and Human Resources. Specifically, this small sub-team seeks to assure management, stakeholders and customers that operations are performed in compliance with legislation, regulations, standards, government policies and proven methodologies.

4.2.3. Third Line of Defence (3LOD)

The Internal Audit Function is responsible for providing assurance on the adequacy of the HSE's internal control, risk management, compliance and governance systems and activities, and to bring deficiencies therein to the notice of management, the HSE EMT, the Board, ARC and Board committees.

As part of the duties outlined above and based on the results of the individual internal audit engagements, the Head of Internal Audit concluded in 2019 that ''Limited Assurance'' can be provided in respect of the governance, risk management, and internal control processes within the HSE. This opinion still stands today.

4.3 Activities and Processes

PREVENT

4.3.1. Minimum requirements for 1LOD functions performing compliance related monitoring and assurance activities

As noted in **Section 4.2**, there are multiple 1LOD functions that perform compliance related monitoring and assurance activities across the HSE. To date, these functions were not required to follow or up-hold minimum requirements or expectations in delivering these activities. Minimum requirements for 1LOD functions performing compliance related monitoring and assurance activities have been defined in the draft Compliance Framework across the following lenses: (1) Formality of Mandate; (2) Independence; (3) Adequacy of resourcing; (4) Formality of approach and methodology; (5) Formality of output; and (6) Adequacy of the Governance path followed.

Given the Compliance Framework has been recently developed as part of this review, the minimum requirements relative to the above six lenses have not been rolled out or applied to date.

4.3.2. Set Policy

A draft Compliance Framework has been developed as part of this review and is pending approval by the ARC and EMT. The new Compliance Framework sets out the: (1) Regulatory context in which the HSE manages Compliance Risks; (2) Governance arrangements in place to manage Compliance Risks; (3) Roles and Responsibilities across the Three Lines of Defence (3LOD) in relation to the management of Compliance Risks; (4) Key prevention activities and processes performed to manage Compliance Risks; (5) Monitoring and assurance activities relative to managing Compliance Risks; and (6) Reporting of Compliance Risks. See **Appendix D** for details.

The Compliance Framework references a suite of supporting Compliance Policies, tools and methods which have not been developed.

4.3.3. Compliance Obligations Register

The design of the Compliance Obligation Register (COR) has been developed and the output was agreed by the HSE Steering Group (see **Appendix C** for details). The initial set of Compliance Obligations have been identified by the HSE and included in the COR. This listing is in draft form and is being refined. Subsequently, it will be validated by EMT members.

4.3.4. Compliance Risk Assessments (CRAs)

A set of criteria to classify obligations by materiality has been recently defined as part of the development of the draft Compliance Framework. As at the date of this report, Compliance Obligations have not been risk assessed or classified by materiality.

4.3.5. Training and awareness

Compliance specific training is made up of statutory training. For example, health and safety related training provided to HSE employees when starting employment. We also noted evidence of specific compliance related training in relation to monitoring and assuring activities performed by 1LOD functions. For example, a Controls Assurance Review Process (CARP) training was delivered by the Finance team in November 2021. However, a HSE organisation wide Compliance related training plan has not been developed or delivered.

DETECT

4.3.6. Monitoring and Assurance process

Examples of 1LOD functions that perform compliance related monitoring and assurance activities include: Finance has a leading role in the System of Internal Control (SIC) process; Procurement performs some monitoring activities relative to contract compliance; The Compliance Unit for Funded Agencies performs a level of monitoring and assurance of s.38 and s.39 agencies; the Quality and Patient Safety Function has a key role in commissioning audits by the National Office for Clinical Audit (NOCA); the Human Resources function provides oversight in relation to staff payments; and the Capital & Estates function performs monitoring and assurance activities relative to the adequacy and compliance of HSE sites (premises) in relation to aspects such as fire, health and safety.

A detailed overview of the compliance related monitoring and assurance activities performed by 1LOD functions has been documented in the HSE 4LOD Integrated Assurance Map (see **Appendix G** for details). The effectiveness and quality of the monitoring and assurance activities being performed by those 1LOD functions was not part of the scope of this review. However, based on interviews, we note that the maturity of those activities for the most part is relatively immature. In addition, we also note that a risk based HSE wide Compliance Monitoring Plan is not in place.

RESPOND

4.3.7. Issues Management and Investigation

The management, remediation and reporting of compliance related issues is currently addressed by the respective 1LOD function responsible for the issue. In doing so, teams use internal sources of information such a national data repository and reporting database maintained by Finance (which is currently under development) to log and manage compliance related issues.

4.3.8. Compliance Reporting

The CRO reports on the HSE's top corporate risks on a quarterly basis to the EMT, the ARC and to the Board (as needed) via the Corporate Risk Register Report (CRR). The CRO may also provide ad-hoc compliance related updates. Other compliance related reporting takes place across 1LOD functions performing compliance related monitoring and assurance activities. For example, the Compliance Unit for Funded Agencies reports on the outcomes of the reviews performed by an external professional services firm; and the Finance Function reports on the SIC process. Centralised consolidated compliance related reporting is not in place.

4.4 Technology and Data

Compliance related information in 1LOD functions is largely managed in manual form through spreadsheets and audit type reports such as the funded agencies related reviews performed on s.38 and s.39 agencies. Some bespoke systems are also used such as those that support the aggregation and reporting of performance data to NPOG meetings. We also note that improvements are underway. For example, the national data repository and reporting database being developed by the Finance function, and the Quality and Patient Safety (QPS) surveillance function which is under development and that in the future will seek to centralise under one system all the QPS related data, e.g. complaints, NOCA audits, incidents, and balance scorecard metrics.

4.5 People and Skills

4.5.1 2LOD Compliance Resources

As outlined in **Section 4.2.2**, the HBS Standards and Compliance function has a total Whole Time Equivalent (WTE) resources of 8 staff. The HBS and other functions is currently led by an Assistant National Director of Governance and Compliance, until a head for the new CCF is recruited and appointed. The HBS Standards and Compliance team is the only 2LOD team that performs compliance related activities and the 8 staff are allocated as follows: the Head of the function, 4 WTEs dedicated to Protected Disclosures; 2 WTEs that provide administrative support; and 1 WTE that performs Compliance related activities. **This means that only 1 WTE and the Head of the function support compliance for shared services functions in the HSE such as Procurement and Human Resources.**

We also note that a skills assessment has not been performed.

4.5.2 1LOD Compliance Resources

From 1 LOD perspective, it was not within the scope of this review to determine the resources allocated to compliance related monitoring and assurance activities performed by 1LOD functions. However, these functions and the activities they perform have been identified through the work carried out to develop the HSE 4LOD Integrated Assurance Map. Also, through interviews, we have identified total Whole Time Equivalent (WTE) resource allocation for the following 1LOD functions that perform compliance related monitoring and assurance activities:

- Finance Specialist Compliance team: 8 WTEs;
- Compliance Unit for Funded Agencies (Section 38 and Section 39 providers): 11 WTEs;
- HR Pay Compliance Unit: 8 WTEs;
- Children Hospital Assurance Programme: 1 WTE;
- Project Management Improvement Unit (PMIU):14 WTEs;
- Probity team in Operations (Schemes & Reimbursement): 60 WTEs; and
- Corporate Procurement Planning and Compliance Improvement: 30 WTEs.

A skills assessment for the above functions has not been performed.

4.6 Performance Management

There are four Compliance related KPIs outlined in the National Scorecard and reported on through the monthly Performance Profile which is then considered by NPOG and the EMT. These are:

- Governance and Compliance: (i) Procurement – expenditure (non-pay) under management; and (ii) % of internal audit recommendations implemented, against total no. of recommendations, within 12 months of report being received;
- Disability Act Compliance: % of assessments completed within the timelines as provided for in the regulations; and,
- HIQA Inspection Compliance: % compliance with regulations following HIQA inspection of disability residential services.

5. Detailed Findings and Recommendations

5.1. Summary observations and recommendations

Based on the above, we noted several key opportunities that will assist the HSE significantly increase the effectiveness of Compliance Management processes and set the recently created Central Compliance Function (CCF) up for success. We have identified 15 improvement opportunities and 46 associated recommendations. These are summarised below

■ **Low** = Area to consider for minor improvement ■ **Medium** = Area for attention ■ **High** = Area for priority focus

Observation Title	REF	Recommendations	Priority
A. Governance and Mandate			
A1. Establish a strong Central Compliance Function (CCF)	**A1.1**	Establish a Central Compliance Function (CCF) with appropriate resources (see recommendations relative to observations B1, B2, and E1 for structure and resourcing considerations of the CCF);	**High**
	A1.2	Establish an EMT led Executive Risk and Compliance Committee (ERCC) to support risk oversight including Compliance Risk	
	A1.3	CRO to provide stand-alone Compliance reports to the Board at least twice a year	
	A1.4	CRO to provide stand-alone Compliance reports to the ARC, Other Board Committees (as relevant) and to the EMT on a quarterly basis	
	A1.5	CRO to either be a formal member of the EMT or attend the duration of EMT the meetings	
	A1.6	CCF to have a formal review and challenge role at key strategic and operational change fora	
	A1.7	Expand the remit of the CRST or establish an equivalent forum to support Compliance activity and risk oversight	
	A1.8.	Re-assess appropriateness of CRO reporting line as Risk and Compliance functions mature	
A2. Implement the Compliance Mandate, Compliance Framework, and Compliance Risk Appetite	**A2.1**	Approve the draft Compliance Framework (which also includes the Compliance mandate) and communicate the Framework across the HSE to help set guidance and expectations across the organisation	**High**
	A2.2	Develop a Compliance Risk Appetite Statement for the HSE including measures, tolerances, and limits	
	A2.3	Expand Board level Risk Appetite reporting to include Compliance Risk profile vs appetite	
B. Organisation and Location			
B1. Determine the structure of the CCF	**B1.1**	Identify key duties to be delivered by the CCF as outlined in the Compliance Framework and perform gap analysis against the current set of activities being delivered and implement required changes	**High**

Observation Title	REF	Recommendations	Priority
	B1.2	Determine the staffing requirements and structures for the CCF to support the delivery of the Compliance Framework	
B2. Implement a relationship management framework	B2.1	Appoint a Compliance Business Partner within the CCF for each 1LOD functions, that manages the interaction with the 1LOD on compliance matters and the 1LOD compliance related monitoring activities	Medium
	B2.2	Appoint a Single Point of Contacts (SPOC)) within each 1LOD function for the CCF to interact with on compliance matters	
	B2.3	Set up a schedule of regular relationship management meetings between the 1LOD functions and the CCF. Feedback and insights from these meetings should be centrally collated and disseminated	
	B2.4	Update the Compliance Framework to reflect the new stakeholder Relationship Management Model	
	B2.5	Deliver consultation and communications programme on the Framework and new Relationship Management Model	
C – Activities and Processes			
CA. Prevention			
CA1. Develop and communicate 1LOD Maturity Assessment Model	CA1.1	Implement 1LOD Maturity Assessment Model (including maturity scale definitions)	High
	CA1.2	Provide training to all 1LOD Functions that perform compliance related monitoring and assurance activities to set expectations and support their maturity and adherence to the minimum requirements	
CA2. Develop suite of supporting Compliance Policies, tools, and methods to support the implementation of the Framework	CA2.1	Develop (at a minimum) 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	High
	CA2.2.	Develop artefacts (tools and methods) to support each of the above policies. Refer to the Compliance Framework for a listing of minimum artefacts to be in place	
CA3. Finalise the Compliance Obligations	CA3.1	Validate the listing of HSE applicable obligations	High
	CA3.2	Assign owners to each obligation and map based on materiality each obligation to policies, standards, and operational controls	
	CA3.3	Perform a risk assessment of the COR and classify each obligation by materiality	
Register (COR) and complete risk assessment	CA3.4	Implement reporting of Principal Obligations (PCOR) to the EMT and ARC	High
	CA3.5	Complete compliance risk attestations via Annual Compliance Statements on an annual basis	

Observation Title	REF	Recommendations	Priority
CA4. Develop and deliver Compliance training plan	**CA4.1**	Assess training needs across 1LOD and 2LOD functions. The HSE should consider developing a compliance specific skills matrix to support this	Low
	CA4.2	Develop and deliver a Compliance training plan for 1LOD and 2LOD functions	
CB. Detection			
CB1. Assess maturity of 1LOD Functions performing compliance related monitoring and assurance activities	**CB1.1**	Assess the maturity of 1LOD functions that perform compliance related risk monitoring and assurance activities and determine: (i) where reliance can be placed on the monitoring and assurance activities performed by 1LOD functions; and (ii) where support is needed to mature the activities performed by 1LOD functions that perform compliance related risk monitoring and assurance activities (i.e., those activities deemed not sufficiently mature)	High
	CB1.2	Support the development of the activities performed by 1LOD deemed less mature (this may include training support)	
	CB1.3	Determine monitoring and activities that should be performed by the CCF	
	CB1.4	Report the outcomes of these 1LOD maturity assessments to the relevant governance fora, identifying actions to mature these functions and thematic issues	
CB2. Develop and implement a risk-based Compliance Monitoring Plan	**CB2.1**	Develop and implement a risk-based Compliance Monitoring Plan for the HSE approved by the ARC	High
	CB2.2	Expand Compliance reporting to include progress against the Compliance Monitoring Plan	
	CB2.3	Develop a 3LOD Integrated Assurance Plan (based on coverage and effectiveness)	
CC – Respond			
CC1. Establish a centralised issues management process to identify, manage and report on compliance issues	**CC1.1**	Develop an Issues Management Policy and Issues Log (as per recommendation **REF CA2.1**. and **CA2.2)**	High
	CC1.2	Apply criteria to determine issues that should be reported to the CCF. This may be calibrated to include external obligations (non PPPG obligations) and PPPG related compliance issues deemed to be material	
	CC1.3	Implement central compliance issues log to record compliance issues deemed to be material, and implement monitoring and reporting of these issues.	
CC2. Establish centralised and aggregated reporting	**CC2.1**	Establish centralised and aggregated reporting mechanisms for Compliance matters with Compliance updates tailored to the Board, ARC, Other Board Committees, the EMT, NPOG, the (to be created) ERCC, and the CRCSF in accordance with the guidance and frequency set out in the Compliance Framework.	High

Observation Title	REF	Recommendations	Priority
D – Technology and Data			
D1. Consider implementing an eGRC solution	**D1.1**	Consider implementing eGRC system 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	**Medium**
E – People and Skills			
E1. Determine the CCF and 1LOD Compliance related staffing levels and skills	**E1.1**	Appoint a dedicated Head of Compliance (at Assistant National Director level) to lead the compliance activities under the CCF reporting to the CRO	**High**
	E1.2	Determine and source resources to assist with the implementation of the recommendations of this report and the new Compliance Operating Model	
	E1.3	Perform a forward-looking skills and capacity analysis to determine the headcount and skillset needed to fulfil the mandate of the CCF	
	E1.4	Perform forward-looking skills and capacity analysis to determine the headcount and skillset needed across each 1LOD function performing compliance related monitoring and assurance to deliver on their individual mandate	
F – Performance Management			
F1. Develop and Implement Compliance Performance Indicators	**F1.1**	Develop Compliance Performance Indicators in accordance with key aspects of the Compliance Framework	**Medium**
	F1.2	Assess Compliance related KPIs currently included in the National Scorecard and determine if these need to be updated based on the outcomes of the action above	

5.2. Detailed observations and recommendations

Details for each of the 15 improvement opportunities and 46 associated recommendations are outlined below. Also, refer to Section 6 for additional details relating to all aspects of the proposed operating model.

■ **Low** = Area to consider for minor improvement ■ **Medium** = Area for attention ■ **High** = Area for priority focus

Observation	Recommendation
A. Governance and Mandate	
Ref | **A1** | **Establish a strong Central Compliance Function (CCF)**	**Priority** | **High**
As mentioned at the start of this report, a Central Compliance Function is under development and its design is the subject of this report. Also, as outlined in Section 4.1 **– Governance and Mandate,** the CRO, has responsibility for Compliance and reports to the CSO. The main fora attended by the CRO are the Board, the ARC, EMT meetings and NPOG. The CRO also Chairs the CRST. Specific compliance related duties for each of these governance fora have been outlined in the draft Compliance Framework. Based on interviews, documentation review and comparison against good practices, in our view, a CCF should be established and the profile of the CRO relative to the coverage of Compliance risks should be enhanced on: (1) the Board, the ARC and other Board Committees; (2) the EMT; (3) the CRST; and (4) Strategic and Change Fora. **See Section 6.1** for details of the proposed 'To Be' state and proposed changes. Specifically, we note the following: **Central Compliance Function (CCF)** ▪ A CCF is not in place. The establishment of a well-resourced CCF with an appropriate organisational mandate, profile and standing is needed to increase effectiveness of compliance activities. **CRO attendance and reporting at the Board, ARC and Other Board Committees** ▪ **Board and Other Board Committees (excluding the ARC)**. The CRO attends the Board and Other Board Committee meetings and provides ad-hoc compliance related updates when needed (for example, in case of an incident). This means that Compliance related updates are not provided to the Board or Other Board Committees at an agreed frequency, and that these updates do not follow a standard and dedicated compliance specific reporting format. As a result, visibility over Compliance matters at the Board and Other Committees may be limited. ▪ **ARC**. The CRO attends every ARC meeting. Risk Management updates are provided by the CRO via the Corporate Risk Register (CRR) Report, and these may at times include compliance related elements (see additional details in **Section 4.5 – Reporting**). However, dedicated reporting or standing agenda items dedicated to compliance matters are not in place.	We recommend the following: **A1.1**. Establish a Central Compliance Function (CCF) with appropriate resources (see recommendations relative to observations A2, B1, B2, and E1 for mandate, structure and resourcing considerations of the CCF); **A1.2**. CRO to provide stand-alone Compliance reports to the Board at least twice a year; **A1.3**. CRO to provide stand-alone Compliance reports to the ARC, Other Board Committees (as relevant) and to the EMT on a quarterly basis; **A1.4**. CRO to either be a formal member of the EMT or attend the duration of EMT the meetings; **A1.5**. CCF to have a formal review and challenge role at key strategic, regulatory and operational change fora; **A1.6.** Expand the remit of the CRST or establish an equivalent forum to support Compliance activity and risk oversight; **A1.7**. Establish an EMT led Executive Risk and Compliance Committee (ERCC) to support risk oversight including Compliance Risk; and

Observation	Recommendation
This format limits the visibility and airtime in which Compliance updates can be discussed and overseen at the ARC. **CRO attendance and reporting at EMT Meetings** - The CRO attends EMT meetings on at least a quarterly basis. Similar to the ARC, Compliance related updates may at times take place as part of broader Risk Management updates provided by the CRO via the CRR Report. This means that dedicated reporting or a standing agenda item dedicated to compliance matters are not in place. This format limits the visibility and airtime in which Compliance updates can be discussed and overseen at the EMT. - In addition, we note that the CRO is not a member of the EMT and attends specific parts of EMT meetings as opposed to their entire duration. The CRO should either be a member of the EMT or (at a minimum) attend for the duration of the meetings. **Compliance related 2LOD Committees / Working Groups** - From a 2LOD perspective, the CEO is advised on Risk matters by the CRO supported by the CRST. However, the remit of the CRST does not include Compliance Risks. - In addition, we note that the CRST is a cross-functional group led by one or two levels below EMT level. This means that the HSE do not have an EMT led Executive Committee to support the CEO in relation to the oversight of Risk and Compliance matters. This is a normal practice at comparable organisations and would help uplift the coverage, prominence, and visibility of Compliance matters at an Executive level. **Voice of Compliance at Strategic and Change Fora** - Based on interviews (including with the Chair of the ARC), we note that 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. Therefore, there is no voice of Compliance or documented Compliance opinion to highlight potential compliance or regulatory risks in relation to organisational or strategic change. **Compliance reporting line** - The CRO with responsibility for Compliance is currently at National Director level, which apart from the CEO and Chief Officers who are direct reports to the CEO (such as the CSO or CFO), is the most senior level in HSE. Whilst good practice would indicate a direct reporting line (for CRO) to the CEO, with the appropriate mandate, profile, attendance at EMT and direct reporting mechanisms to Board and ARC, the current reporting line of the CRO can be considered appropriate. This should be reassessed as both the Risk and Compliance functions mature.	**A1.8.** Re-assess appropriateness of CRO reporting line as Risk and Compliance functions mature. Specific recommendations and details relative to the content of compliance updates are outlined in **Ref CC2 – Establish centralised and aggregated reporting.**

Observation			Recommendation	
Ref	**A2**	**Implement the Compliance Mandate, Compliance Framework, and Compliance Risk Appetite**	**Priority**	**High**
▪ A Compliance Framework that sets out the Compliance mandate and principles and processes for the HSE to manage compliance across the organisation was not in place until recently. We note that the Compliance Framework (which also includes the Compliance mandate) was developed and documented as part of this engagement. The Compliance Framework is in draft form and needs to be approved by the EMT and ARC. ▪ In addition, based on documentation reviewed we note that the HSE Risk Appetite Statement 2021 / 2022 includes coverage of 12 risk areas and outlines tolerances and target risk appetite levels. However, the Risk Appetite Statement does not currently include Compliance Risk measures, tolerances, or limits. We note that this is being considered for inclusion in the next iteration of the Risk appetite statement.			We recommend the following: **A2.1**. Approve the draft Compliance Framework (which also includes the Compliance mandate) and communicate the Framework across the HSE to help set guidance and expectations across the organisation; **A2.2**. Develop a Compliance Risk Appetite Statement for the HSE including measures, tolerances, and limits; and, **A2.3**. Expand Board level Risk Appetite reporting to include Compliance Risk profile vs appetite.	
B. Organisation and Location				
Ref	**B1**	**Determine the structure of the CCF**	**Priority**	**High**
▪ As outlined in Section 4.2 **– Organisation and Location**, currently, the CCF is under development. This Function is currently made up of the HBS Standards and Compliance team and has 8 WTEs, though only 1 WTE is dedicated to compliance related activities (in addition to the Head of the function). The current structure has not been reviewed in light of the recently developed Compliance Framework. As a result, the duties outlined in the draft Compliance Framework have not been allocated to members of the team. ▪ The HBS Standards and Compliance team performs a degree of 2LOD compliance related activities. However, these activities are limited to supporting shared services functions and are not fully aligned to the duties and requirements outlined in the draft Compliance Framework. As such, the functional structure of the CCF needs to be determined. See Section 6.2 for proposed details relating the CCF functional and indicative initial resourcing structure.			We recommend the following: **B1.1** Identify key duties to be delivered by the CCF as outlined in the Compliance Framework and perform gap analysis against the current set of activities being delivered and implement required changes; and, **B1.2** Determine the staffing requirements and structures for the CCF to support the delivery of the Compliance Framework.	
Ref	**B2**	**Implement a relationship management framework**	**Priority**	**Medium**
The draft Compliance Framework defines a formal 3LOD model for the HSE to manage Compliance activities and risks. As part of this, the Framework sets Compliance related requirements and expectations across teams under each of the HSE's 3LOD including specific roles and responsibilities. However, until the Framework is approved and implemented, a Compliance Risk Relationship Management model cannot be determined. As a result, there is no documented Compliance Risk Relationship Management			Once the Compliance Framework is approved, we recommend the following: **B2.1** Appoint a Compliance Business Partner within the CCF for each 1LOD function, that manages the interaction with the 1LOD on compliance matters and	

Observation			Recommendation	
model or framework in place to establish the mechanism for interaction between the CCF and 1LOD functions. For example, Single Points of Contact (SPOC) for the CCF to engage with the various 1LOD functions that perform compliance related monitoring and assurance activities.			the 1LOD compliance related monitoring activities; **B2.2** Appoint a Compliance Relationship Partner (Single Point of Contact (SPOC)) within each 1LOD function for the CCF to interact with on compliance matters; **B2.3.** Set up a schedule of regular relationship management meetings between the 1LOD functions and the CCF. Feedback and insights from these meetings should be centrally collated and disseminated; **B2.4.** Update the Compliance Framework to reflect the new stakeholder Relationship Management Model; and, **B2.5.** Develop and deliver communications programme on the Framework and new Relationship Management Model.	
C. Activities and Processes				
CA. PREVENT				
Ref	**CA1**	**Develop and communicate 1LOD Maturity Assessment Model**	**Priority**	High
As outlined in Section 4.3 **– Activities and Processes,** minimum requirements for 1LOD functions performing compliance related monitoring and assurance activities have been defined in the draft Compliance Framework across the following lenses: (1) Formality of Mandate; (2) Independence; (3) Adequacy of resourcing; (4) Formality of approach and methodology; (5) Formality of output; and (6) Adequacy of the Governance path followed. In addition, as part of this review, a maturity assessment model has been developed to support the assessment of these minimum requirements. However, templates and artefacts to support the implementation of the assessment need to be developed. In addition, guidance and training support has not been provided to those 1LOD functions that perform compliance related monitoring and assurance activities.			We recommend the following: **CA1.1**. Implement a 1LOD Maturity Assessment Model (including maturity scale definitions); and **CA1.2**. Provide training to all 1LOD Functions that perform compliance related monitoring and assurance activities to set expectations and support their maturity and adherence to the minimum requirements. **Note:** 1LOD Functions that perform compliance related monitoring and assurance activities have been identified in the 4LOD Integrated Assurance Map (**see** Appendix G).	

Observation			Recommendation	
Ref	**CA2**	**Develop suite of supporting Compliance Policies, tools, and methods to support the implementation of the Framework**	**Priority**	High
The draft Compliance Framework references a suite of supporting Compliance Policies, tools, and methods. We note that these need to be developed and include: ▪ **Compliance Policies and Standards** to support the Framework by providing detailed guidance including step by step processes to manage different Compliance Risk Management activities such as: Compliance Risk Assessments; Compliance Issue Management; Compliance Monitoring and Assurance (CMA); and Compliance training and communication; and ▪ **Artefacts (Tools and Methods)** to support the operationalisation of Compliance Policies and Standards via artefacts that can be used to implement Compliance Risk Management activities. For example: The Compliance Obligations Register; the Compliance Monitoring Plan among other artefacts.			We recommend the following: **CA2.1**. Develop (at a minimum) 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; and, **CA2.2.** Develop artefacts (tools and methods) to support each of the above policies. Refer to the Compliance Framework for a listing of minimum artefacts to be in place.	
Ref	**CA3**	**Finalise the Compliance Obligations Register (COR) and complete risk assessment**	**Priority**	**High**
As outlined in **Section 4.3.3**. **– Compliance Obligations Register (COR)**, the HSE COR has been populated with a preliminary listing of obligations. We note that the listing is not final and is undergoing iterations with members of the EMT. We also note that owners have not been assigned to each obligation and controls have not been mapped. In addition, we note that until the COR is completed and validated by the EMT, obligations cannot be risk assessed or classified by materiality to identify Principal Obligations to be reported to the ARC and to support the development of the Compliance Monitoring Plan. We also note that compliance assurance of applicable obligations (for example through attestations) is not currently provided.			We recommend the following: **CA3.1**. Validate the listing of HSE applicable obligations; **CA3.2**. Assign owners to each obligation and based on materiality map obligations to policies, standards, and operational controls; **CA3.3.** Perform a risk assessment of the COR and classify each obligation by materiality; **CA3.4**. Implement reporting of Principal Obligations (PCOR) to the EMT and ARC; and, **CA3.5**. Complete compliance risk attestations via Annual Compliance Statements on an annual basis.	
Ref	**CA4**	**Develop and deliver Compliance training plan**	**Priority**	**Low**
Compliance specific training is largely consistent of statutory training (for example, health and safety related training provided to HSE employees) and specific training provided by 1LOD functions that perform compliance related monitoring and assuring activities (such as the Controls Assurance Review Process (CARP) training provided by Finance). However, an HSE organisation wide Compliance training plan is not in place. We also note			We recommend the following: **CA4.1**. Assess training needs across 1LOD and 2LOD functions. The HSE should consider developing a	

Observation	Recommendation
that a compliance specific skills assessment process is not in place.	compliance specific skills matrix to support this; and, **CA4.2**. Develop and deliver a Compliance training plan for 1LOD and 2LOD functions.
CB. DETECT	
Ref | **CB1** | **Assess maturity of 1LOD Functions performing compliance related monitoring and assurance activities**	**Priority** | **High**
As outlined in Section 4.3.5 – **Monitoring and Assurance**, a detailed overview of the compliance related monitoring and assurance activities performed by 1LOD functions has been documented in the HSE 4LOD Integrated Assurance Map. This includes details relative to reviews and Risk and Compliance related monitoring and assurance activities performed by Finance, the Compliance Unit for Funded Agencies, Procurement, HR, IT , Capital and Estates, and the Children's Hospital Assurance Programme. The extent of coverage of these activities across the HSE's key processes and functions is outlined in the 4LOD Integrated Assurance Map (see Appendix G) based on the self-assessment performed by key senior stakeholders from each area. However, based on interviews and documentation reviewed we note that: ▪ The effectiveness and quality of the monitoring and assurance activities being performed by those 1LOD functions is not fully known and is not documented. ▪ Most interviewees noted that the maturity of the compliance related monitoring and assurance activities performed by 1LOD functions are for the most part relatively immature and there is a need for these activities to be formally assessed against a set criteria. Once assessed, actions need to be developed to assist the maturing of these functions and to support aggregated reporting by the CCF to the EMT, ARC and Board.	We recommend that the CCF: **CB1.1**. Assess the maturity of 1LOD functions that perform compliance related risk monitoring and assurance activities and determine: (i) where reliance can be placed on the monitoring and assurance activities performed by 1LOD functions; and (ii) where support is needed to mature the activities performed by 1LOD functions that perform compliance related risk monitoring and assurance activities (i.e., those activities deemed not sufficiently mature); See Appendix F for an example related to the Compliance Unit for Funded Agencies to illustrate 'As Is' Operating Model vs 'To Be' Operating model, including key benefits. **CB1.2**. Support the development of the activities performed by 1LOD deemed less mature (this may include training support); **CB1.3**. Determine monitoring and activities that should be performed by the CCF; and, **CB1.4**. Report the outcomes of these 1LOD maturity assessments to the relevant governance fora, identifying actions to mature these functions and thematic issues.

Observation			Recommendation	
Ref	CB2	Develop and implement a risk-based Compliance Monitoring Plan	Priority	High
As noted in observation **Ref CA3 – Finalise the Compliance Obligations Register (COR) and complete risk assessment,** the HSE COR is not yet finalised and has not as yet been risk assessed or classified by materiality. In addition, as noted in **Ref CB1 – Assess maturity of 1LOD Functions performing compliance related monitoring and assurance activities**, the effectiveness of 1LOD functions performing compliance related monitoring activities was not fully assessed as part of this review and therefore it is unclear which activities (if any) the CCF can place reliance on. In addition to the above, we also note that key sources of information have not been assessed centrally to form a view of the most significant compliance risks to the HSE. For example: outcomes from previous monitoring and assurance reviews; compliance breaches; regulatory findings (C&AG, HIQA, MHC, other regulatory bodies); relevant complaint trends/findings/issues; emerging regulations; key initiatives/changes; Governance fora/ CRO requests; and Internal Audit/CRO planned assurance and monitoring. As a result of the above, we also note that a risk-based Compliance Monitoring plan is not in place.			We recommend the following: **CB2.1**. Develop and implement a risk-based Compliance Monitoring Plan for the HSE approved by the ARC; The Plan should be informed by a number of information sources which will include but not be limited to: CRAs (the risk assessment of the COR); outcomes from previous monitoring and assurance reviews; compliance breaches; reviews of 1LOD functions adherence to minimum compliance monitoring and assurance requirements; regulatory findings (C&AG, HIQA, MHC, other regulatory bodies); relevant complaint trends/findings/issues; emerging regulations; key initiatives/changes; Governance fora/ CRO requests; and, Internal Audit/CRO planned assurance and monitoring. **CB2.2**. Expand Compliance reporting to include progress against the Compliance Monitoring Plan; and, **CB2.3**. Develop and implement a 3LOD Integrated Assurance Plan (based on coverage and effectiveness).	
C-RESPOND				
Ref	CC1	Establish a centralised issues management process to identify, manage and report on compliance issues	Priority	High
As outlined in Section 4.3.7 **– Issues Management and Investigation**, currently compliance issues are managed in a decentralised manner whereby each 1LOD function manages, remediates and reports on each compliance related issue. Although a degree of consolidation is sought to be established via a Finance led initiative to implement an issues database, we note the following: ▪ There is no centralised process or policy in place to identify, record, classify, remediate, and report on compliance issues; ▪ Issues reported by 1LOD Functions do not follow a standard format, are not classified by materiality, and do not follow an agreed upon governance pathway; ▪ There is no formal reporting of compliance issues to the CCF. As a result, visibility of thematic issues and			We recommend the following: **CC1.1**. Develop an Issues Management Policy and Issues Log (as per recommendation **REF CA2.1**. and **CA2.2)**; **CC1.2**. Apply criteria to determine issues that should be reported to the CCF. This may be calibrated to include external obligations (non PPPG obligations) and PPPG related compliance issues deemed to be material; and,	

Observation	Recommendation
consolidated/aggregated reporting of material compliance issues is limited; and ▪ The Finance led data depository and reporting tool to support the analysis of key controls is part of a wider controls improvement initiative and is under development.	**CC1.3**. Implement central compliance issues log to record compliance issues deemed to be material, and implement monitoring and reporting of these issues. **Note**: In addressing the above, the HSE should seek to leverage the Finance led data depositary and reporting tool.
Ref **CC2** **Establish centralised and aggregated reporting**	**Priority** **High**
Ref A1 – Enhance the Profile of the Central Compliance Function (CCF), we commented on the reporting frequency and the types of updates to be provided by the CCF to key HSE governance fora. In this section, we will refer to the content of compliance related reporting to be provided by the CCF. As outlined in **Section 4.3.8 – Compliance Reporting,** the CRO reports on the HSE's top corporate risks to the EMT, the ARC and to the Board via the Corporate Risk Register Report (CRR). However, based on interviews and documentation reviewed we note the following: ▪ Compliance risk updates are covered within wider risk updates included in the CRR report, but these updates are dependent on the risk rating assigned for the period. For example, the CRR Report of Q4 2021 included Risk ID#16 – Regulatory Non-Compliance because this risk type was considered high, but the CRR of Q1 2022 did not include the reporting of any compliance risks. This means that stand-alone compliance reporting is not in place and that compliance related updates can be missing altogether for any given reporting period. This limits the ability of the Board, ARC, EMT, CEO and CRO to oversee compliance matters. ▪ Compliance related updates are also provided by different 1LOD functions performing compliance related monitoring and assurance activities such as Finance. This means that currently: centralised consolidated compliance related reporting is not in place; there are no clear or agreed upon governance paths for compliance related updates; and there is no aggregate compliance related reporting relative to the HSE compliance risk profile for any governance fora including the Board, ARC, Other Board Committees or EMT.	We recommend the following: **CC2.1**. Establish centralised and aggregated reporting mechanisms for Compliance matters with Compliance updates tailored to the Board, ARC, Other Board Committees, the EMT, NPOG, the (to be created) ERCC, and the CRCSF in accordance with the guidance and frequency set out in the Compliance Framework.
D – Technology and Data	
Ref **D1** **Consider implementing an eGRC solution**	**Priority** **Medium**
The HSE uses a degree of technology enabled solutions to manage specific compliance processes. For example (as noted in the previous observation) the NIMS is used a key source to manage patient and service user safety related issues. Some improvements are also underway. Based on our review, we note the following: ▪ Compliance related activities are being primarily managed and tracked through manual processes such as spreadsheets. For example, to report on Section 38 and Section 39 related findings; the reporting of HR	We recommend the following **D1.1** Consider implementing eGRC system to support the delivery of key Compliance processes such as COR maintenance; performance of risk and compliance

Observation	Recommendation
payments related findings; and Procurement related contract compliance findings. ▪ In addition, from a 2LOD perspective, we note that once core CCF processes are established, there is opportunity for the HSE to implement a eGRC solution to support compliance aspects such as COR maintenance, performing risk and compliance reviews, centralising and automating the recording of material Compliance issues and tracking these to completion; and in general, to support the aggregation of data points and sources to provide a view of the Compliance risk profile and the automation of consolidated reporting.	reviews; and to support centralised and aggregated reporting.
E – People and Skills	
Ref **E1** **Review and the CCF and 1LOD Compliance related staffing levels and skills**	**Priority** **High**
CCF Resources As outlined in Section 4.5 **– People and Skills**, the CCF is under development. Currently, the function is made up of the HBS Standards and Compliance team and has a total Whole Time Equivalent (WTE) resource allocation of 8. However, only 1 WTE (in addition to the Head of the function) is dedicated to Compliance related activities. The other WTEs are dedicated to Protected Disclosures (4 WTEs) and to administrative support (2 WTEs). Based on our review, we note the following: ▪ The CCF is provisionally led by the Assistant National Director of Governance and Compliance. A dedicated Head for the CCF, Chief Compliance Officer equivalent, has not been formally appointed. ▪ The HBS Standards and Compliance team is the only 2LOD team that currently performs compliance related activities. As noted above, only 1 WTE (in addition to the Head of the function) is dedicated to compliance related activities, and as such is significantly under-resourced. ▪ A skills assessment of CCF resources in light of the draft Compliance Framework has not been performed. As outlined on **Ref B1 – Review the structure of the CCF**, the structure, roles, and responsibilities of the CCF will need to be re-aligned to deliver the duties and requirements specified in the Compliance Framework. ▪ Key activities to inform staffing levels needed to fulfil the mandate of the CCF have not been carried out. This includes approving the CCF operating model; completing the risk assessment of the COR; and determining the maturity of 1LOD functions. As such, it is not currently possible to realistically assess resourcing needs (number of resources and skills of those resources). ▪ The above considerations may result in some resources currently in place being re-allocated within and outside of the CCF. It is also important to note, that to implement recommendations from this report, and to implement the Compliance Framework, will require substantial effort, over and above any 'business as usual' (BAU) activities. See Section 6.2 for additional details **1LOD Compliance Resources** As noted, throughout our review, multiple 1LOD functions perform compliance related monitoring and	We recommend the following: **E1.1** Appoint a dedicated Head of Compliance (at Assistant National Director level) to lead the compliance activities under the CCF reporting to the CRO; **E1.2.** Determine and source resources to assist with the implementation of the recommendations of this report and the new Compliance Operating Model; **E1.3.** Perform a forward-looking skills and capacity analysis to determine the headcount and skillset needed to fulfil the mandate of the CCF. However, 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. See **Section 6.2** for additional details; and, **Note**: the above analysis should be undertaken once the following has been completed: (i) design of the structure of the CCF; (ii) risk assessment of the COR; and (iii) maturity of 1LOD functions performing compliance related monitoring and assurance activities has been determined. **E1.4.** Perform forward-looking skills and capacity analysis to determine the headcount and skillset needed

Observation			**Recommendation**	
assurance activities. However, we note that a skills assessment for these functions has not been performed. In addition, we note that minimum requirements for 1LOD functions performing compliance related monitoring and assurance activities have not been implemented. As such, 1LOD resourcing and capability needs cannot be determined until 1LOD functions formalise their mandate and are assessed against minimum requirements.			across each 1LOD function performing compliance related monitoring and assurance to deliver on their individual mandate. The above analysis should be conducted once 1LOD minimum requirements are agreed and assessed. **Note**: A reassessment of the appropriate resourcing model may need to be performed once Regional Health Areas (RHAs) are established.	
F – Performance Management				
Ref	**F1**	**Develop and Implement Compliance Performance Indicators**	**Priority**	**Medium**
As outlined in Section 4.6 **– Performance Management,** four compliance related Key Performance Indicators (KPIs) are monitored and reported as part of National Scorecard KPIs included in the monthly performance profile. This includes the following KPIs: ▪ Governance and Compliance: (i) Procurement – expenditure (non-pay) under management; and (ii) % of internal audit recommendations implemented, against total no. of recommendations, within 12 months of report being received; ▪ Disability Act Compliance: % of assessments completed within the timelines as provided for in the regulations; and ▪ HIQA Inspection Compliance: % compliance with regulations following HIQA inspection of disability residential services However, based on our review we note that a suite of Compliance Performance measures that takes into consideration the Compliance Framework will need to be developed. As such, key components of the Compliance Framework that may need to be tracked and measured have not been determined. For example: Training – percentage of 1LOD Functions performing monitoring and assurance activities that have received compliance training; Compliance Monitoring Plan – completion percentage; Compliance issues - % of compliance issues remediated on time.			We recommend the following: **F1.1** Develop Compliance Performance Indicators in accordance with key aspects of the Compliance Framework; and, **F1.2** Assess Compliance related KPIs currently included in the National Scorecard and determine if these need to be updated based on the outcomes of the action above.	

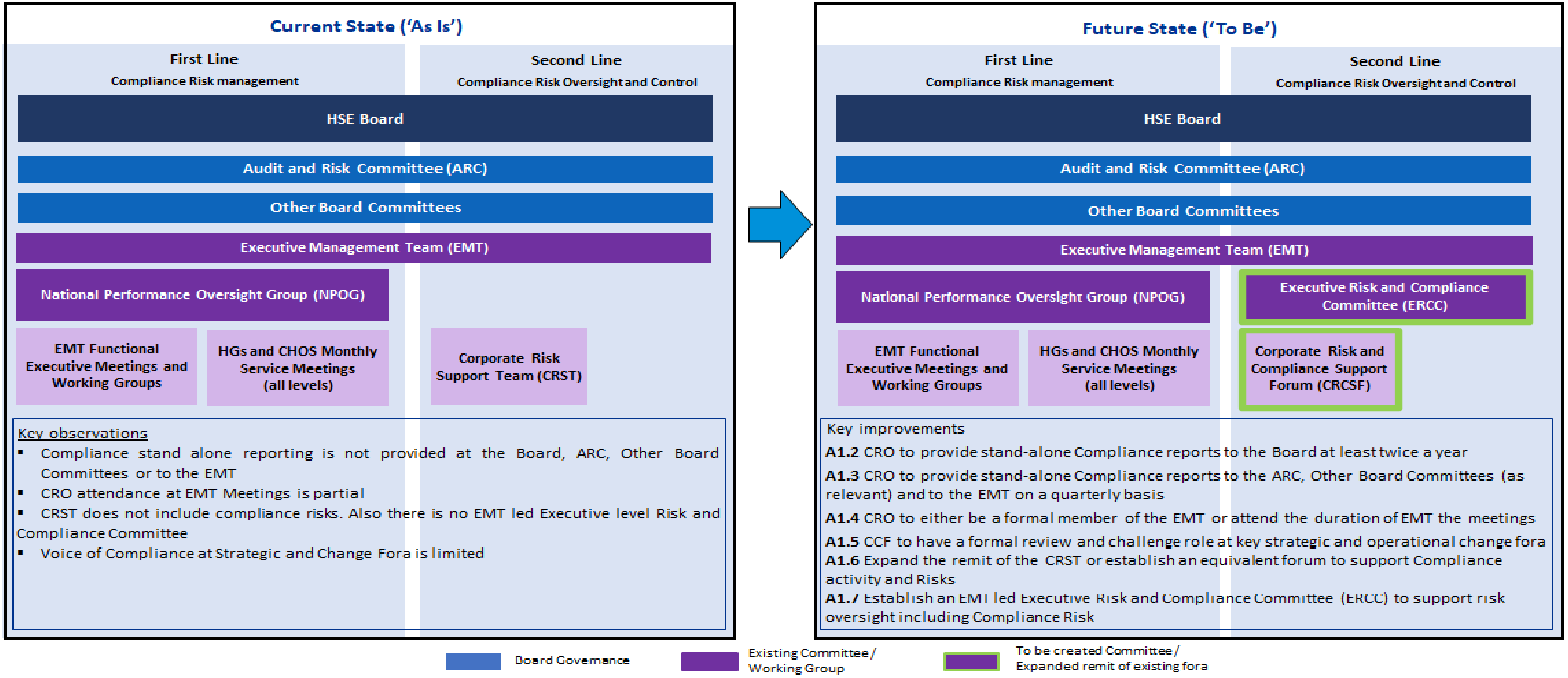
6. Proposed Future State Operating Model and Key Considerations

6.1. Governance and Mandate

As part of observations and recommendations outlined in observation **A1 – Enhance the Profile of the Central Compliance Function (CCF)** in relation to improvement opportunities to enhance Governance arrangements to oversee Compliance matters**,** we issued several recommendations that seek to enhance the profile of the Central Compliance Function and of the CRO, and the visibility of Compliance related matters across theHSE.

Below (see figure 4) is a summary articulation of the Governance structure in place across the HSE to support the management of Compliance Risks (Current State – As Is). We have also illustrated proposed changes and mapped the recommendations issued (Future State – To Be), including new structures and enhancements to be implemented.

Figure 4. To Be Compliance Related Governance Structure



Current State ('As Is')

First Line
Compliance Risk management

Second Line
Compliance Risk Oversight and Control

HSE Board

Audit and Risk Committee (ARC)

Other Board Committees

Executive Management Team (EMT)

National Performance Oversight Group (NPOG)

EMT Functional Executive Meetings and Working Groups

HGs and CHOS Monthly Service Meetings (all levels)

Corporate Risk Support Team (CRST)

Key observations

- Compliance stand alone reporting is not provided at the Board, ARC, Other Board Committees or to the EMT
- CRO attendance at EMT Meetings is partial
- CRST does not include compliance risks. Also there is no EMT led Executive level Risk and Compliance Committee
- Voice of Compliance at Strategic and Change Fora is limited

Future State ('To Be')

First Line
Compliance Risk management

Second Line
Compliance Risk Oversight and Control

HSE Board

Audit and Risk Committee (ARC)

Other Board Committees

Executive Management Team (EMT)

National Performance Oversight Group (NPOG)

Executive Risk and Compliance Committee (ERCC)

EMT Functional Executive Meetings and Working Groups

HGs and CHOS Monthly Service Meetings (all levels)

Corporate Risk and Compliance Support Forum (CRCSF)

Key improvements

A1.2 CRO to provide stand-alone Compliance reports to the Board at least twice a year

A1.3 CRO to provide stand-alone Compliance reports to the ARC, Other Board Committees (as relevant) and to the EMT on a quarterly basis

A1.4 CRO to either be a formal member of the EMT or attend the duration of EMT the meetings

A1.5 CCF to have a formal review and challenge role at key strategic and operational change fora

A1.6 Expand the remit of the CRST or establish an equivalent forum to support Compliance activity and Risks

A1.7 Establish an EMT led Executive Risk and Compliance Committee (ERCC) to support risk oversight including Compliance Risk

Board Governance

Existing Committee / Working Group

To be created Committee / Expanded remit of existing fora

6.2. Organisation and Location

The HSE will follow a 4LOD model in relation to Compliance. This 4LOD considers organisational nuances such as: (i) Corporate Functions vs local Functions (e.g., for Finance, Human Resources, Procurement); (ii) role in overseeing funded agencies and Hospital Groups; (iii) role of specialist functions; (iv) self-certification processes; and (iv) the importance of HIQA inspections, among other considerations. Summarised below are key attributes, control activities, assurance activities and teams for each HSE LOD.

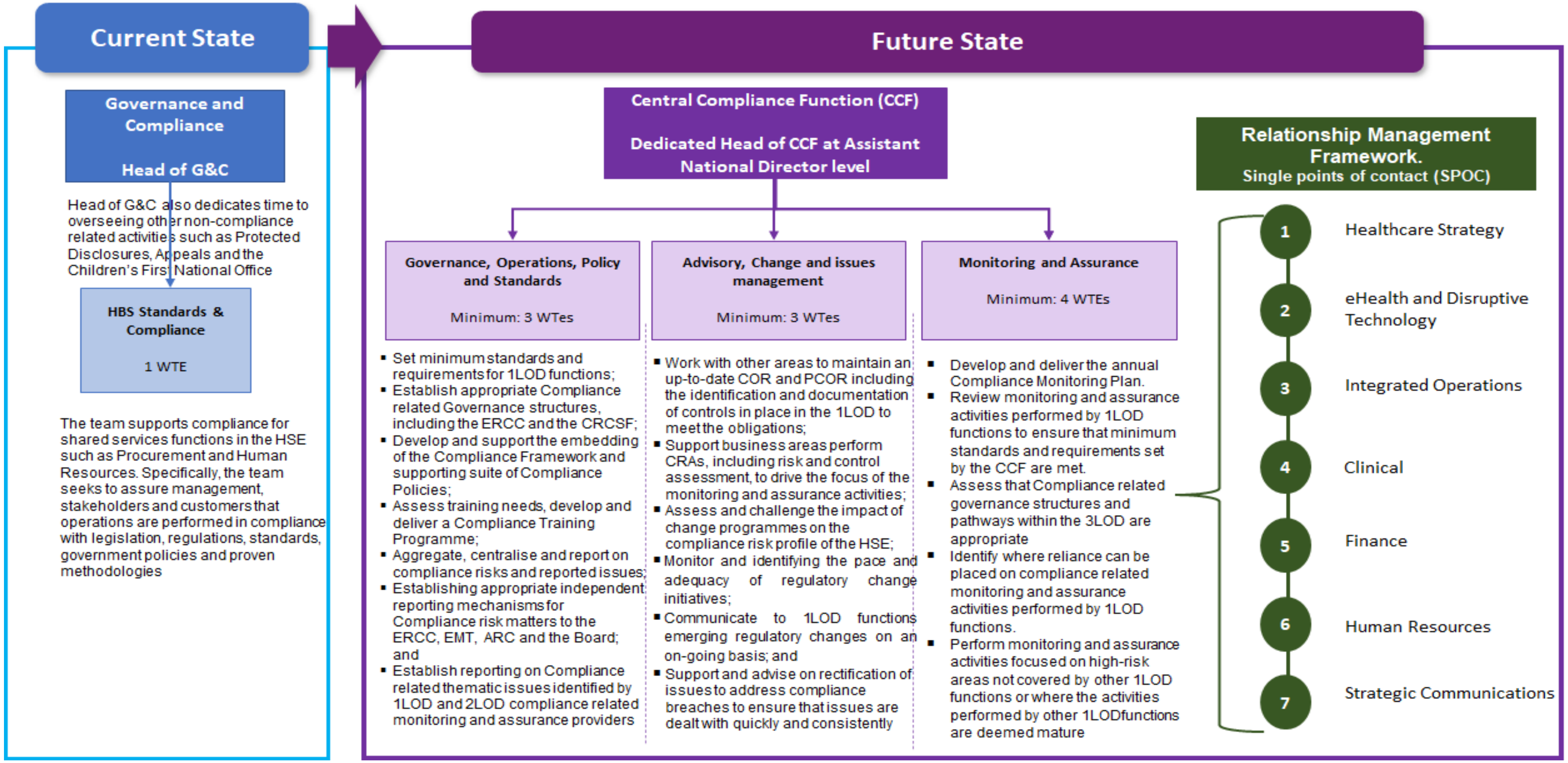
Figure 5. HSE 4LOD model

LOD	Key attributes and control activities	HSE LOD Activities	HSE Assurance Mechanism	HSE LOD Function
1LOD	▪ Owns and manages risks on a day to day ▪ Responsible for ensuring that controls are appropriate and operate effectively ▪ Applies risk policies and frameworks (as opposed to developing them) ▪ Oversight, monitoring, assurance ▪ Functional Area reporting to the HSE CEO	• These activities are the day-to-day policies, procedures and related controls which operate within each of the processes / functions within the HSE. • The 1LOD activities consist of any 1LOD oversight group, self-assessments or accreditation assessments performed by 1LOD functions. They also include control testing programmes, whether these activities are performed locally (e.g. hospital groups) or by Corporate Functions (e.g. Finance).	▪ Management oversight groups (chaired by 1LOD Functions) ▪ Self-assessments / self-certifications ▪ Independent reviews commissioned by 1LOD teams ▪ Control reviews performed by 1LOD teams independently from other 1LOD control owners. These activities can fall between two lines of defence under the concept of line 1.5. ▪ QPS reviews ▪ Performance and accountability oversight (NPOG)	▪ Human Resources ▪ Procurement ▪ Compliance Unit for funded agencies ▪ Operations ▪ Technology ▪ Finance ▪ Legal ▪ Corporate Affairs ▪ Strategy (excluding GRC) ▪ QPS Function
2LOD	▪ Monitoring and assurance over 1LOD activities ▪ Develops risk and compliance policies and frameworks to be applied by 1LOD Functions ▪ Function independent from 1LOD teams	▪ These activities provide oversight, monitoring and assurance that the 1LOD activities are operating as intended. ▪ The assurance providers in the 2LOD are internal to the organisation but independent of the activities over which they provide assurance.	▪ Risk and Compliance Assurance reviews (as developed) ▪ Assurance by NOCA	▪ Governance, Risk and Compliance ▪ NOCA
3LOD	▪ Provides assurance over 1LOD and 2LOD processes ▪ Independent from 1LOD and 2LOD Functions – Functional Reporting line to the Audit Committee	▪ These activities provide assurance over the processes owned and performed by 1LOD and 2LOD Functions.	▪ Internal Audit reports including health care audits	▪ Internal Audit
4LOD	▪ External party to the organisation	▪ These activities provide other form of independent assurance, external to the HSE, e.g. external audits. ▪ Reviews by regulators are also included given their value in informing internal HSE assurance efforts.	▪ Regulatory reviews	▪ HIQA/MHC ▪ C&AG

Organisation and Location (continued)

The structure of the CCF will be aligned with the Compliance Framework (as detailed in **B1 – Determine the structure of the CCF**). A Relationship Management Framework will be implemented to facilitate the interaction between the CCF and the 1LOD functions performing compliance related monitoring and assurance activities (as outlined in **B2 – Implement a relationship management framework**). Below is an indicative structure for the CCF including potential sub-teams, activities each team may perform, and how the CCF may interact with 1LOD functions to deliver its review and challenge and support role. To deliver these BAU activities at a minimum level (i.e. deliver minimum services) and recognising coverage limitations, **we estimate that a minimum of 10 WTEs, in addition to the dedicated head of the CCF, will be needed in the short term**. Further resources may be needed in the medium term once the maturity of 1LOD functions is known and the COR is risk assessed. A skills and capacity analysis will inform the size of the function in the medium term, as outlined in Section 6.5.

Figure 6. Organisation Structure of CCF



Current State

Governance and Compliance

Head of G&C

Head of G&C also dedicates time to overseeing other non-compliance related activities such as Protected Disclosures, Appeals and the Children's First National Office

HBS Standards & Compliance

1 WTE

The team supports compliance for shared services functions in the HSE such as Procurement and Human Resources. Specifically, the team seeks to assure management, stakeholders and customers that operations are performed in compliance with legislation, regulations, standards, government policies and proven methodologies

Future State

Central Compliance Function (CCF)

Dedicated Head of CCF at Assistant National Director level

Governance, Operations, Policy and Standards

Minimum: 3 WTes

- Set minimum standards and requirements for 1LOD functions;
- Establish appropriate Compliance related Governance structures, including the ERCC and the CRCSF;
- Develop and support the embedding of the Compliance Framework and supporting suite of Compliance Policies;
- Assess training needs, develop and deliver a Compliance Training Programme;
- Aggregate, centralise and report on compliance risks and reported issues;
- Establishing appropriate independent reporting mechanisms for Compliance risk matters to the ERCC, EMT, ARC and the Board; and
- Establish reporting on Compliance related thematic issues identified by 1LOD and 2LOD compliance related monitoring and assurance providers

Advisory, Change and issues management

Minimum: 3 WTes

- Work with other areas to maintain an up-to-date COR and PCOR including the identification and documentation of controls in place in the 1LOD to meet the obligations;
- Support business areas perform CRAs, including risk and control assessment, to drive the focus of the monitoring and assurance activities;
- Assess and challenge the impact of change programmes on the compliance risk profile of the HSE;
- Monitor and identifying the pace and adequacy of regulatory change initiatives;
- Communicate to 1LOD functions emerging regulatory changes on an on-going basis; and
- Support and advise on rectification of issues to address compliance breaches to ensure that issues are dealt with quickly and consistently

Monitoring and Assurance

Minimum: 4 WTEs

- Develop and deliver the annual Compliance Monitoring Plan.
- Review monitoring and assurance activities performed by 1LOD functions to ensure that minimum standards and requirements set by the CCF are met.
- Assess that Compliance related governance structures and pathways within the 3LOD are appropriate
- Identify where reliance can be placed on compliance related monitoring and assurance activities performed by 1LOD functions.
- Perform monitoring and assurance activities focused on high-risk areas not covered by other 1LOD functions or where the activities performed by other 1LODfunctions are deemed mature

Relationship Management Framework.
Single points of contact (SPOC)

1 Healthcare Strategy

2 eHealth and Disruptive Technology

3 Integrated Operations

4 Clinical

5 Finance

6 Human Resources

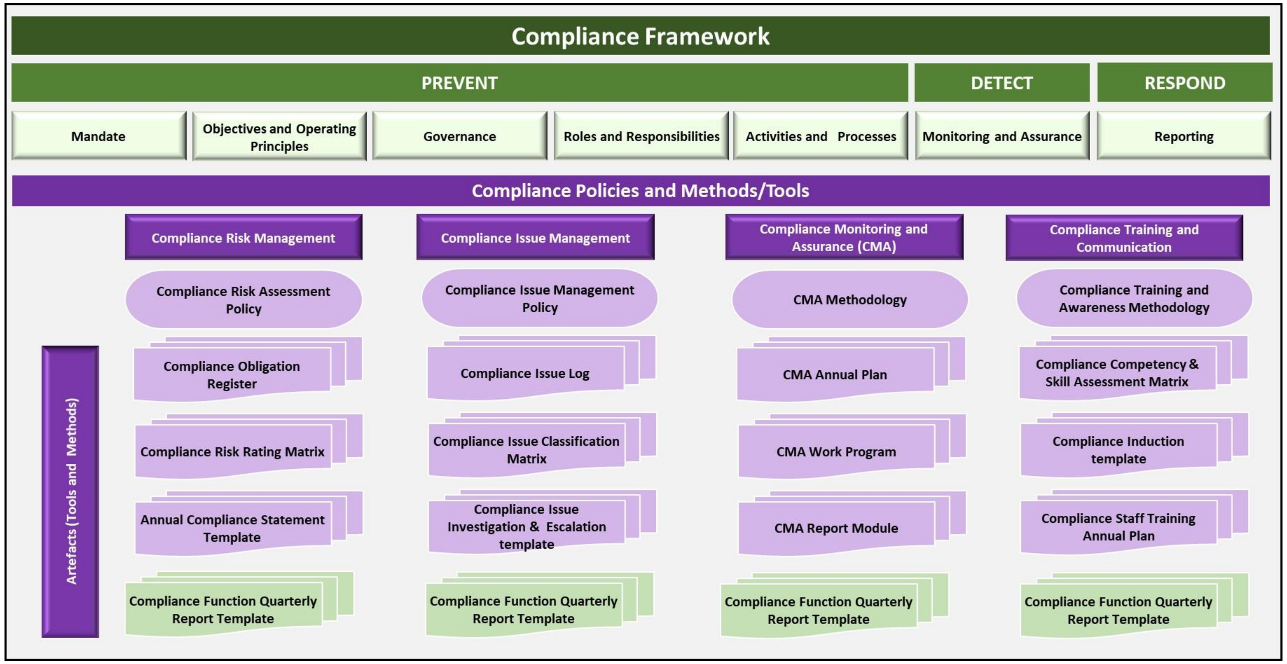
7 Strategic Communications

6.3. Activities and Processes: Prevent, Detect and Respond

Compliance requirements and guidance will be documented (as detailed in **CA2** – **Develop suite of supporting compliance policies, tools, and methods to support the implementation of the Framework)**. The 2LOD Compliance Risk Management Architecture will consist of:

- **Compliance Framework.** Sets out the principles, governance arrangements, roles and responsibilities, internal control, monitoring and assurance processes in place to support Compliance Management.
- **Compliance Policies and Standards.** Supports the Framework by providing additional minimum requirements and/or standards for the 1LOD to adhere to. Certain 2LOD methodologies will provide detailed guidance including step by step processes to manage different Compliance Risk Management activities such as: Compliance Risk Assessments; Compliance Issue Management; Compliance Monitoring and Assurance (CMA); and Compliance training and communication.
- **Artefacts (Tools and Methods).** Supports the operationalisation of Compliance Policies and Standards via artefacts that can be used to implement Compliance Risk Management activities. For example: The Compliance Obligations Register; Compliance Issues trackers; the Compliance Monitoring Plan among other artefacts.

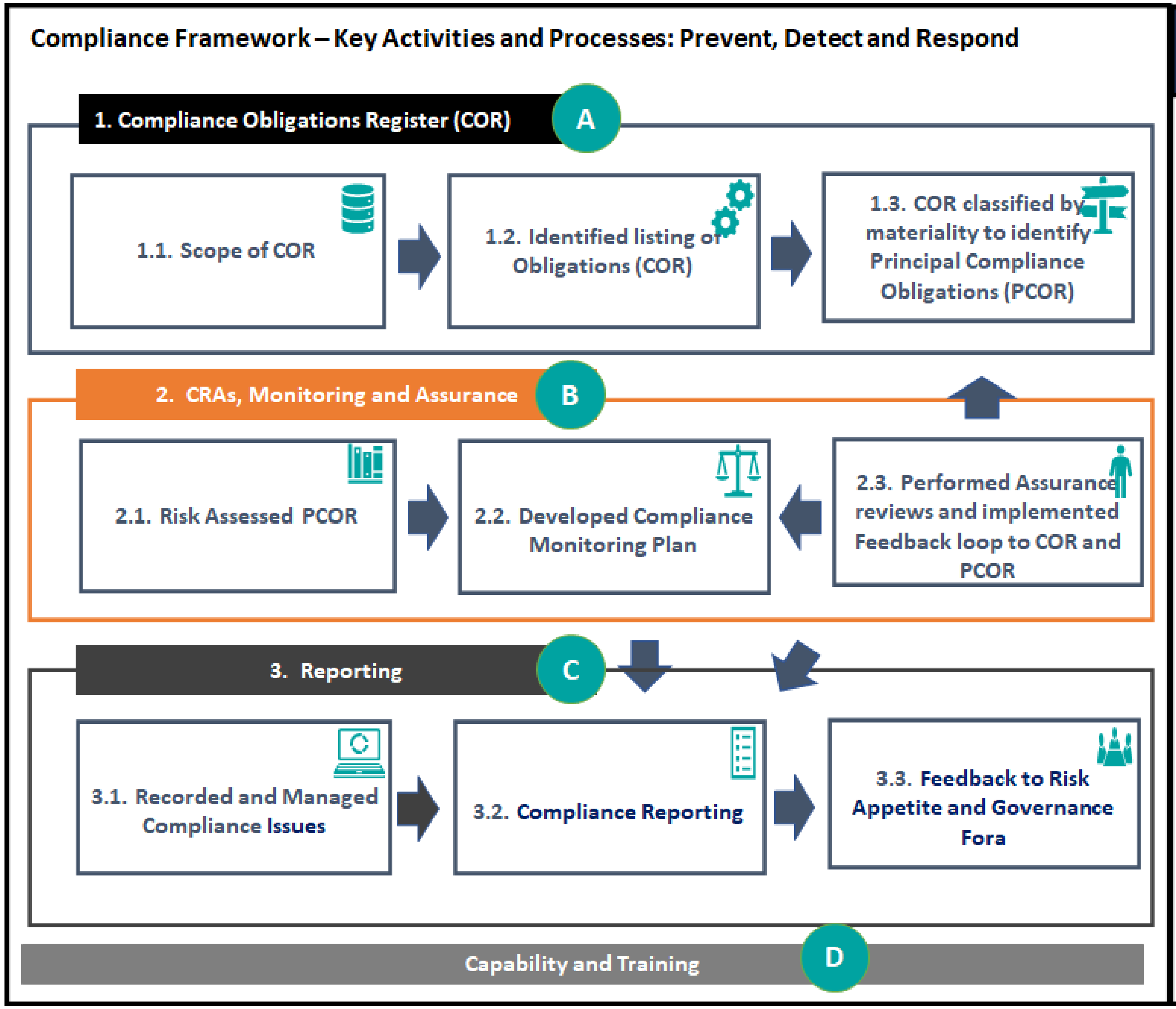
Figure 7. Compliance Management Architecture


Compliance Framework
PREVENT
DETECT
RESPOND
Mandate
Objectives and Operating Principles
Governance
Roles and Responsibilities
Activities and Processes
Monitoring and Assurance
Reporting
Compliance Policies and Methods/Tools
Compliance Risk Management
Compliance Issue Management
Compliance Monitoring and Assurance (CMA)
Compliance Training and Communication
Compliance Risk Assessment Policy
Compliance Issue Management Policy
CMA Methodology
Compliance Training and Awareness Methodology
Artefacts (Tools and Methods)
Compliance Obligation Register
Compliance Issue Log
CMA Annual Plan
Compliance Competency & Skill Assessment Matrix
Compliance Risk Rating Matrix
Compliance Issue Classification Matrix
CMA Work Program
Compliance Induction template
Annual Compliance Statement Template
Compliance Issue Investigation & Escalation template
CMA Report Module
Compliance Staff Training Annual Plan
Compliance Function Quarterly Report Template
Compliance Function Quarterly Report Template
Compliance Function Quarterly Report Template
Compliance Function Quarterly Report Template

Activities and Processes: Prevent, Detect and Respond (continued):

Key activities and processes to operationalise the Compliance Framework are outlined below along with expected high-level benefits:

Figure 8. Compliance Framework – key activities and processes: Prevent, Detect, and Respond



Compliance Framework – Key Activities and Processes: Prevent, Detect and Respond

1. Compliance Obligations Register (COR)
A
1.1. Scope of COR
1.2. Identified listing of Obligations (COR)
1.3. COR classified by materiality to identify Principal Compliance Obligations (PCOR)
2. CRAs, Monitoring and Assurance
B
2.1. Risk Assessed PCOR
2.2. Developed Compliance Monitoring Plan
2.3. Performed Assurance reviews and implemented Feedback loop to COR and PCOR
3. Reporting
C
3.1. Recorded and Managed Compliance Issues
3.2. Compliance Reporting
3.3. Feedback to Risk Appetite and Governance Fora
Capability and Training
D

Key Benefits

A Applicable obligations identified in the COR, and classified by materiality to determine the Principal Compliance Obligations (PCOR). This will enable a risk based approach to monitoring and assurance activities and will also allow allocating efforts and resources to the right activities.

B PCOR risk assessed to inform a risk based Compliance Monitoring Plan. This will help to review highest risk areas and provide assurance on same.

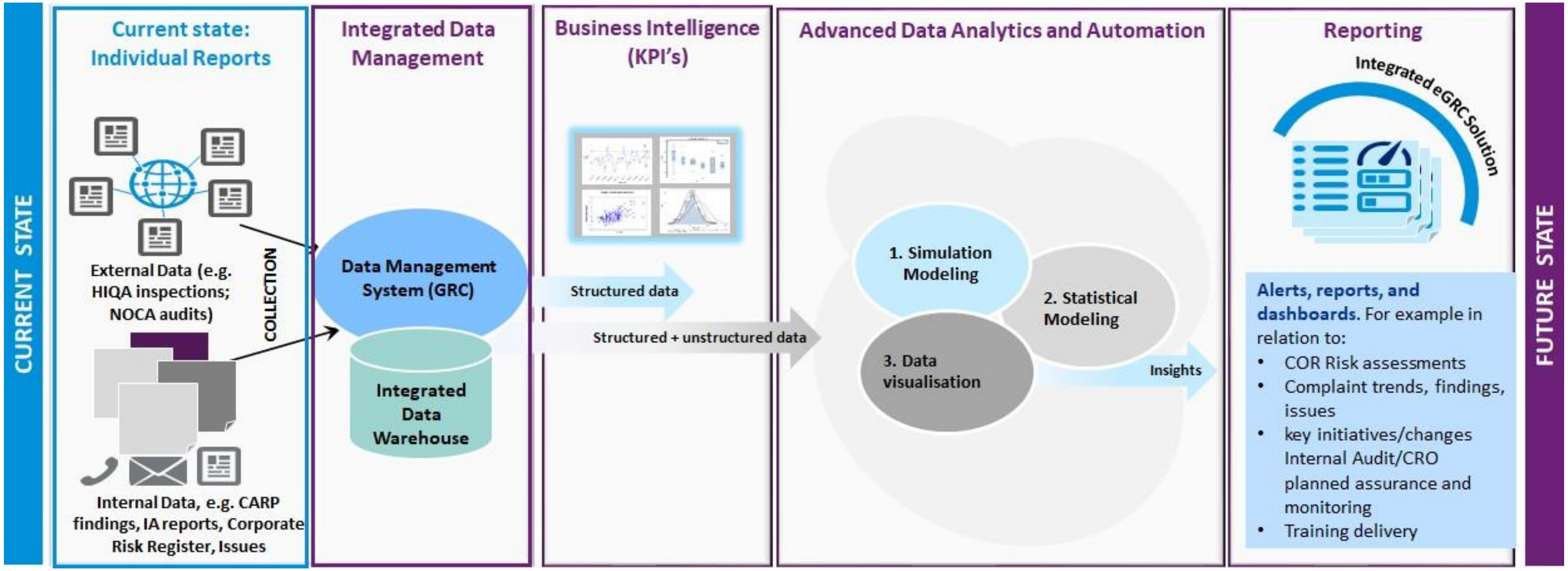
C Centralised, aggregated and timely reporting to the Board, ARC, Other Board Committees (as relevant), EMT, NPOG, ERCC, the expanded CRST (to be named Corporate Risk and Support Forum (CRCSF)), the CEO and CRO to provide an accurate and up date view on the compliance risk profile of the HSE.

D Capability of 1LOD Functions is enhanced to help mature the delivery of the compliance related monitoring and assurance activities they perform

6.4. Technology and Data

In the Future State technology and data will be leveraged to deliver efficiencies, streamline, and automate processes, and deliver data driven insights. An eGRC solution may be implemented to support compliance aspects such as COR maintenance, performing risk and compliance reviews, centralising and automating the recording of material Compliance issues and tracking these to completion; and in general, to support the aggregation of data points and sources to provide a view of the Compliance risk profile and the automation of consolidated reporting. Among other benefits, this would enable the implementation of centralised reporting, better transparency through objective and quantifiable analysis of compliance risks, and smart visualization reporting for risk and compliance matters. Below is the illustrative journey from current state to future state:

Figure 9. eGRC illustrative journey


CURRENT STATE
Current state: Individual Reports
External Data (e.g. HIQA inspections; NOCA audits)
COLLECTION
Internal Data, e.g. CARP findings, IA reports, Corporate Risk Register, Issues
Integrated Data Management
Data Management System (GRC)
Integrated Data Warehouse
Business Intelligence (KPI's)
Structured data
Structured + unstructured data
Advanced Data Analytics and Automation
1. Simulation Modeling
2. Statistical Modeling
3. Data visualisation
Insights
Reporting
Integrated eGRC Solution
FUTURE STATE

Alerts, reports, and dashboards. For example in relation to:

- COR Risk assessments
- Complaint trends, findings, issues
- key initiatives/changes Internal Audit/CRO planned assurance and monitoring
- Training delivery

6.5. People and Skills

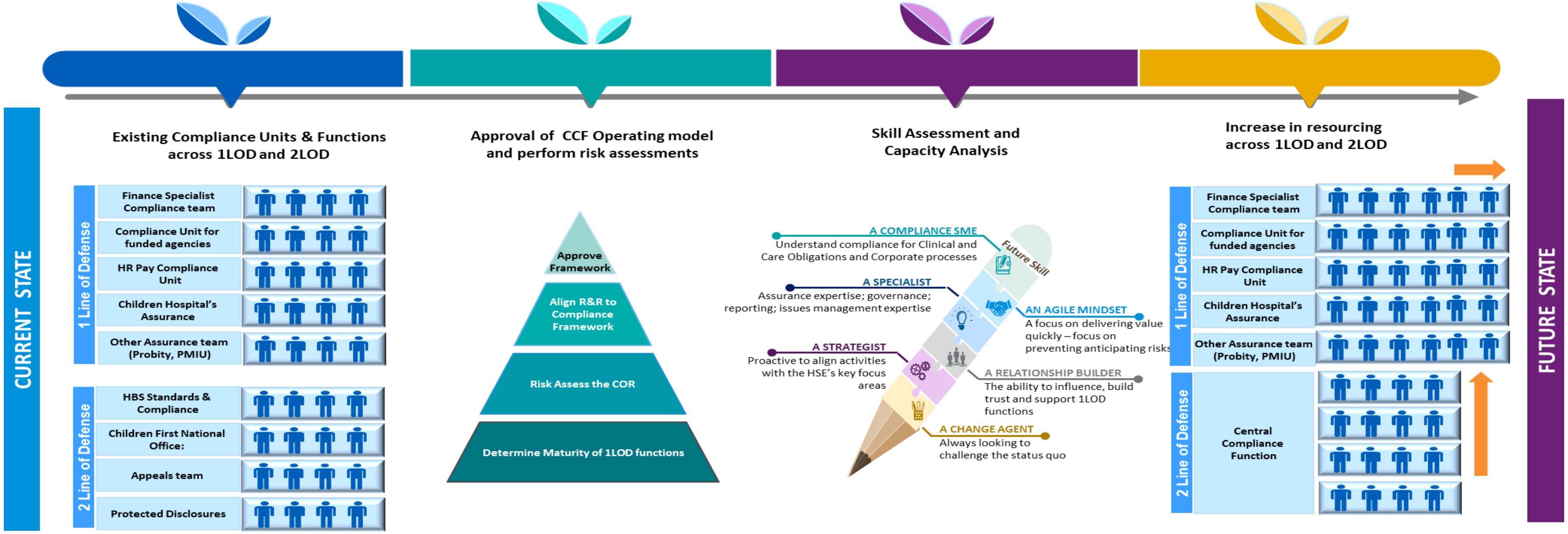
2LOD Central Compliance Function (CCF)

- **The HSE Board through its Audit and Risk Committee (ARC) and the EMT strongly supports the establishment of a robust, impactful, well embedded, and value adding Central Compliance Function (CCF)**. Having the right skills, culture and capabilities will be critical to drive forward the activities to be performed by the CCF.
- The skills and size of the CCF will be determined once the CCF operating model is approved; the COR is risk assessed; and the maturity of 1LOD functions is determined.
- A skills assessment of CCF resources will then be performed. This may result in some of the resources currently in place being re-allocated within and outside of the CCF.

1LOD Compliance Resources

- A skills assessment for 1LOD functions performing compliance related monitoring and assurance activities will be performed once 1LOD functions formalise their mandate and are assessed against minimum requirements. Staffing and capability actions will be determined and raised at the ERCC

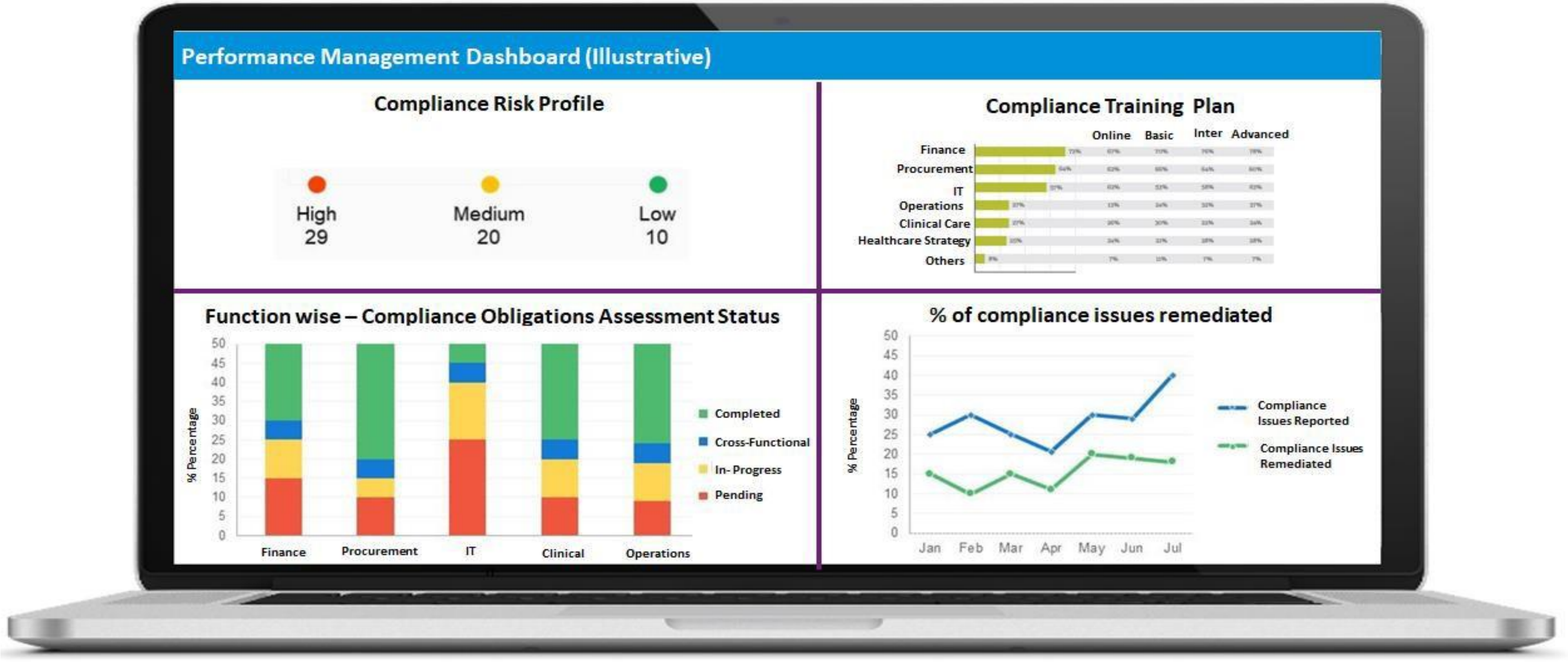
Figure 10. Resourcing future state considerations


CURRENT STATE
Existing Compliance Units & Functions across 1LOD and 2LOD
1 Line of Defense
Finance Specialist Compliance team
Compliance Unit for funded agencies
HR Pay Compliance Unit
Children Hospital's Assurance
Other Assurance team (Probity, PMIU)
2 Line of Defense
HBS Standards & Compliance
Children First National Office:
Appeals team
Protected Disclosures
Approval of CCF Operating model and perform risk assessments
Approve Framework
Align R&R to Compliance Framework
Risk Assess the COR
Determine Maturity of 1LOD functions
Skill Assessment and Capacity Analysis
Future Skill
A COMPLIANCE SME
Understand compliance for Clinical and Care Obligations and Corporate processes
A SPECIALIST
Assurance expertise; governance; reporting; issues management expertise
AN AGILE MINDSET
A focus on delivering value quickly – focus on preventing anticipating risks
A STRATEGIST
Proactive to align activities with the HSE's key focus areas
A RELATIONSHIP BUILDER
The ability to influence, build trust and support 1LOD functions
A CHANGE AGENT
Always looking to challenge the status quo
Increase in resourcing across 1LOD and 2LOD
1 Line of Defense
Finance Specialist Compliance team
Compliance Unit for funded agencies
HR Pay Compliance Unit
Children Hospital's Assurance
Other Assurance team (Probity, PMIU)
2 Line of Defense
Central Compliance Function
FUTURE STATE

6.6. Performance Management

The HSE will adopt a **continuous improvement** mind-set to Compliance management. Measuring and reporting on key performance metrics will support **Compliance Management becoming a discipline as opposed to a process**. Example KPIs and dashboard has been outlined below. Data gathering, consolidation and data visualisation processes may be automated through the eGRC solution as described in [Section 6.4.](#)

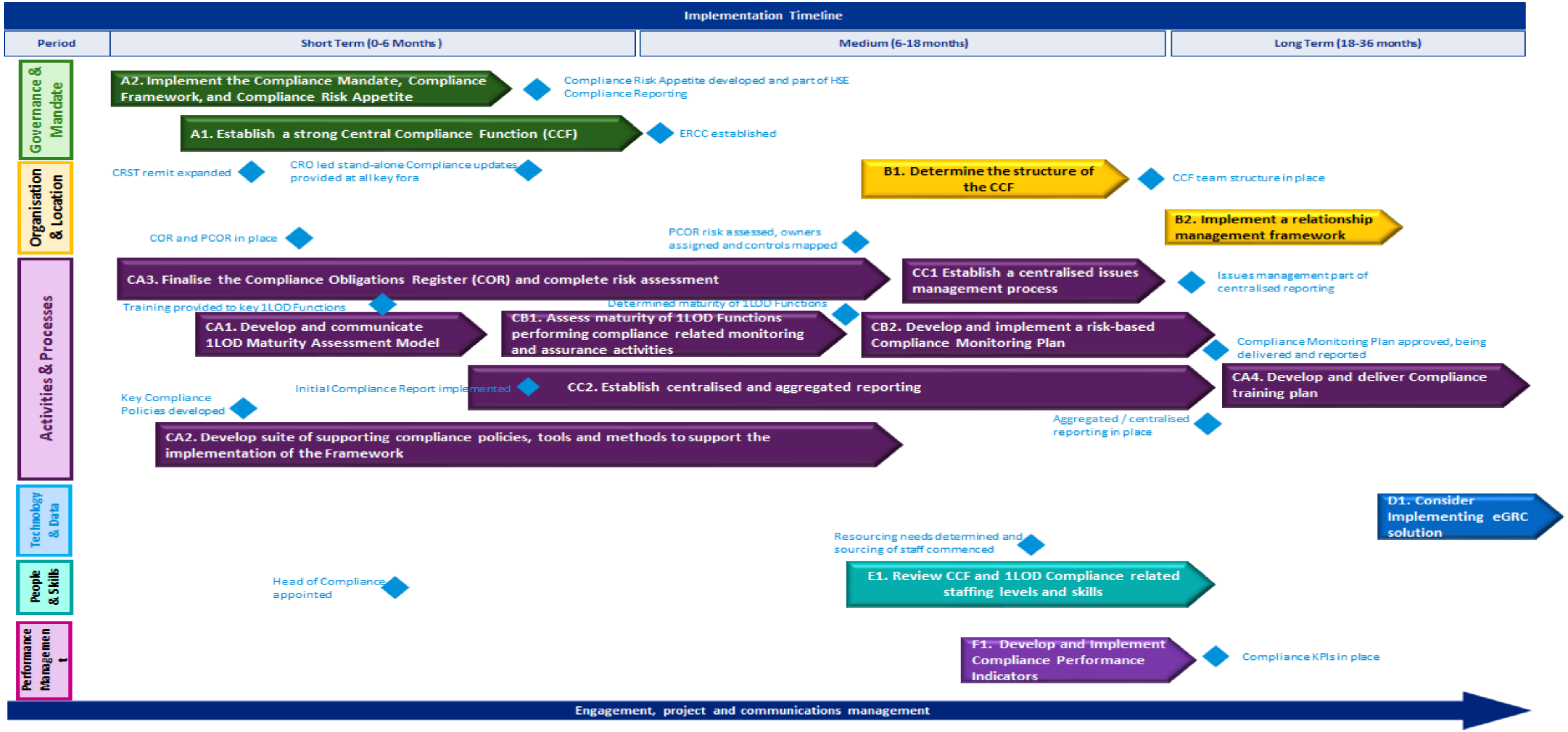
Figure 11. Performance management illustrative dashboard



7. High-Level Roadmap

Based on the improvement opportunities identified in Section 5, below we have illustrated a high-level roadmap of activities for the HSE to implement the proposed operating model. This assumes that appropriate sponsorship and resources are assigned to both the implementation programme and the CCF. Quick wins have been identified in Section 1.7 **– Quick wins – within 6 months**

Figure 12. High Level Roadmap



Implementation Timeline

Period | Short Term (0-6 Months) | Medium (6-18 months) | Long Term (18-36 months)

Governance & Mandate

A2. Implement the Compliance Mandate, Compliance Framework, and Compliance Risk Appetite

Compliance Risk Appetite developed and part of HSE Compliance Reporting

A1. Establish a strong Central Compliance Function (CCF)

ERCC established

Organisation & Location

CRST remit expanded

CRO led stand-alone Compliance updates provided at all key fora

B1. Determine the structure of the CCF

CCF team structure in place

COR and PCOR in place

PCOR risk assessed, owners assigned and controls mapped

B2. Implement a relationship management framework

Activities & Processes

CA3. Finalise the Compliance Obligations Register (COR) and complete risk assessment

CC1 Establish a centralised issues management process

Issues management part of centralised reporting

Training provided to key 1LOD Functions

Determined maturity of 1LOD Functions

CA1. Develop and communicate 1LOD Maturity Assessment Model

CB1. Assess maturity of 1LOD Functions performing compliance related monitoring and assurance activities

CB2. Develop and implement a risk-based Compliance Monitoring Plan

Compliance Monitoring Plan approved, being delivered and reported

Key Compliance Policies developed

Initial Compliance Report implemented

CC2. Establish centralised and aggregated reporting

CA4. Develop and deliver Compliance training plan

Aggregated / centralised reporting in place

CA2. Develop suite of supporting compliance policies, tools and methods to support the implementation of the Framework

Technology & Data

D1. Consider Implementing eGRC solution

People & Skills

Resourcing needs determined and sourcing of staff commenced

Head of Compliance appointed

E1. Review CCF and 1LOD Compliance related staffing levels and skills

Performance Management

F1. Develop and Implement Compliance Performance Indicators

Compliance KPIs in place

Engagement, project and communications management

8. Next Steps

Below are the immediate next steps needed to implement the roadmap of activities

1	Obtain ARC and EMT approval on the Compliance Framework and discuss the outcomes of this report. Also, assign appropriate sponsorship and resources to both an implementation programme to implement changes and to the CCF for quick wins and business as usual activities. At a minimum, the CCF will require minimum 5 WTEs (with relevant organisational and risk/compliance competencies) to deliver quick wins. As an indication, we estimate the CCF will require circa 10 WTE's, in addition to the dedicated Head of the CCF, to deliver on the foundational elements of the Compliance operating model for at least 12 months pending the outcome of a more detailed resourcing assessment. However, this is indicative, depending on the outcome of the maturity assessment of the 1LOD functions that provide compliance related monitoring and assurance activities. A skills and capacity analysis will inform the size of the function in the medium term. An implementation programme will need to be established to drive and implement the changes required to the operating model. This will require project and change resources in addition to the CCF resources noted above.
2	Assign owners and timelines to each of the recommendations outlined in **Section 5**
3	Establish implementation programme to deliver the roadmap of activities. This should include structuring a Steering Committee led by the CRO, a design authority, and appointing a programme lead along with project, delivery and change resources.
4	Develop programme delivery plan including workstreams and workstream leads. This should include the development of an overall programme plan and work stream plans.
5	Agree frequency of reporting to the Steering Committee and approve overall delivery plan.

9. Appendices

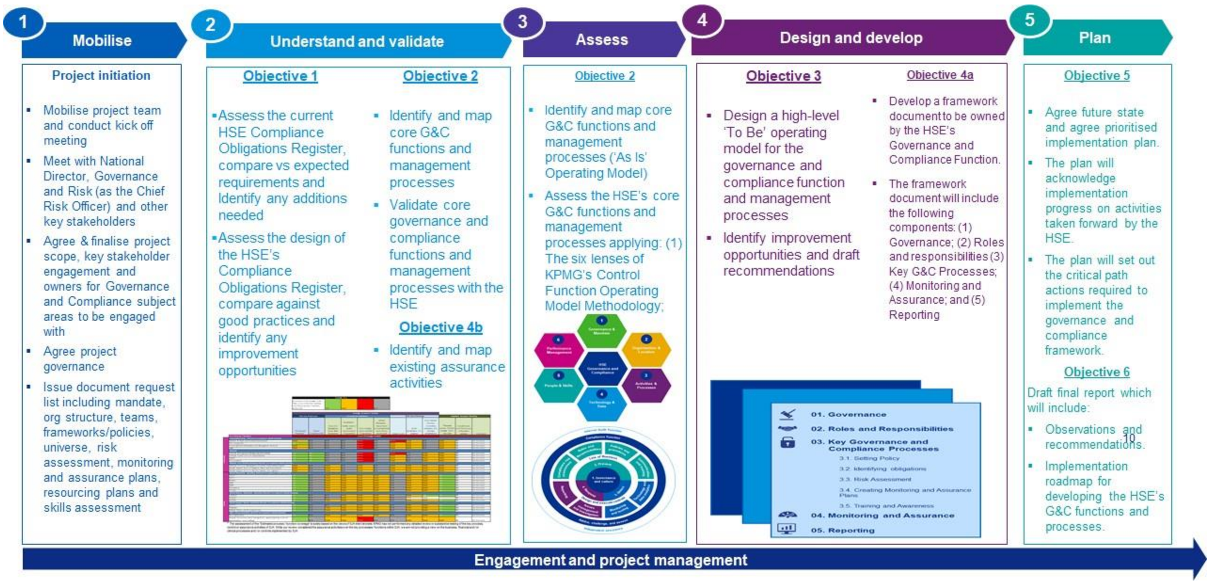
Appendix A. Scope of Services

The scope of services undertaken sought to achieve the below six objectives:

1. **Objective 1: Support the development of a Compliance Obligations Register (COR)**. For the HSE to identify and validate the core compliance responsibilities.
2. **Objective 2: Document the current state (“As is”) of the HSE Compliance activities and processes.** To understand and map the HSE’s core compliance functions and management processes and identify any gaps
3. **Objective 3. Develop the HSE Compliance Framework**. To design a framework for the HSE’s Central Compliance Function outlining its mandate and its role vis a vis other governance and compliance functions in the HSE.
4. **Objective 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. **Objective 5 and Objective 6. 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 resourcing plan to deliver the recommendations from this review.

The approach followed is summarised below.

Figure 13. Approach and key activities



1 Mobilise

Project initiation

- Mobilise project team and conduct kick off meeting
- Meet with National Director, Governance and Risk (as the Chief Risk Officer) and other key stakeholders
- Agree & finalise project scope, key stakeholder engagement and owners for Governance and Compliance subject areas to be engaged with
- Agree project governance
- Issue document request list including mandate, org structure, teams, frameworks/policies, universe, risk assessment, monitoring and assurance plans, resourcing plans and skills assessment

2 Understand and validate

Objective 1

- Assess the current HSE Compliance Obligations Register, compare vs expected requirements and Identify any additions needed
- Assess the design of the HSE's Compliance Obligations Register, compare against good practices and identify any improvement opportunities

Objective 2

- Identify and map core G&C functions and management processes
- Validate core governance and compliance functions and management processes with the HSE

Objective 4b

- Identify and map existing assurance activities

3 Assess

Objective 2

- Identify and map core G&C functions and management processes ('As Is' Operating Model)
- Assess the HSE's core G&C functions and management processes applying: (1) The six lenses of KPMG's Control Function Operating Model Methodology;

4 Design and develop

Objective 3

- Design a high-level 'To Be' operating model for the governance and compliance function and management processes
- Identify improvement opportunities and draft recommendations

Objective 4a

- Develop a framework document to be owned by the HSE's Governance and Compliance Function.
- The framework document will include the following components: (1) Governance; (2) Roles and responsibilities (3) Key G&C Processes; (4) Monitoring and Assurance; and (5) Reporting

01. Governance
02. Roles and Responsibilities
03. Key Governance and Compliance Processes
3.1. Setting Policy
3.2. Identifying obligations
3.3. Risk Assessment
3.4. Creating Monitoring and Assurance Plans
3.5. Training and Awareness
04. Monitoring and Assurance
05. Reporting

5 Plan

Objective 5

- Agree future state and agree prioritised implementation plan.
- The plan will acknowledge implementation progress on activities taken forward by the HSE.
- The plan will set out the critical path actions required to implement the governance and compliance framework.

Objective 6

Draft final report which will include:

- Observations and recommendations.
- Implementation roadmap for developing the HSE's G&C functions and processes.

Engagement and project management

Out of Scope

For the avoidance of doubt, and as agreed with Management:

- Our review was based solely on reviews of documentation provided to us and discussions with the agreed stakeholders;

- Our review did not include testing of the operational effectiveness of Compliance risk related policies, processes, or controls;
- Our review did not include a detailed gap analysis of existing policies and procedures against regulatory requirements;
- Our review did not assess the adequacy or operating effectiveness of Risk Management Frameworks or Risk Policies;
- Our review did not assess the adequacy and/or effectiveness of Risk and/or Compliance review activities across the HSE, including those of the 1LOD compliance related monitoring and assurance activities; or
- The quality or accuracy of data and MI included in Compliance related reporting.

Appendix B. Stakeholder Interviews

As part of our review, we conducted 28 interviews with key stakeholders throughout the organisation including the Chair of the ARC, the Chief Risk Officer (CRO), Chief Financial Officer (CFO), Chief Strategy Officer (CSO), the Head of Internal Audit, and multiple National Directors, Assistant National Directors and Heads of Functions. Interviews included discussions on the compliance related monitoring and assurance activities undertaken across the HSE, the mandate of the CCF, key activities, structure and staffing strategy of the CCF, and overall opinions on the future operating model of the Function. See below details of the key stakeholders interviewed.

Table 1. List of interviews conducted.

#	Name	Role/Team
1	Patrick Lynch	National Director Governance and Risk and Chief Risk Officer
2	Mairead Dolan	Assistant CFO
3	Dara Purcell	Board Secretary and Head of Legal Affairs
4	Brian Murphy	Head of Corporate Affairs, Office of the CEO
5	Rosemary Grey	Assistant National Director Governance and Compliance
6	Kevin Cleary	Head of Compliance Unit [Funded agencies]
7	Dean Sullivan	Chief Strategy Officer
8	Anne O'Connor	Chief Operations Officer
9	Stephen Mulvany	Chief Financial Officer
10	Fran Thompson	Chief Information Officer
11	Tom Malone	Head of Internal Audit
12	Colm Henry	Chief Clinical Officer
13	Liam Woods	National Director Acute Operations
14	Yvonne O'Neill	National Director Community Operations
15	Paul Reid	Chief Executive Officer
16	Brendan Lenihan	Chair, Audit and Risk Committee
17	Martin McKeith	Assistant Lead Director, CHP&P
18	Paul de Freine	Interim National Director Capital & Estates
19	Ann Marie Hoey	National Director, Human Resources
20	John Swords	National Director, Procurement
21	Declan Lyons	CEO, Ireland East Hospital Group (IEHG)
22	Orla Healy	National Clinical Director, National Quality and Patient Safety
23	Johnny Farren	HSE Interim DPO
24	Maria Lordan Dunphy	Assistant National Director, National Quality and Patient Safety
25	Mark Brennock	National Director, Communications
26	Damien McCallion	Interim, Chief Operations Officer
27	David Walsh	National Director Schemes & Reimbursement
28	Joe Ryan	National Director, Operational Performance and Integration

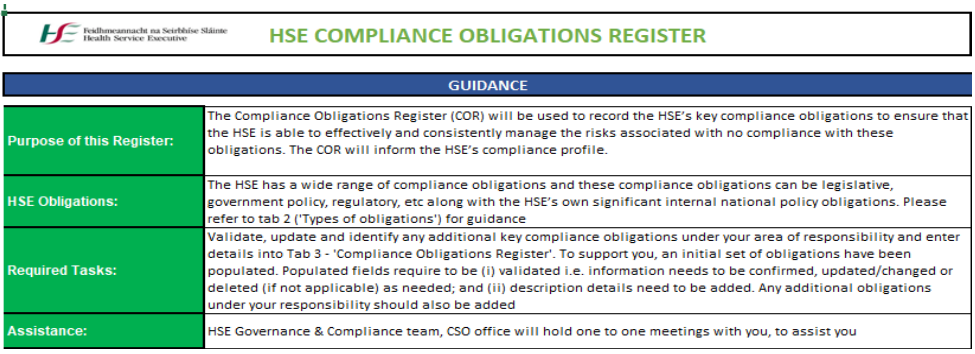
Appendix C. Compliance Obligation Register

KPMG supported in developing the design of the Compliance Obligation Register (COR) and the output was agreed by the key HSE stakeholders. The purpose of the Compliance Obligations Register (COR) is to act as a central repository for the HSE's applicable obligations, including laws, regulations, and internal policies. The HSE COR consists of the following sections: (A) Description and tiering; (B) Ownership and documentation; (C) Impacted teams; (D) Oversight and adherence; and (E) Sign-off.

Approach to populate and Assess COR

The initial set of compliance obligations have been populated with the support of a HSE working group (key nominees from all HSE Divisions). The first draft of COR was developed and populated with key regulatory/legislative, Health Regulatory, Public Policy and core PPPG's (as recorded in the 2015 Code of Governance). At the time of reporting, the initial listing of obligations in the COR is being validated by HSE stakeholders, and subsequently, a Principal Compliance Obligations Register (PCOR) consisting of key/material obligations to the HSE will be identified. The criteria to assess the PCOR is being finalised. After the assessment criteria is finalised, prioritisation exercise should be performed to assess the compliance risk and develop the compliance monitoring plan. Below we have illustrated key aspects of the COR designed:

Figure 14. COR Guidance Sheet



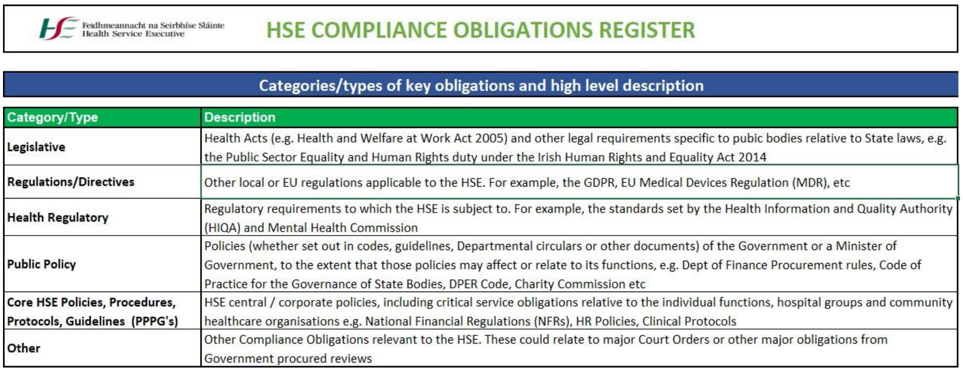
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

HSE COMPLIANCE OBLIGATIONS REGISTER

GUIDANCE

Purpose of this Register:	The Compliance Obligations Register (COR) will be used to record the HSE's key compliance obligations to ensure that the HSE is able to effectively and consistently manage the risks associated with no compliance with these obligations. The COR will inform the HSE's compliance profile.
HSE Obligations:	The HSE has a wide range of compliance obligations and these compliance obligations can be legislative, government policy, regulatory, etc along with the HSE's own significant internal national policy obligations. Please refer to tab 2 ('Types of obligations') for guidance
Required Tasks:	Validate, update and identify any additional key compliance obligations under your area of responsibility and enter details into Tab 3 - 'Compliance Obligations Register'. To support you, an initial set of obligations have been populated. Populated fields require to be (i) validated i.e. information needs to be confirmed, updated/changed or deleted (if not applicable) as needed; and (ii) description details need to be added. Any additional obligations under your responsibility should also be added
Assistance:	HSE Governance & Compliance team, CSO office will hold one to one meetings with you, to assist you

Figure 15. Types of Obligations



Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

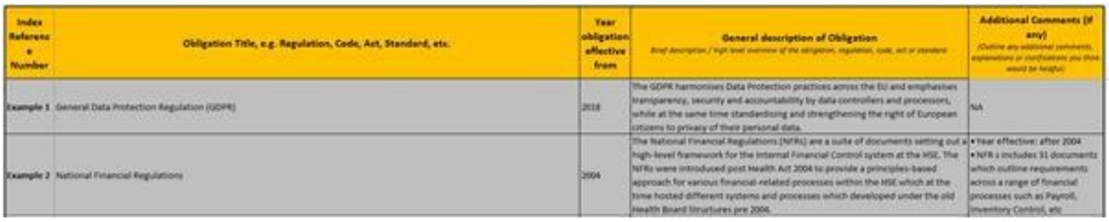
HSE COMPLIANCE OBLIGATIONS REGISTER

Categories/types of key obligations and high level description

Category/Type	Description
Legislative	Health Acts (e.g. Health and Welfare at Work Act 2005) and other legal requirements specific to pubic bodies relative to State laws, e.g. the Public Sector Equality and Human Rights duty under the Irish Human Rights and Equality Act 2014
Regulations/Directives	Other local or EU regulations applicable to the HSE. For example, the GDPR, EU Medical Devices Regulation (MDR), etc
Health Regulatory	Regulatory requirements to which the HSE is subject to. For example, the standards set by the Health Information and Quality Authority (HIQA) and Mental Health Commission
Public Policy	Policies (whether set out in codes, guidelines, Departmental circulars or other documents) of the Government or a Minister of Government, to the extent that those policies may affect or relate to its functions, e.g. Dept of Finance Procurement rules, Code of Practice for the Governance of State Bodies, DPER Code, Charity Commission etc
Core HSE Policies, Procedures, Protocols, Guidelines (PPPG's)	HSE central / corporate policies, including critical service obligations relative to the individual functions, hospital groups and community healthcare organisations e.g. National Financial Regulations (NFRs), HR Policies, Clinical Protocols
Other	Other Compliance Obligations relevant to the HSE. These could relate to major Court Orders or other major obligations from Government procured reviews

Compliance Obligation Register

Figure 16. COR template (partial extract). Complete COR design is appended above



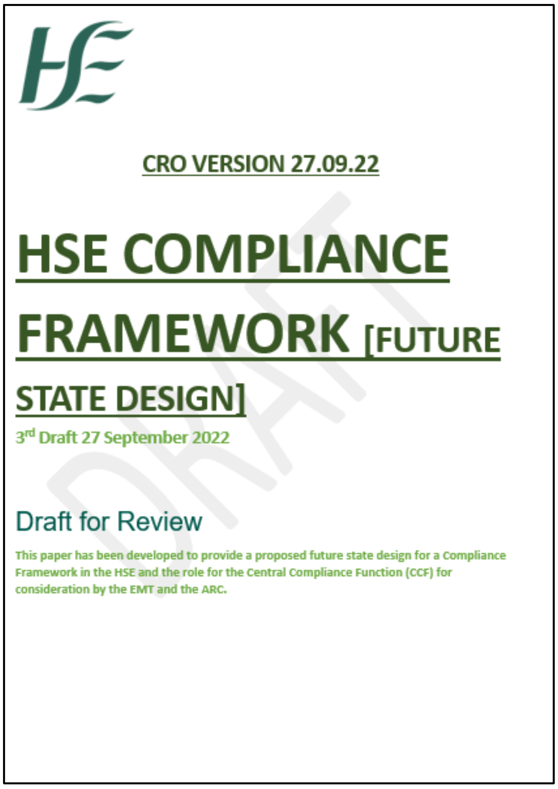
Index Reference Number	Obligation Title, e.g. Regulation, Code, Act, Standard, etc.	Year obligation effective from	General description of Obligation Brief description / high level overview of the obligation, regulation, code, act or standard	Additional Comments (if any) (Outline any additional comments, explanations or clarifications you think would be helpful)
Example 1	General Data Protection Regulation (GDPR)	2018	The GDPR harmonises Data Protection practices across the EU and emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to privacy of their personal data.	NA
Example 2	National Financial Regulations	2004	The National Financial Regulations (NFRs) are a suite of documents setting out a high-level framework for the internal Financial Control system at the HSE. The NFRs were introduced post Health Act 2004 to provide a principles-based approach for various financial-related processes within the HSE which at the time hosted different systems and processes which developed under the old Health Board Structures pre 2004.	• Year effective: after 2004 • NFR s includes 31 documents which outline requirements across a range of financial processes such as Payroll, Inventory Control, etc

Appendix D. HSE Compliance Framework

KPMG supported the development of the HSE's Compliance Framework. This Framework outlines the mandate of the Central Compliance Function and defines the HSE's approach to manage Compliance Risks. The Framework also sets out key requirements which are to be adopted across the HSE in relation to: (1) Governance; (2) Roles and Responsibilities; (3) PREVENT - Activities and Processes; (4) DETECT – Monitoring and Assurance; and (5) RESPOND – Reporting.

The Compliance Framework has been approved by the HSE Steering Group and is subject to final approval by the HSE ARC and EMT. See below for a summary of the contents of the Framework. For complete details please see the appended document.

Figure 17. HSE Compliance Framework



CRO VERSION 27.09.22

HSE COMPLIANCE FRAMEWORK [FUTURE STATE DESIGN]

3rd Draft 27 September 2022

Draft for Review

This paper has been developed to provide a proposed future state design for a Compliance Framework in the HSE and the role for the Central Compliance Function (CCF) for consideration by the EMT and the ARC.

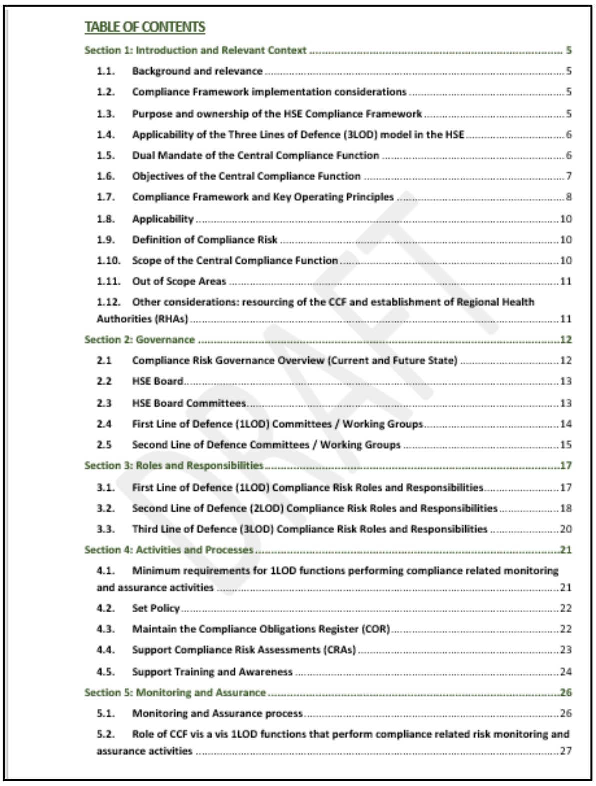


TABLE OF CONTENTS

HSE Compliance Framework 3rd DRAF

Appendix E. Maturity Criteria for 1LOD Monitoring and Assurance functions

Below is the maturity criteria for the CCF to assess the maturity of compliance related monitoring and assurance activities performed by 1LOD functions. This includes assessment against the six lenses below (see diagram). Minimum requirements for each of these six lenses have been outlined in the next page and have also been included in the Compliance Framework. The CCF will rate the maturity of 1LOD functions across the following maturity scale – **1.0 Initial, 2.0 Developing and 3.0 Established**.

Figure 18. Maturity Criteria

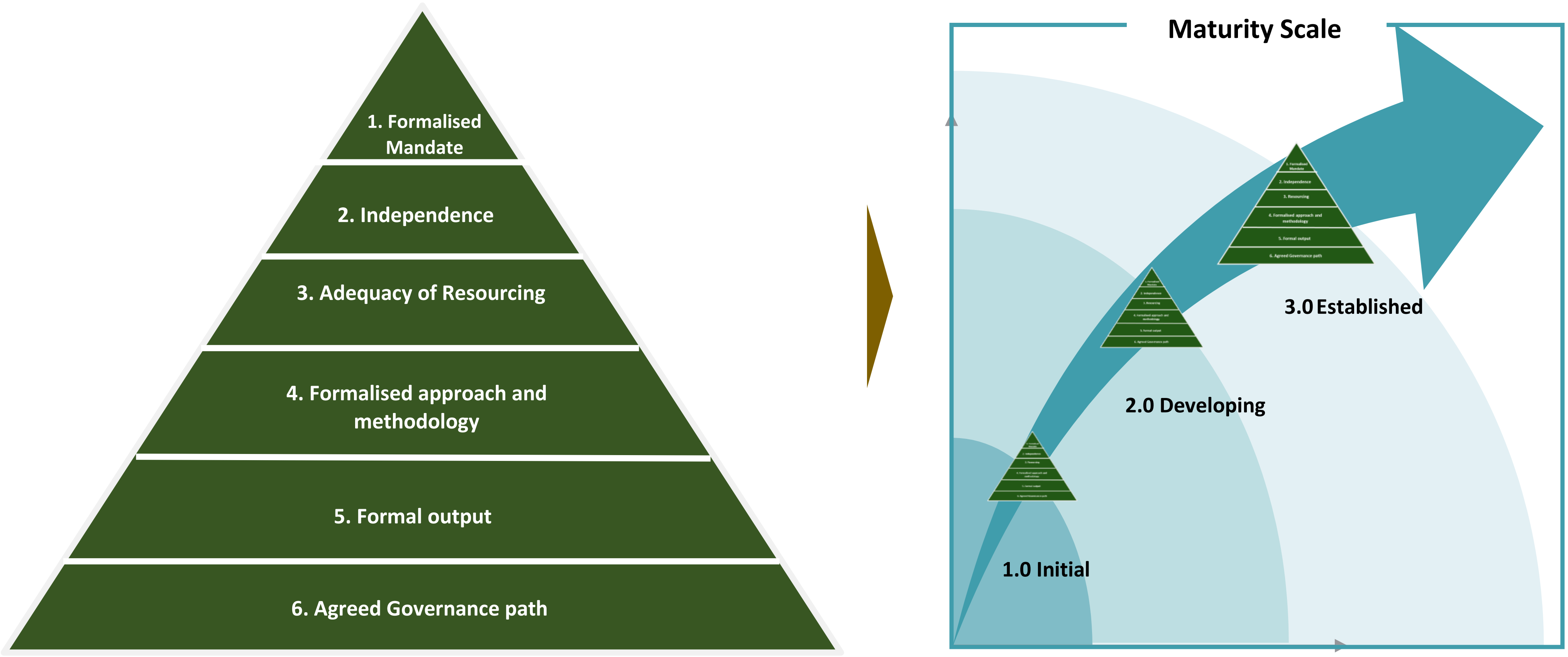
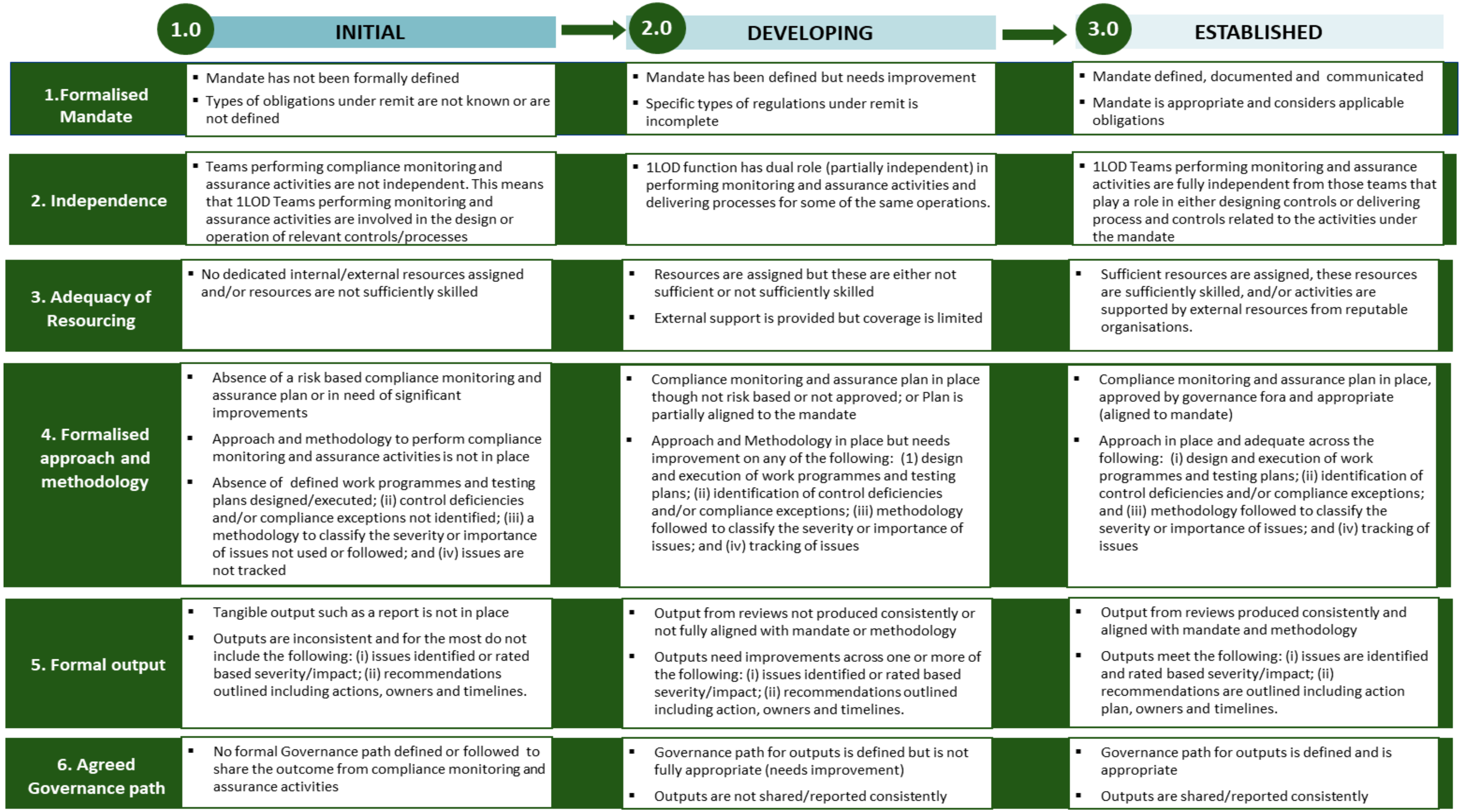


Figure 19. Maturity Criteria for FLOD

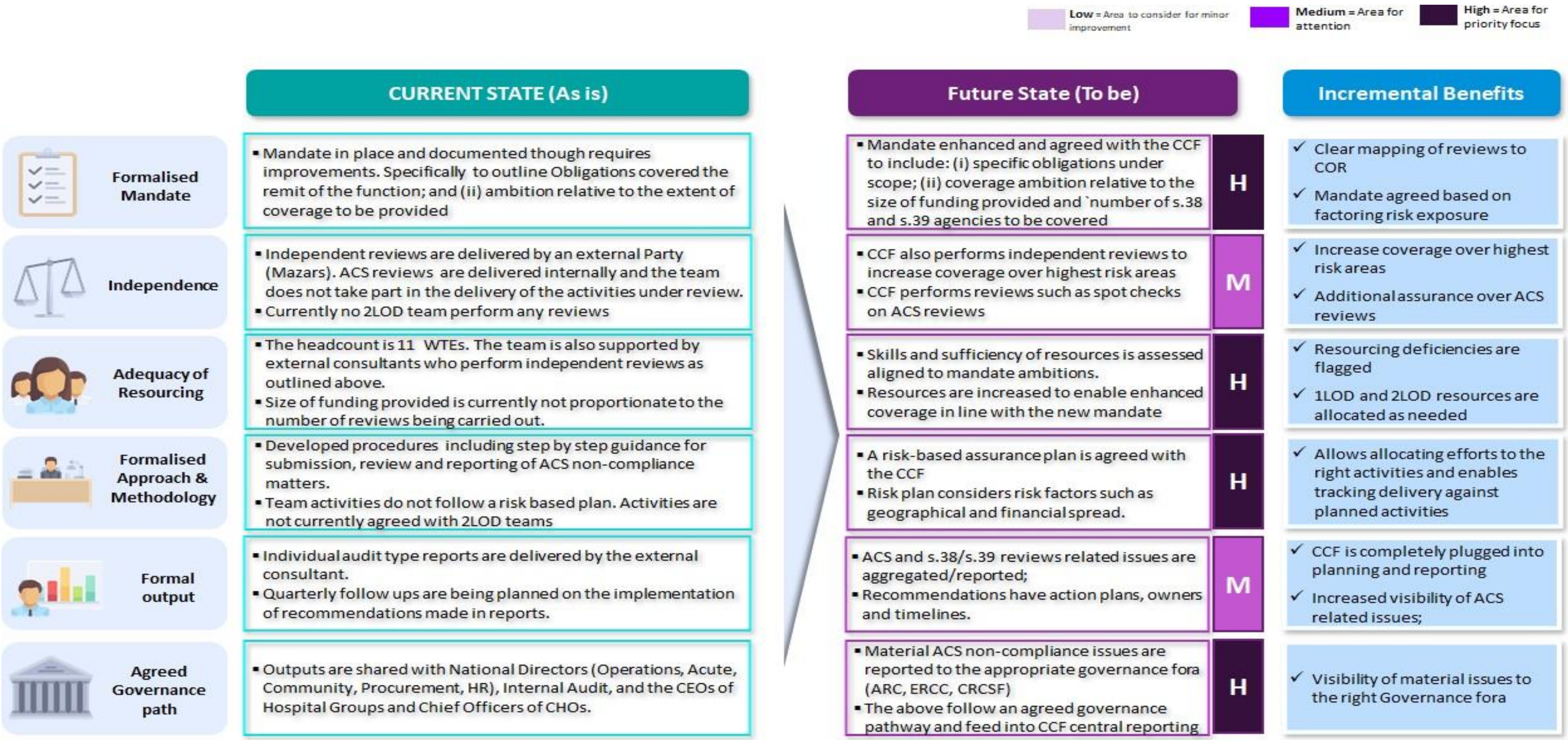


	1.0 INITIAL	2.0 DEVELOPING	3.0 ESTABLISHED
1.Formalised Mandate	▪ Mandate has not been formally defined ▪ Types of obligations under remit are not known or are not defined	▪ Mandate has been defined but needs improvement ▪ Specific types of regulations under remit is incomplete	▪ Mandate defined, documented and communicated ▪ Mandate is appropriate and considers applicable obligations
2. Independence	▪ Teams performing compliance monitoring and assurance activities are not independent. This means that 1LOD Teams performing monitoring and assurance activities are involved in the design or operation of relevant controls/processes	▪ 1LOD function has dual role (partially independent) in performing monitoring and assurance activities and delivering processes for some of the same operations.	▪ 1LOD Teams performing monitoring and assurance activities are fully independent from those teams that play a role in either designing controls or delivering process and controls related to the activities under the mandate
3. Adequacy of Resourcing	▪ No dedicated internal/external resources assigned and/or resources are not sufficiently skilled	▪ Resources are assigned but these are either not sufficient or not sufficiently skilled ▪ External support is provided but coverage is limited	▪ Sufficient resources are assigned, these resources are sufficiently skilled, and/or activities are supported by external resources from reputable organisations.
4. Formalised approach and methodology	▪ Absence of a risk based compliance monitoring and assurance plan or in need of significant improvements ▪ Approach and methodology to perform compliance monitoring and assurance activities is not in place ▪ Absence of defined work programmes and testing plans designed/executed; (ii) control deficiencies and/or compliance exceptions not identified; (iii) a methodology to classify the severity or importance of issues not used or followed; and (iv) issues are not tracked	▪ Compliance monitoring and assurance plan in place though not risk based or not approved; or Plan is partially aligned to the mandate ▪ Approach and Methodology in place but needs improvement on any of the following: (1) design and execution of work programmes and testing plans; (ii) identification of control deficiencies and/or compliance exceptions; (iii) methodology followed to classify the severity or importance of issues; and (iv) tracking of issues	▪ Compliance monitoring and assurance plan in place, approved by governance fora and appropriate (aligned to mandate) ▪ Approach in place and adequate across the following: (i) design and execution of work programmes and testing plans; (ii) identification of control deficiencies and/or compliance exceptions; and (iii) methodology followed to classify the severity or importance of issues; and (iv) tracking of issues
5. Formal output	▪ Tangible output such as a report is not in place ▪ Outputs are inconsistent and for the most do not include the following: (i) issues identified or rated based severity/impact; (ii) recommendations outlined including actions, owners and timelines.	▪ Output from reviews not produced consistently or not fully aligned with mandate or methodology ▪ Outputs need improvements across one or more of the following: (i) issues identified or rated based severity/impact; (ii) recommendations outlined including action, owners and timelines.	▪ Output from reviews produced consistently and aligned with mandate and methodology ▪ Outputs meet the following: (i) issues are identified and rated based severity/impact; (ii) recommendations are outlined including action plan, owners and timelines.
6. Agreed Governance path	▪ No formal Governance path defined or followed to share the outcome from compliance monitoring and assurance activities	▪ Governance path for outputs is defined but is not fully appropriate (needs improvement) ▪ Outputs are not shared/reported consistently	▪ Governance path for outputs is defined and is appropriate ▪ Outputs are shared/reported consistently

Appendix F. ‘As Is’ Operating Model vs ‘To Be’ Operating model

Two worked examples were developed to illustrate key features of the Current State and how these will be improved in the Future State in relation to the maturity of 1LOD functions performing compliance related monitoring and assurance activities. In doing so, we considered (i) the parameters defined in Maturity Scale (See Appendix E); (ii) interviews; and (iii) relevant documentation. Below are two examples to help illustrate benefits for the HSE once the future state of compliance operating model is in place. Example #1 relates to the Compliance Unit for Funded Agencies; and example #2 relates to Procurement.

Example # 1. Compliance Unit for Funded Agencies



Low = Area to consider for minor improvement | Medium = Area for attention | High = Area for priority focus

	CURRENT STATE (As is)	Future State (To be)		Incremental Benefits
Formalised Mandate	▪ Mandate in place and documented though requires improvements. Specifically to outline Obligations covered the remit of the function; and (ii) ambition relative to the extent of coverage to be provided	▪ Mandate enhanced and agreed with the CCF to include: (i) specific obligations under scope; (ii) coverage ambition relative to the size of funding provided and `number of s.38 and s.39 agencies to be covered	H	✓ Clear mapping of reviews to COR ✓ Mandate agreed based on factoring risk exposure
Independence	▪ Independent reviews are delivered by an external Party (Mazars). ACS reviews are delivered internally and the team does not take part in the delivery of the activities under review. ▪ Currently no 2LOD team perform any reviews	▪ CCF also performs independent reviews to increase coverage over highest risk areas ▪ CCF performs reviews such as spot checks on ACS reviews	M	✓ Increase coverage over highest risk areas ✓ Additional assurance over ACS reviews
Adequacy of Resourcing	▪ The headcount is 11 WTEs. The team is also supported by external consultants who perform independent reviews as outlined above. ▪ Size of funding provided is currently not proportionate to the number of reviews being carried out.	▪ Skills and sufficiency of resources is assessed aligned to mandate ambitions. ▪ Resources are increased to enable enhanced coverage in line with the new mandate	H	✓ Resourcing deficiencies are flagged ✓ 1LOD and 2LOD resources are allocated as needed
Formalised Approach & Methodology	▪ Developed procedures including step by step guidance for submission, review and reporting of ACS non-compliance matters. ▪ Team activities do not follow a risk based plan. Activities are not currently agreed with 2LOD teams	▪ A risk-based assurance plan is agreed with the CCF ▪ Risk plan considers risk factors such as geographical and financial spread.	H	✓ Allows allocating efforts to the right activities and enables tracking delivery against planned activities
Formal output	▪ Individual audit type reports are delivered by the external consultant. ▪ Quarterly follow ups are being planned on the implementation of recommendations made in reports.	▪ ACS and s.38/s.39 reviews related issues are aggregated/reported; ▪ Recommendations have action plans, owners and timelines.	M	✓ CCF is completely plugged into planning and reporting ✓ Increased visibility of ACS related issues;
Agreed Governance path	▪ Outputs are shared with National Directors (Operations, Acute, Community, Procurement, HR), Internal Audit, and the CEOs of Hospital Groups and Chief Officers of CHOs.	▪ Material ACS non-compliance issues are reported to the appropriate governance fora (ARC, ERCC, CRCSF) ▪ The above follow an agreed governance pathway and feed into CCF central reporting	H	✓ Visibility of material issues to the right Governance fora

Example # 2. Corporate Procurement Planning and Compliance Improvement

■ **Low** = Area to consider for minor improvement ■ **Medium** = Area for attention ■ **High** = Area for priority focus

	CURRENT STATE (As is)	Future State (To be)		Incremental Benefits
Formalised Mandate	▪ Mandate of the team has been recently documented as part the HSE Corporate Procurement Plan 2022-2024 ▪ Responsible for compliance improvement across Hospital Groups, CHO's, Section 38 and 39 Agencies and Corporate Services	▪ Mandate to also include: (i) specific obligations under scope; (ii) types of reviews and target coverage to be performed on contracts and expense returns for HGs, CHOs, Funded Agencies, etc	H	✓ Clear mapping of reviews to COR ✓ Mandate agreed based on factoring risk exposure
Independence	▪ Team provides support on self-assessments of expenditure over €20K and carrying out analysis of expenditures. ▪ Ad-hoc reviews were carried out by external consultants on self assessments made by budget holders in relation to expenditure. Currently no 2LOD team perform any reviews.	▪ CCF also performs independent reviews to increase coverage over highest risk areas ▪ CCF performs reviews such as spot checks of returns against the HSE central register of contracts for compliance	M	✓ Enhanced coverage over highest risk areas ✓ Additional assurance over procurement compliance
Adequacy of Resourcing	▪ Not fully known. The headcount is 30 WTEs. However, most of the WTEs are made up of business analysts not dedicated to compliance ▪ Ad-hoc support is also provided by external consultants (per above)	▪ Skills and sufficiency of resources is assessed aligned to mandate ambitions. ▪ Resources are increased to enable enhanced coverage in line with the mandate	H	✓ Resourcing deficiencies are flagged ✓ 1LOD and 2LOD resources are allocated as needed
Formalised Approach & Methodology	▪ Approach and methodology to perform compliance monitoring and assurance activities has been identified but not formalised. ▪ Risk based compliance monitoring and assurance plan is not in place. Activities are not currently agreed with 2LOD teams	▪ Approach & methodology to perform compliance monitoring and assurance activities is formalised. A risk-based assurance plan is agreed with the CCF on compliance with public procurement regulations	H	✓ Allows allocating efforts to the right activities and enables tracking delivery against planned activities
Formal output	▪ Areas of non-compliance associated with 2021 SIC reviews were examined. However, outputs are inconsistent and for the most do not include the following: (i) severity of the issues identified; (ii) recommended actions including owners and timelines	▪ Output from reviews are aligned with mandate and methodology ▪ Recommendations have action plans, owners and timelines.	H	✓ CCF is completely plugged into planning and reporting ✓ Enhanced visibility of non-compliance related issues;
Agreed Governance path	▪ Outputs are shared with the Head of Procurement, the Chief Financial Officer and with the ARC.	▪ Material non-compliance issues are reported to the appropriate governance fora (ARC, ERCC, CRCSF) ▪ The above follow an agreed governance pathway and feed into CCF central reporting	H	✓ Consistent visibility of material issues to the Governance fora ✓ Documented governance structure

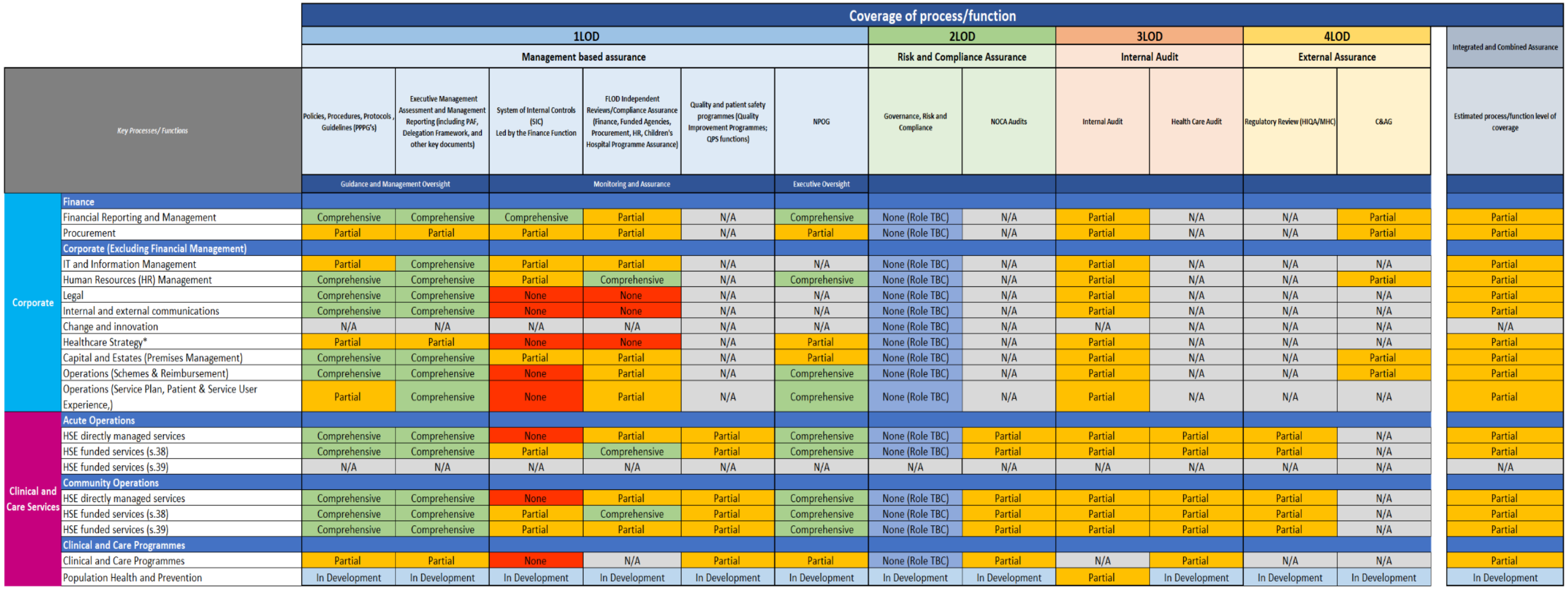
Appendix G. Four Line of Defence (4LOD) Integrated Assurance Map

A 4LOD Integrated Assurance Map was developed. In doing so, we considered (1) the context in which the HSE operates; and (2) how the 4LOD model can apply from a Corporate HSE perspective.

Our role in creating the HSE 4LOD Assurance matrix was to gain an understanding of other risk and compliance related monitoring and assurance activities that take place across the key HSE functions/process areas. **The assessment of the estimated process function coverage is solely based on the views of HSE interviewees and has been provided with no reference to a Compliance Obligations Register, as this is still in development. For the avoidance of doubt, KPMG did not perform any detailed review or testing of the key process, control or assurance activities of the HSE. Equally, KPMG did not provide a view on whether the assurance or coverage is appropriate, is designed appropriately or operateseffectively.**

Details of the coverage key and resulting outputs are appended in the Attached 2 documents and summarised below. Coverage key definitions are described on the following page.

Figure 20. HSE 4LOD Integrated Assurance map



		Coverage of process/function												
		1LOD						2LOD		3LOD		4LOD		Integrated and Combined Assurance
		Management based assurance						Risk and Compliance Assurance		Internal Audit		External Assurance		
Key Processes/ Functions		Policies, Procedures, Protocols , Guidelines (PPPG's)	Executive Management Assessment and Management Reporting (including PAF, Delegation Framework, and other key documents)	System of Internal Controls (SIC) Led by the Finance Function	FLOD Independent Reviews/Compliance Assurance (Finance, Funded Agencies, Procurement, HR, Children's Hospital Programme Assurance)	Quality and patient safety programmes (Quality Improvement Programmes; QPS functions)	NPOG	Governance, Risk and Compliance	NOCA Audits	Internal Audit	Health Care Audit	Regulatory Review (HIQA/MHC)	C&AG	Estimated process/function level of coverage
		Guidance and Management Oversight		Monitoring and Assurance			Executive Oversight							
Corporate	Finance													
	Financial Reporting and Management	Comprehensive	Comprehensive	Comprehensive	Partial	N/A	Comprehensive	None (Role TBC)	N/A	Partial	N/A	N/A	Partial	Partial
	Procurement	Partial	Partial	Partial	Partial	N/A	Partial	None (Role TBC)	N/A	Partial	N/A	N/A	Partial	Partial
	Corporate (Excluding Financial Management)													
	IT and Information Management	Partial	Comprehensive	Partial	Partial	N/A	N/A	None (Role TBC)	N/A	Partial	N/A	N/A	N/A	Partial
	Human Resources (HR) Management	Comprehensive	Comprehensive	Partial	Comprehensive	N/A	Comprehensive	None (Role TBC)	N/A	Partial	N/A	N/A	Partial	Partial
	Legal	Comprehensive	Comprehensive	None	None	N/A	N/A	None (Role TBC)	N/A	Partial	N/A	N/A	N/A	Partial
	Internal and external communications	Comprehensive	Comprehensive	None	None	N/A	N/A	None (Role TBC)	N/A	Partial	N/A	N/A	N/A	Partial
	Change and innovation	N/A	N/A	N/A	N/A	N/A	N/A	None (Role TBC)	N/A	N/A	N/A	N/A	N/A	N/A
	Healthcare Strategy*	Partial	Partial	None	None	N/A	Partial	None (Role TBC)	N/A	Partial	N/A	N/A	N/A	Partial
	Capital and Estates (Premises Management)	Comprehensive	Comprehensive	Partial	Partial	N/A	Partial	None (Role TBC)	N/A	Partial	N/A	N/A	Partial	Partial
	Operations (Schemes & Reimbursement)	Comprehensive	Comprehensive	None	Partial	N/A	Comprehensive	None (Role TBC)	N/A	Partial	N/A	N/A	Partial	Partial
	Operations (Service Plan, Patient & Service User Experience,)	Partial	Comprehensive	None	Partial	N/A	Comprehensive	None (Role TBC)	N/A	Partial	N/A	N/A	N/A	Partial
Clinical and Care Services	Acute Operations													
	HSE directly managed services	Comprehensive	Comprehensive	None	Partial	Partial	Comprehensive	None (Role TBC)	Partial	Partial	Partial	Partial	N/A	Partial
	HSE funded services (s.38)	Comprehensive	Comprehensive	Partial	Comprehensive	Partial	Comprehensive	None (Role TBC)	Partial	Partial	Partial	Partial	N/A	Partial
	HSE funded services (s.39)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Community Operations													
	HSE directly managed services	Comprehensive	Comprehensive	None	Partial	Partial	Comprehensive	None (Role TBC)	Partial	Partial	Partial	Partial	N/A	Partial
	HSE funded services (s.38)	Comprehensive	Comprehensive	Partial	Comprehensive	Partial	Comprehensive	None (Role TBC)	Partial	Partial	Partial	Partial	N/A	Partial
	HSE funded services (s.39)	Comprehensive	Comprehensive	Partial	Partial	Partial	Comprehensive	None (Role TBC)	Partial	Partial	Partial	Partial	N/A	Partial
	Clinical and Care Programmes													
	Clinical and Care Programmes	Partial	Partial	None	N/A	Partial	Partial	None (Role TBC)	Partial	N/A	Partial	N/A	N/A	Partial
	Population Health and Prevention	In Development	In Development	In Development	In Development	In Development	In Development	In Development	In Development	Partial	In Development	In Development	In Development	In Development

~Coverage level may change based on further validation/alignment

** includes Strategy, Appeals,Protected Disclosures, Children's First and former HBS Compliance*

Estimated Coverage Key				
Assessment of the coverage of the Four LoD activities over the key process / functions of the HSE	Comprehensive	Partial	None	N/A

First LoD

Comprehensive: There is a comprehensive complement of formally documented policies, procedures and management reporting in the process / functional areas.

Partial: There are some formally documented policies, procedures, and management reporting in the process / functional areas. However, they do not fully cover all the activities of the relevant process / function.

None: There are no formally documented policies, procedures, or management reporting in the process / functional areas over the activities of the relevant process / function.

N/A: The activities performed by the 1LOD are unrelated to the process / function and are not intended to provide any coverage over the process / function.

Second, Third and Fourth LoD

Comprehensive: A formal assurance output (such as a report) is produced and shared at appropriate HSE governance fora. Comprehensive coverage over the key activities of the relevant process / function is/shall be provided by the activities of the Second, Third or Fourth LoD assurance provider.

Partial: A formal assurance output (such as a report) is produced and shared at appropriate HSE governance fora. Some but not full coverage is /shall be provided over the key activities of the relevant process / function by the activities of the Second, Third or Fourth LoD assurance provider or the output of the external assurance is not reported internally at appropriate HSE governance fora.

None: The Second, Third or Fourth LoD assurance provider does not provide any coverage over the relevant function / process

N/A: The Second, Third or Fourth LoD assurance provider activities are not intended to provide any coverage over the process / function, or we have not been made aware of any assurance related activities.

Healthcare Strategy* process areas provides coverage to Strategy, Appeals, Protected Disclosures, Children's First and former HBS Compliance across this document.

4LOD Integrated Assurance Map. Octol

HSE 4LOD Integrated Assurance Map Ratior

Appendix H. Documentation Reviewed

We reviewed over 100 documents which relate to different elements of the HSE's current organisational set and operating model to manage compliance processes. See summary details below.

Table 2. Summarised list of documents

#	Document	Available
A	**Governance and Mandate**	
1	Compliance Governance Structure, including sub-committees and relevant working groups	Limited
2	Terms of Reference for the Board and Board level committees	Yes
3	Business Plans, Mandate, Goals and Objectives of the Governance and Compliance team	Yes
4	Governance and Compliance related Management Information/Strategic Scorecard reported to the Board, ARC, and other relevant fora.	Limited
B	**Organisation and Location**	
5	Current Organisation Structure, including functional areas across each Directorate	Yes
6	Delegation orders / Delegation of Authority Matrix and Delegation Policy Framework	Yes
C	**Activities and Processes**	
7	Compliance – Policy, Framework, Assurance Plan, Methodology, Risk Register, Reports	No
8	Compliance Risk Appetite Statements including limits and thresholds	No
9	Former HBS Compliance Framework	Yes
10	Quarterly Risk Reporting to Board/ARC/ EMT	Yes
11	Process/method to assess the effectiveness of Internal Controls	Yes
D	**Technology and Data**	
12	Repository of GRC tools and System	No
E	**People and Skillset**	
13	Skills matrix for compliance team and Compliance Training Plan	No
14	Compliance Team structure and headcount	Yes
F	**Performance Management**	
15	Performance and Accountability Framework	Yes
16	Success Measures/ KPI for Governance and Compliance function	No
G	**Other Documents for Assurance Activities**	
17	HSE Management Control Handbook, System of Internal Controls (SIC) process	Yes
18	Clinical Programmes and Clinical Audit	Yes
19	Corporate and National Service Plans	Yes
20	Policy and Procedure for ACS review of Funded Agencies, Performance Reviews	Yes
21	Incidents Management Policy Framework and Incident Report	Yes
22	Operating model (roles and responsibilities) of the Cosec and Legal Affairs	Yes
23	IT Governance for project, service desk with sample Report and Dashboard	Yes
24	Capital Manual and Protocol (roles and governance mechanism)	Yes
25	Procurement - Plan, Code of practice and report to ARC	Yes
26	Risk Management Policy, Report, Corporate Risk Register	Yes
27	Internal Audit Assurance plan, methodology, Reports (2021)	Yes

Contact us

The contacts at KPMG in connection with this report are set out below.

Patrick Farrell

Partner, Risk and Regulatory Consulting

M: + 353 87 0504029

E: patrick.farrell@kpmg.ie

Hermes Peraza

Director, Risk and Regulatory Consulting

M: +353 (0) 87 744 1981

E: hermes.peraza@kpmg.ie