Health Information Quality Authority (HIQA)

Review of the System of Internal Controls (SIC):
Internal Financial Controls &
Internal Control Questionnaire

Internal Audit Report for Review and Approval by the Audit, Risk & Governance Committee

11 January 2022

mazars

mazars

Contents

mazars

1. Executive Summary

In accordance with provision 1.8 of the Code of Practice for the Governance of State Bodies that came into effect in September 2016, *"The Board has responsibility for ensuring that effective systems of internal control are instituted and implemented including financial controls which also forms part of this review. The Board is required to confirm annually to the relevant Minister that the State body has an appropriate system of internal and financial control in place."* In its statement on the System of Internal Control the Board is also required to confirm that there has been a review of the effectiveness of the system of internal control.

The role of Internal Audit is to provide assurance to the Health Information Quality Authorities (HIQA) Audit, Risk & Governance Committee on its risk management, control, and governance processes in operation. Whilst the internal audit function has a key role in providing independent assurance on the effectiveness of elements of the System of Internal Control, the Board and management are specifically responsible for the design and implementation of the System of Internal Control.

This report set out the objectives for our high-level review of the internal financial controls, and internal control questionnaires of HIQA, which forms part of the overall assurance required by the Board.

1.1 Summary of Results

1.1.1 Internal Financial Controls

Our audit identified **no High Priority or Medium Priority** finding that requires immediate management attention. We identified **three Low Priority** findings which should be actioned when practicable which are detailed in Section 3. If implemented fully, these recommendations will further strengthen the existing system of internal control.

1.1.2 Internal Control Questionnaire

The Internal Control Questionnaire was completed by management and Internal Audit reviewed the responses provided. Our review did highlight any **High Priority** findings that requires immediate management attention. We identified **one Medium and three Low Priority** findings which should be actioned when practicable which are detailed in Section 4. If implemented fully, these recommendations will further strengthen the system of internal control.

The Internal Control Questionnaire, completed by management, is included in Appendix 1.

1.2 Audit Opinion

1.2.1 Internal Financial Controls Opinion

In accordance with the classification of audit opinion stated in section 2.4 below and with the exception of the identified payroll issue, the audit results indicate that **Reasonable Assurance** can be placed on the effectiveness and operation of internal controls to mitigate and/or manage one or more of those key inherent risks to which the financial activities are exposed.

mazars

The following table sets out the number of findings, summarised by priority ranking level:

Priority Ranking	Description	Number of Findings
High	A significant weakness which could compromise internal control and/or operational efficiency, potentially resulting in a substantial error, loss, fraud, or damage to reputation. Recommendations related to this observation require management action as a matter of urgency to ensure that the organisation does not continue to be exposed to an unacceptably high level of risk.	0
Medium	A control weakness which can undermine the system of internal control and/or operational efficiency. Recommendations related to this observation should be addressed in the short term to avoid exposing the organisation to significant or increased risk.	0
Low	A weakness which does not seriously detract from the system of internal control and/or operational efficiency, but which should nevertheless be addressed by management to improve internal control in general and ensure good practice. Recommendations related to this observation should be actioned when practicable to enhance the control environment.	3
Total		3

1.2.2 Internal Controls Assessment

The Internal Control Questionnaire was completed in the form of a self-assessment by management and reviewed by internal audit to establish (at a high level) whether evidence of controls reported by management is in place, and to summarise the results of the control questionnaires by management.

Based on our high-level review of the completed questionnaires, we have not identified any high priority items, but we have noted some areas for improvement.

The following table sets out the number of findings, summarised by priority ranking level:

Priority Ranking	Description	Number of Findings
High	A significant weakness which could compromise internal control and/or operational efficiency, potentially resulting in a substantial error, loss, fraud or damage to reputation. Recommendations related to this observation require management action as a matter of urgency to ensure that the organisation does not continue to be exposed to an unacceptably high level of risk.	0
Medium	A control weakness which can undermine the system of internal control and/or operational efficiency.	1

Priority Ranking	Description	Number of Findings
	Recommendations related to this observation should be addressed in the short term to avoid exposing the organisation to significant or increased risk.	
Low	A weakness which does not seriously detract from the system of internal control and/or operational efficiency, but which should nevertheless be addressed by management to improve internal control in general and ensure good practice. Recommendations related to this observation should be actioned when practicable to enhance the control environment.	3
Total		4

1.3 Acknowledgements and Limitations

We would like to thank all those members of management and staff in HIQA who assisted us in the course of our fieldwork.

Our review was conducted remotely and focused on specific areas (as detailed in Section 2.1) and was conducted based on interview, walkthroughs, document review and limited substantive testing (where possible) and may not necessarily disclose all significant matters relating to the current environment within the HIQA.

Our work, unless otherwise indicated, consisted principally of the review and analysis of information provided to us, discussions with staff and management of the HIQA, and a review of relevant policies and documentation. We have relied on explanations provided to us without having sought to validate these with independent sources. We have, however, satisfied ourselves that explanations received are consistent with other information furnished to us.

The contents of this report should be considered in the context of the following:

- The findings identified have been based on the information provided by HIQA.

- Limited substantive testing of the controls which are in place has been conducted, where possible.

- The findings and associated risks identified are not exhaustive and no assurance is provided that additional risks do not exist.

- This review is a point in time indication of the possible gaps which may exist within HIQA for the period 1 November 2020 to 31 October 2021.

Mazars assumes no responsibility in respect of or arising out of or in connection with the contents of this report to parties other than to HIQA. If others choose to rely in any way on the contents of this report they do so entirely at their own risk.

mazars

2. Terms of Reference

2.1 Audit Objectives and Scope

Under the 2016 Code of Practice for the Governance of State Bodies, the Board is responsible for ensuring that effective systems of internal control are instituted and implemented including financial controls which is the subject of this review.

Whilst the internal audit function has a key role in providing independent assurance on the effectiveness of elements of the system of internal control, the Board and management are specifically responsible for the design and implementation of the system of internal control, and for the overarching annual review of this system. This review approach is set down in the Code and further clarified in recently issued DPER guidelines, as follows:

- Management to complete assurance statements (in the case of HIQA through internal control questionnaires) to confirm the adequacy of internal controls currently in place

- Internal audit to review risk-based audit areas, including from time-to-time key areas where independent assurance may be required by the Board, such as financial control systems, risk management systems etc.

- Audit, Risk & Governance Committee to consider assurances received from management and internal audit, and consider the work of external audit, Board, and other subcommittees to inform its view of the internal control systems in place. On this basis, the Audit, Risk & Governance Committee should make a recommendation to the Board on whether the Statement on Internal Control prepared by management reflects the adequacy of the systems in place.

This internal audit function therefore performed a review of elements of the System of Internal Control, including financial controls, which then needs to be used by the Audit, Risk & Governance Committee (and the Board) to inform its own review of the effectiveness of the System of Internal Control. This assessment needs to be formally undertaken by the Board to satisfy itself as to the overall effectiveness of the System of Internal Control when considering the overall governance obligations.

This report will summarise the results of the review of internal financial controls and internal control questionnaires returned by management, for consideration by the Board as part of the review of the System of Internal Control for the period from 1 November 2020 to 31 October 2021. The main objectives of this assignment will be performed in two stages as described below.

Systems of Internal Financial Controls (SIFC)

Internal audit performed a high-level review of the System of Internal Financial Controls (SIFC) for the 2021 period, including confirming on a sample basis that the following key controls exist for the financial areas listed below;

- ➢ Income and Accounts Receivable management
- ➢ Payroll
- ➢ Travel and subsistence
- ➢ Fixed Assets
- ➢ Bank and Treasury Management

mazars

> ➢ Credit Cards
> ➢ Purchases, Procurement and Accounts Payable
> ➢ Management reporting and budgeting

Our audit work involved testing whether appropriate key controls exist and, if so, operate effectively. We reviewed and independently tested the underlying systems and key controls to form an opinion on the level of financial control risk in the system. All our work was performed in accordance with our understanding and interpretation of best practice applicable to HIQA.

Our testing was not designed to provide absolute assurance, and indeed sample-based testing would not provide this, but to provide a reasonable level of assurance that expected systems are in place and work in practice. Our work was performed through observation, questionnaires, walkthrough procedures, a series of meetings and discussions and independent audit testing.

Internal audit will continue to provide an overall opinion in respect of the internal audit of key financial controls. The responsibility for carrying out and monitoring these controls remains with HIQA management and staff.

Internal Control Questionnaire

We provided a high-level System of *Internal Control Questionnaire* ("ICQ") in a separate document, for completion by management (under delegated responsibility) to inform the overall Board assessment of the System of Internal Control. The completed ICQ is included in Appendix 1.

The questionnaire included a control self-assessment questions in the following areas (aligned to the Code):
- Procedures are in place to ensure an appropriate control environment exists within the organisation, such as clearly defined management responsibilities and evidence of reaction to control failures when necessary.
- Risk Management procedures are in place to identify business risks and to identify their financial impact.
- Major information systems are in place, such as budgets, and a means of comparing actual results with budgets during the year is in place.
- Procedures are in place for addressing the financial implications of major business risks, such as financial instructions and documented procedures, documented delegation of authority, segregation of duties and methods for detecting and preventing fraud.
- Procedures are in place to monitor the effectiveness of the internal control system, including management reporting.

Responsibility for the design and implementation of the system of internal financial controls remains the responsibility of the Board and management of the organisation. Our work consisted of the development of the internal control questionnaire (ICQ) and the performance of high-level, desktop-based validation of evidence relevant to the System of Internal Control framework as outlined by management.

As internal audit forms part of the overall system of control, it cannot provide an overall opinion in respect of the overall effectiveness of the system. Where potential medium to high-risk weaknesses is identified based on the completion of this questionnaire and verification of supporting evidence and documentation, we provided findings and recommendations which are aimed at enhancing the

mazars

System of Internal Control and informing the Board's own assessment of the effectiveness of the System of Internal Control.

Our report will not replace the Board's own assessment of the effectiveness of the System of Internal Control and should be used as an input into the Board's overall assessment of the effectiveness of the System of Internal Control.

The Board should define the process for the annual assessment to support its statement on internal control in the annual report and financial statements.

2.2 Audit Approach and Methodology

This review was delivered in line with the Mazars review methodology, and the specific approach developed for each review. We performed appropriate work to test whether the appropriate policies, processes, procedures, and key controls to ensure compliance with the policies and procedures exist and, if so, have been placed in operation.

Our review included the following:

- Review of relevant policies and procedures in place
- Interviews with management and staff to identify and evaluate internal financial controls
- Limited sample testing of key controls
- Preparation of draft report, including findings, recommendations and obtaining management responses

2.3 Reporting Arrangements

Draft audit findings were discussed in the form of a "closing meeting" with the key individuals. This meeting discussed the factual accuracy and risk associated with the findings identified and document provisional management responses. Subsequent to the completion of the closing meeting, a draft copy of the report was provided to Management for review and completion of management responses. The final draft report was presented to the HIQA Audit, Risk & Governance Committee.

2.4 Classification of Audit Opinion

The Internal Audit function will issue an opinion in its reports within the following assurance levels:

Assurance Level	Description
Substantial Assurance	Audit results indicate that substantial assurance can be placed on the adequacy and operating effectiveness of internal controls to mitigate and/or manage those inherent risks to which the activity under review is exposed.
	There is a sound system of governance, risk management and framework of internal control in place and the controls are being consistently applied to ensure risks are managed effectively which should ensure that objectives are fully achieved.
	The absence of high and medium priority observations means that normal on-going management supervision, together with the resolution of any findings raised in the audit report, should ensure that the control risk remains low.

mazars

Assurance Level	Description
Reasonable Assurance	Audit results indicate that reasonable assurance can be placed on the adequacy and operating effectiveness of internal controls to mitigate and/or manage those inherent risks to which the activity under review is exposed.

Overall, there is an adequate and effective system of governance, risk management and internal control. While some control risks were identified, this should not significantly impact on the achievement of objectives.

The disclosure of some high and/or medium priority observations means that normal on-going management supervision, together with the resolution of any findings raised in this report, should ensure that the control risk remains low. |
| **Limited Assurance** | Audit results indicate that limited assurance can be placed on the adequacy of and/or operating effectiveness of internal controls to mitigate and/or manage one or more of those key inherent risks to which the activity under review is exposed.

There is an inadequate and/or ineffective system of governance, risk management and internal control in place and there is a significant risk that the system will fail to meet its objectives.

The disclosure of a number of high and/or medium priority observations is indicative of increased levels of control risk. Prompt management action is required to address these observations together with increased managerial supervision and on-going oversight to ensure controls are being consistently applied and risks are managed effectively. |
| **No Assurance** | Audit results indicate that assurance cannot be placed on the adequacy of the and/or operating effectiveness of internal controls to mitigate and/or manage one or more of those key inherent risks to which the activity under review is exposed.

The system of governance, risk management and/or internal control has failed or there is a real and substantial risk that the system will fail to meet its objectives.

The disclosure of mostly high priority observations in combination with medium priority observations is indicative of heightened control risk. Urgent management action is required to address these observations together with increased managerial supervision and closer on-going oversight to ensure control risks are reduced. |

mazars

3. System of Internal Financial Controls - Detailed Findings and Recommendations

Items assigned a **High Priority** require **urgent** action, **Medium Priority** items require action in the **short term** and items assigned a **Low Priority** require action **when practicable**. See section 1.2 for a detailed description of each of the priority ratings assigned.

Findings	Risk and/or Implication	Recommendation	Management Comment
3.1 Non-competitive Procurement			**Priority: Low**
In the *Procurement Policy* in place for HIQA it is required that all non-competitive procurement for goods and services must be approved by the Chief Operations Officer and the Chief Executive Officer. We noted that, in line with good practice, HIQA does not have a "non-competitive procurement form" in place to record the supplier details, reasons/ justification for the non-competitive process and approval for the non-competitive procurement, including sole supplier procurement.	Risk that HIQA are not complying with Procurement guidelines to maintain detailed records of non-competitive procurement.	We recommend that HIQA consider introducing a formal non-competitive procurement form as part of the procurement procedures to record the supplier details, reasons/ justification for the non-competitive process and approval for the non-competitive procurement, including sole supplier procurement.	**Management Comment:** HIQA accepts this recommendation. **Agreed Action:** HIQA will included the suggested form into its procurement policy and procedure documents **Completion Date:** 28 February 2022 **Person Responsible:** Eleanor Noonan

mazars

Findings	Risk and/or Implication	Recommendation	Management Comment
3.2 Fixed Asset Disposals			**Priority: Low**
We reviewed the procedures in place for the disposal of fixed assets. Based on the testing of a sample of three fixed asset disposals we noted that for two samples the signed version of the disposal form could not be located. From discussion with management, this was an oversight due to working from home and numerous changes in personnel.	Risk of unauthorised disposal of a fixed assets where appropriate records of approval is not retained in line with procedures.	We recommend the following: a) That HIQA ensure that all fixed asset disposal forms are signed and retained. b) That a procedure is designed and implemented to accommodate signing of documents where these cannot be physically signed. These procedures could include the use of electronic signatures.	**Management Comment:** HIQA accepts that this finding relates to the misfiling of paperwork and change of personnel in the ICT area of the business. **Agreed Action:** The importance of this document will be highlighted again with the relevant area of business. Additionally, Finance will ensure that it receives a copy of this document after each disposal and will file appropriately. **Completion Date:** 31 January 2022 **Person Responsible:** Shay Fox and Eleanor Noonan

![mazars]

Findings	Risk and/or Implication	Recommendation	Management Comment
3.3 Version Control for Documented Procedures			**Priority: Low**
From reviewing the documented procedures, we noted that these documents are in word format and do not record the document owner and effective date in line with good practice.	Risk that unauthorised changes are made to procedures without proper review and approvals.	We recommend that HIQA consider the following: a) That procedure documents are made available in an un-editable format to reduce the risk of unauthorised changes in procedures. b) That each procedure document record at a minimum the implementation/effective date and the document owner who is responsible for updating the related procedures.	**Management Comment:** HIQA accepts this recommendation **Agreed Action:** Current procedures will be amended to have a separate document amend password and a section to reflect who and when the documents were amended. **Completion Date:** 30 April 2022 **Person Responsible:** Eleanor Noonan

4. Internal Control Questionnaire (ICQ) – Detailed Findings

We provided a high-level Internal Control Questionnaire ("ICQ") for completion by the HIQA management (under delegated responsibility) to inform the overall Board assessment of the System of Internal Control (SIC).

The SIC explains that the system of internal control is designed to manage rather than eliminate risk. The system can therefore only provide reasonable and not absolute assurance that assets are safeguarded, transactions authorised and properly recorded, and that material errors or irregularities are either prevented or detected in a timely manner. We also note that the ICQs represent a self-assessment and, while internal audit completed a high-level review of evidence to support the statements made, we have not completed an in-depth audit of the detailed controls noted.

The Board should define the process for the annual assessment to support its statement on internal control in the annual report and financial statements. Timely completion of the annual review is critical if it is to fulfil its objectives of providing assurance in relation to the operation of controls in the reporting period. The annual review should be conducted close to the end of the period under review or as soon as possible after the end of the financial period under review, and no later than three months after the period end. Our summary observations from our review of the Internal Control Questionnaires as completed by HIQA management are as follows:

Findings	Risk and/or Implication	Recommendation	Management Comment
███████████████			██████████
████████████████████ ████████████████████ ████████████ ████████████████ ███████████ █ ███████████ ██ █ ███████████████ ██	██████████████ ████████████ ████████████	██████████████ ████████████████ ███████████ ████████████████ █████████████	██████████████ █████████████████ ███████████████ ███████████████ █████████ ████████████████ ████████████████ ████████████████

Findings	Risk and/or Implication	Recommendation	Management Comment
			████████████████████ ████████ ███████████████████ ████████████████████ ████████ ████████████████████ ███████████ ██████████████ ████████████████████ ███████████████ ███████
4.2 Review of Documented Policies			**Priority: Low**
ICQ 2.2.8: Has the Board developed and implemented a suitable ethical framework, including related policies and procedures such as: • *Protected Disclosure Policy,* • *Code of Conduct for Board Members,* • *Code of Conduct for Employees,* • *Employee Handbook.*	In the absence of a regular review of policy documents, there is a risk that published policies may not be up to date.	It is recommended that the following documents are reviewed, updated as required and presented for formal approval: • Protected Disclosure last review in 2018 • Code of Conduct for Board Members & Employees last reviewed in 2017	**Management Comment:** HIQA accepts this recommendation. The Protected Disclosure Policy was due to be reviewed in Oct 2021 and this was concluded in December 2021. **Agreed Action:**

Findings	Risk and/or Implication	Recommendation	Management Comment
Whilst it was confirmed that these policies are in place, it was noted that the following policies have not been reviewed recently in accordance with good practice: • Protected Disclosure last review in 2018 • Code of Conduct for Board Members & Employees last reviewed in 2017 • Employee Handbook last reviewed in 2017		• Employee Handbook last reviewed in 2017	The remaining documents will be reviewed in 2022. **Timeline for completion:** 30th September 2022 **Action Owner:** Kathleen Lombard
4.3 Regular Review of User Access Rights			**Priority: Low**
ICQ 2.2.20: Do management review application user access rights periodically to ensure individual access rights are aligned with job responsibilities? *Are access rights immediately removed when an employee leaves the organisations?* *Are access rights immediately assessed if an employee moves department?* *Please provide most recent user access rights review.* Procedures are in place to remove system access of staff leaving the organisation and to assign appropriate access of new staff members.	In the absence of a regular review of user access rights of all staff members, there is a risk that staff may have inappropriate access to systems.	It is recommended that HIQA introduce a process for regular review and confirmation of user access rights of all staff members.	**Management Comment:** The current joiners, movers and leavers processes cover the removal of access rights when staff leave or change roles. The current process is being reviewed by BDO and will be updated in line with recommendations and also it will be aligned with the new draft access control policy. The new processes once defined and agreed will be formalised with HR and other stakeholders in HIQA. When implemented, the new processes will cover proper

Findings	Risk and/or Implication	Recommendation	Management Comment
A full review of user access has not been completed recently.			routine reviews to be conducted in future. **Agreed Action:** The JML process will be updated with the newly agreed access control policy. Access rights implementation in-line with the newly agreed process will be implemented as part of the strategic PRISM replacement and other future strategic projects (SharePoint, Teams, etc.) Existing systems review will be undertaken to determine a viable schedule for access rights. A new project request will be brought to PGB for prioritisation and implementation. **Timeline for completion:** Target date for the process documentation Q2 2022. Project request to PGB by Q2 2022. **Action Owner:** Information Governance and assurance Manager (Robert Lambert) and HR business operations

mazars

Findings	Risk and/or Implication	Recommendation	Management Comment
4.4 Internal Audit Charter			**Priority: Low**
ICQ 2.3.6: Is there a formal Internal Audit charter setting out the role of Internal Audit which has been approved by the Board / Subcommittee e.g. Audit & Risk Committee? An Internal Audit Charter is in place that was last reviewed in 2017. Based on management responses, it is understood that the charter will be subject to review in 2022.	There is a risk that the Charter does not reflect the current role if not reviewed and updated regularly.	It is recommended that the existing Internal Audit Charter is reviewed, updated as required and presented to the Audit, Risk & Governance Committee for approval.	**Management Comment:** HIQA accepts this recommendation and is aware that this document is overdue for review. **Agreed Action:** The Internal Audit Charter will be reviewed in Q 2, 2022 **Timeline for completion:** 30 June 2022 **Action Owner:** Kathleen Lombard

mazars

Appendix 1 Self-Assessment - Internal Control Questionnaire

2.2: Adequate steps are taken to ensure an appropriate control environment (such as clearly defined management responsibilities and evidence of reaction to control failures) exists within the organisation.
Note: Code of Practice for the Governance of State Bodies, Business & Financial Reporting Requirements Appendix D ("Appendix D") Statement on Internal Controls in a State Body, Section 3, vi)

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities and/or response to question(s)
1	Is there a formally documented organisational chart? (including Board and Board Subcommittees) If so, please provide.	Y	An organisational restructure project is currently underway so providing an org chart will not reflect current changing circumstances
2	Is there a formal term of reference in place for the Board and each Subcommittee? If so, please provide.	Y	
3	Does the Board have a formal schedule of matters specifically reserved for its decision to ensure proper direction and control of the organisation? If so, please provide.	Y	
	Has the Board delegated any authority to management in specific areas, and is this formally documented? If so, please provide.	Y	
4	Are there any key internal control areas where the organisation has not documented policies and procedures? Including but not limited to Finance, Risk Management, IT, HR etc.	Y	There are policies to be developed in relation to information security management and data classification as advised by BDO in the cyber controls review
5	Have key policies been recently reviewed, updated and approved to ensure that they reflect a remote working environment? Including but not limited to financial policies, IT policies and HR policies.	Y	A Remote Working Policy and a Right to Disconnect Policy were created to address remote working arrangements during the pandemic. These policies are reviewed and updated regularly and in line with government guidance.
6	Does the Board have arrangements in place to direct and monitor the overall control environment? Please provide evidence of the most recent Board pack and each of the most recent Subcommittee packs, including agenda, minutes and reporting items.	Y	Finance report, HR report, Corporate performance reports, risk reports are all standing items on the Board agenda. Significant items are overseen by the Board committee relevant to their remit. Risk and corporate performance are overseen at a more detailed level by the committees
7	Does the Board have adequate arrangements in place to identify and monitor adherence to all relevant legal and regulatory compliance obligations?	Y	Arrangements are being strengthened currently. New software module developed on Vision whereby each piece of legislation is recorded and reviewed (Statutory Compliance Directory). See attached Statutory Compliance Report.

mazars

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities and/or response to question(s)
8	Has the Board developed and implemented a suitable ethical framework, including related policies and procedures such as: • Protected Disclosure Policy, • Code of Conduct for Board Members, • Code of Conduct for Employees, • Employee Handbook.	Y	All of the documents mentioned in the question are in place
9	Were any breaches of control been identified within the reporting period? Such breaches might include non-compliance with procurement rules or instances where other elements of the control system (e.g. internal audit, Audit and Risk Committee or other committees) were not operational[1]. If yes, please explain.	Y	All minor – a standing item on the EMT agenda related to internal control failures where any issues are reported. Attaching copy of log of control failures for 2021.
10	Have there been any events or incidents giving rise to the need for disclosure of details of any material losses or frauds[2]?	N	
11	Are suitably defined human resources policies and procedures maintained, implemented and kept up to date in line with relevant legislation updates? Is there an Employee Handbook in place and do staff have easy access to it?	Y	A full suite of HR policies is available on the staff Intranet under Precision. These policies are reviewed as standard every 3 years or updated when required by legislative change. Or when scheduled There is no hard copy Employee Handbook in place, Staff members have ongoing access to all documents and are guided during HR Induction to key resources and policies as part of their standard induction programme
12	Is there a formal policy on remote working arrangements?	Y	Yes, as per question 5
13	Do all staff have a Contract of Employment?	Y	Contracts are issued as part of the formal on boarding process
14	Are job descriptions regularly updated to reflect a staff members role within the organisation? If so, what is the process in place for updating job descriptions.	Y	New Role Descriptions and templates are in place since 2020. These have been created to accommodate the new HIQA Competency Framework and role proficiency mapping. They are updated as required during the recruitment and selection cycle.

---

[1] Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body Section 3, ii)
[2] Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body Section 3, iii)

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities and/or response to question(s)
15	Are there procedures to ensure that HR records are maintained up to date for each employee? If so, please provide a short description on how HR ensure that records are up to date.	Y	A HRIS system is in place to manage staff member details. All staff members have access to their records through ESS and can amend certain data fields such as address etc. as required HRIS procedures are in place to manage the overall updating of employee records
16	Is there a formal, HR performance management system in place and operating fully throughout the period? If yes, please provide the policy for same. Does HR formally monitor completion of performance appraisals by staff within the organisation?	Y	Response provided above.
17	Has management implemented policies and procedures in relation to the objective of protecting data? Please provide the following: • Data Protection Policy • User Access Rights/Permissions Policy	Y	Full range of measures for protecting personal data in place. Liam McKenna of Mazars is currently HIQA's Data Protection Officer
18	Does the organisation have a suitably designed IT Disaster Recovery and Business Continuity Plan in place? Is all relevant financial and operational data backed up on an regular basis and periodically tested for recoverability? Please provide evidence of back-up and recoverability testing performed during the period.	Y	There is a disaster recovery plan and a range of business continuity plans in place covering each of the business areas. We have provided a copy of the disaster recovery plan. Relevant financial and operational data is backed up every night.
19	Has the organisation assessed the security controls in place in relation to employees accessing the network remotely? Is multi factor authentication in use for employees to gain access to the network?	Y	There is a policy covering remote working which is provided and covers how this is carried out. Staff can only use Fortinet VPN to gain access to the network, which requires two factor authentication using staff account/password and Symantec VIP access on mobile device. BDO security review assessed this. Note we can provide a review of the information of BDO security review in the same manner as being done for the cyber security audit.
20	Do management review application user access rights periodically to ensure individual access rights are aligned with job responsibilities?	Y	There are procedures covering joiners/movers leavers, where if an individual changes role then ICT should be notified by their manager so that access can be removed where required. When employees move department ICT should be notified by the manager of the old department that their access

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities and/or response to question(s)
	Are access rights immediately removed when an employee leaves the organisations? Are access rights immediately assessed if an employee moves department? Please provide most recent user access rights review.		should be removed and likewise the new manager should provide details of the required access for their new role. The joiners/movers/leavers process is currently being reviewed and updated with further improvements. Any staff leaving the organisation or going on extended leave will have their access rights suspended as a part of the Leavers process. A full review of all staff user access rights has not been recently carried out and it is recognised that this required when updated access controls are in place
21	Are there automated IT system controls in place to ensure that access to systems (e.g. passwords) by individuals are regularly changed for security purposes?	Y	Automated IT controls are in place to ensure that staff domain passwords must be changed every month.

2.3: Adequate processes are used to identify business risks and to evaluate their financial implications?

Note: Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body, Section 3, vii)

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities
1	Does the Board approve the Strategic Plan and annual Business Plans? Are realistic goals and measurable key performance indicators set for both the Strategic Plan and annual Business Plans?	Y Y	These come to the Board for approval
2	Is there a documented risk management policy / framework in place that was formally approved by the Board? If so, please provide. Is there a documented risk appetite statement? If so, please provide.	Y Y	There is a risk management policy and a risk management handbook in place. Both were approved by the ARGC in 2020. HIQA's risk appetite statement was reviewed by the Board in 2020
3	Is there a formal process in place for identifying and reviewing risks related to each of the organisations established objectives? Are these risks formally identified and documented in a Risk Register?	Y Y	All team, directorate and team risks are logged on HIQA's risk register (Vision). Risks are linked to a strategic or business plan objective on the risk register.
4	Are these risks regularly monitored, reviewed and updated by management and reported to the Board / Subcommittee? Please confirm how often and provide evidence of such reporting during the period.	Y	Standing item on Board and Committee meetings
5	Are specific risk incidents captured, monitored and reported upon, including their financial implications (if any)? If so, please evidence of same.	Y	No specific case, but facility is there
6	Is there a formal Internal Audit charter setting out the role of Internal Audit which has been approved by the Board / Subcommittee e.g. Audit & Risk Committee?	Y	IA charter in place, approved by Board – for review 2022
7	Is the internal audit plan risk based and implemented to provide assurance in respect of key risks impacting the organisation?	Y	IA has Meetings with EMT and ARGC
8	Does the Internal Audit function have defined reporting arrangements and access with the Board / Subcommittee e.g. Audit & Risk Committee?	Y	Terms of reference specifies this

mazars

2.4: Major information systems are in place such as budgets, including means of comparing actual results with budgets during the year

Note: Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body, Section 3, viii)

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities
1	Are year-end/period-end close off processes in place? Are these processes and timelines documented?	Y	Yearend close operates to the same time scale as regular month ends (10 W/D). Once audit date is agreed, an internal schedule of key activities and dates regarding board review/approval, audit clearance and audit cert issuance, all designed so that HIQA can publish its Annual Report in compliance with Health Act.
2	Does the organisation (*for State Bodies*) submit draft unaudited financial statements to its parent Department, no later than two months after the end of the relevant financial year?	N	Draft Financial Statements (FS) are issued in accordance with Health Act stipulations rather than Code of Practice. Final audited FS are presented to the Minister of Health via HIQA@s Annual Report, as per Health Act 2007
3	Is there an annual business planning and annual budgeting cycle in place?	Y	Yes. Any further information requested can be supplied.
4	Is the annual budget approved by the Board? Please provide the most recent budget and evidence of Board approval.	Y	Minutes of Board meeting 24 march
5	Are approved budgets communicated to all budget holders? Do budget holders have timely access to financial reporting against budgets?	Y	Actual versus Budget spend reports are issued to Budget holders each month, with finance follow up on variances, expected future spend etc.
6	Is actual vs budgeted spend monitored, variance explained and reported during the year, including reporting to the Board/ Subcommittee? If so, how often and who is responsible for the preparation and approval of these reports?	Y	Actual versus Budget spend reports are issued to EMT and budget managers on a monthly with a monthly finance presentation on same by Finance Manager. Regular reporting and finance updates are presented to ARGC and Board by Chief Operations Officer as per meeting schedule.
7	Were budgets and forecasts updated throughout the year to reflect changing conditions such as market conditions, competing priorities, resource allocations, etc? If so, were these budgets and forecasts changes approved by the Board/ Subcommittee?	Y	A revised budget is generated usually to capture expected spend for the last 4 months of the financial year, but it was for 6 months in 2021. An expected out-turn for 2021 was presented by Finance to EMT and ARGC in November 2021.

2.5: The procedures for addressing the financial implications of major business risks

Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body, Section 3, ix)

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities
1	Does the organisation's risk assessment process identify any major business risks such as strategic risks, compliance risks, operational risks, financial risks, and reputational risks? If so, how are these reported, to whom, and how often during the year?	Y	Board reports – standing item Committee reports – standing item EMT – regular full reviews Risk workshop for Board
2	Is accountability for major business risk exposures established through a clear policy structure and effectively designed procedures, metrics, measuring, and monitoring procedures?	Y	Risk management policy and handbook
3	Has the organisation put in place financial delegation practices such as authorisation limits, segregation of duties and methods of preventing and detecting fraud? Please explain.	Y	Financial delegation has been incorporated into HIQA's Finance system (Integra) where possible, with support from Finance's process and procedures documents. Segregation of duties with Finance have been implemented where possible as part of standard operating procedures.
4	Were there any material re-statements of the company's financial statements in the past 2 years which have financial implications for the overall business?	Y	Clean Audit Certificates for 2019 & 2020
5	Are major transactions, related party transactions, off-balance sheet activities, and other material events disclosed (if any)?	Y	Clean Audit Certificates for 2019 & 2020
6	Has the organisation obtained independence assurance in respect of the key financial controls operated by the organisation, including the procedures for addressing the financial implications of major business risks?	Y	Annual IFC audit in HIQA's Internal Auditors
7	Are early warning systems in place to both prevent and detect variance from budgets so that the financial implications of major business risks are addressed? If yes, please explain in detail the process in place.	Y	Actual spend Vs Budget/Revised Budget sent to seniors' manager on a monthly basis, with active analysis and input from Finance Business Partners Variance reporting is also presented to EMT monthly with major variances identified with explanations. Similar process for ARGC and Board on agreed intervals.

mazars

2.6 : Adequate procedures are in place for monitoring the effectiveness of the internal control system

Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body, Section 3, x)

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities
1	Has the Board defined the actual system of internal control in place within the organisation? Is an annual review of the effectiveness of the system of control conducted in line with the Code's requirements[3]?	Y Y	Process whereby each committee reviews the controls for the areas for which they have oversight responsibility. ARGC prepares a report for the Board
2	Does the Board meet regularly to discharge its duties effectively? Please provide a listing of the number of Board meetings held during the period and whether they were held in person or remotely. Please provide minutes for first and last meeting held in the period.	Y	The Board must meet 6 times according to the Act. In addition, the Board met 5 times to progress discrete items of business. There were also 3 strategy sessions of the Board All meetings were help remotely in line with public health advice
3	Has a remote working environment presented any major issues in relation to the overall engagement of Board members or attendance at Board meetings?	Y	Attendance and contribution not affected – very healthy engagement
4	Has a remote working environment presented any major issues in relation to engagement with employees and performing operational activities in aiming to achieve the organisations objectives?	Y	No major issues have emerged to date. Staff surveys have also been conducted during the pandemic to ensure staff members can provide feedback and raise concerns on all aspects of remote working.
5	Is there a formally documented process in place for setting the organisations strategy? If not, please provide an overview of the key steps involved.	Y	
6	Is implementation of the organisation's strategy subject to monitoring controls? If so, please provide evidence of the most recent strategic implementation monitoring report provide to the Board.	Y	Corporate performance report is a standing item. A full report is provided twice annually – an exception report is provided at the other 4 statutory required meetings Annual strategy sessions of the Board
7	How does the Board evaluate its own performance and each of its sub-committees? Please provide evidence of the latest evaluations performed.	Y	Board evaluation and committee evaluations about to commence for 2021 SWiFT governance review 2020 External evaluation 2019

---

[3] Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body Sections 1, 2 and 3

mazars

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities
8	Are the terms of appointment of Board members monitored to ensure compliance with the terms set in the Code? Has the Board assessed the 2020 update to the Code with respect to Gender Balance, Diversity and Inclusion?	Y Y	Update to ROC January 2021 Board membership log maintained
9	Did internal audit reporting in the period communicate any material or significant issues to be remediated? If so, please provide managements latest update on the remediation of same.	N	
10	Does the Board / Subcommittee monitor management's response to findings and recommendations identified by the IA function and/or external auditors? If so, please provide evidence of same	Y	Follow up reviews
11	Does the organisation have a Fraud Management Policy in place?	Y	
12	Have management identified fraud risk factors, including the potential for any override of controls? Does the organisation have a Fraud Risk Register, and does it carry out fraud risk assessments? If so, please provide evidence of same.	Y Y	Anti-fraud and Corruption Policy in place Anti-Fraud and Corruption Standard Operating Procedure in place Fraud and Corruption Risk profiling workshop held in August 2020
13	Has the organisation carried out a specific fraud risk assessment focused on the impact of hybrid/remote working?	Y	The finance team looked at the pre "WFH internal controls" in 2020 (shortly after it was clear that WFH was going to be a longer-term thing) and agreed what working internal financial controls should be in the remote working environment and amended the finance procedures accordingly. It especially looked at electronic approval and electronic documentation, reflecting the team WFH. It covered off what the team should do differently, so as to ensure that internal financial controls were sufficient and appropriate.
14	Has the organisation issued guidance to staff with respect to remote working and ensuring data and access to data is stored in a controlled environment and kept confidential at all times?	Y	
15	Has the organisation made changes to the internal controls in place in relation to approvals such as digital signatures, email approvals etc.?	Y	In finance function there was very limited reliance of hard copy or physical signatures even before pandemic: • On lines expense system • Electronic PO creation and invoice approval

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities
			• Electronic backing
			Certain checks that would previously have been evidence by signature now verified by email since remote working during pandemic.
			In Regulation Directorate an electronic signature system is now in place.
16	In the last two years, have there been any weaknesses in internal control which have resulted in material losses, contingencies or uncertainties? If so, please outline for the purpose of disclosure in the financial statements.[4] Please also outline any actions taken or intended to be taken to correct the weaknesses or an explanation of why not action is considered necessary[5]	N	Not Applicable
17	Please consider the following additional sources of assurance (where applicable) and the extent to which any of their activities or reporting indicate any potential material or significant issues which need to be highlighted to the Board and which may impact upon the effectiveness of the system of internal control:		
17.1	Any compliance reporting, including (but not limited to) protected disclosures, Health and safety & freedom of information reporting?	Y	H&S reports and a standing item on Board agendas Protected disclosure – annual accounts chairpersons report FOI – comms assurance report
17.2	Management reporting to the Board?	Y	CEO's Report Corporate Performance Report and HR Risk Report Financial Performance Reports … are standard reports to the Board at their meetings and will, if appropriate indicate any issues which may impact upon the effectiveness of the system of internal control
17.3	Procurement - Is there a Procurement Plan in place with regular reporting? In the last two years, has there been any departure from procurement rules and guidelines as set out by the Office of Government	Y	Supplied previously

---

[4] Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body Section 5

[5] Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body Section 6

No.	Control Self-Assessment Question(s)	Management Response (Yes / No)	Brief outline of activities
	Procurement[6] which require disclosure in the annual financial statements? If none, please state none. If any departures, please outline.		
17.4	Sub-committee reporting?	Y	Committee reports to the Board
17.5	Any other third-party consulting, audit or inspection reports specific to the organisation?	Y	Information Division commissioned reports on cyber security and penetration testing (BDO reports) Operations commissioned a report on the finance function - Grant Thornton report Board Secretary commissioned a governance review - SwiFT Governance report (positive report) HIQA HR has engaged with the NSAI and participated in the Excellence Through People programme for the last 6 years. We have achieved Platinum Certification in the last number of weeks following a recent full audit
17.6	Any other sources of assurance specific to the organisation? (please list)	Y	As above
18	Are suitable arrangements in place to ensure that the Statement on the System of Internal Control is reviewed[7] by the: i) Audit & Risk Committee ii) External auditor	Y	Meetings in Feb and April

---

[6] Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body Section 7

[7] Code of Practice for the Governance of State Bodies, Appendix D Statement on Internal Controls in a State Body, 3, iv) and v)

mazars

Contacts
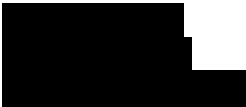
Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.ie