Health Information and Quality Authority

Cyber Security Audit

High Level Overview

Internal Audit – Final Report

March 2022

mazars

mazars

Contents

mazars

1. Executive Summary

The role of Internal Audit is to provide assurance to the Health Information and Quality Authority ('HIQA') Audit, Risk and Governance ('ARG') Committee on its risk management, control and governance processes in operation. For each audit we identify and critically evaluate the framework and controls in place and highlight in our report potential weaknesses that become apparent as a result of our work. We obtain comments and agreed action plans from appropriate management and staff for each weakness identified.

This document sets out the results of the internal audit completed in the area of cyber security with a focus on remote working in line with the scope and objective set out in Section 2.2 below.

Cyber Security has become one of the main risk areas to organisations of all sizes globally. On a daily basis organisations are victims of cyber-attacks impacting the availability, confidentiality and integrity of business data and systems. Cyber-attacks now have far-reaching economic consequences to organisations; beyond financial, reputational and legal ramifications. No industry is immune.

User awareness of the continuously changing cyber security threat (such as: malicious emails, attachments and links), is a key control that organisation should be implementing to reduce the risk of attack. As such this review will examine the level of user awareness training in operation.

Security monitoring and ability to respond to an incident in a defined manner is also critical to reducing the impact and ensuring that services are restored to a secure and normal state efficiently. This review will test the adequacy of IT security monitoring solutions in place as well as conducting a review of the incident management process.

As a result of the Covid-19 pandemic organisations have been forced to further develop and implement remote working solutions to enable staff to continue operating. Current cyber security trends have identified an increase in exploitation of vulnerabilities in remote working solutions that were implemented during the Covid-19 pandemic. Exploitation of security vulnerabilities in remote working solutions could result in unauthorised access to organisations network impacting the confidentiality, integrity and availability of data and systems. In addition, the inability to access the organisations network remotely due to a failure and/or cyber-attack could impact their ability to operate.

Areas of good cyber security practices:

- Enabling of Multi-Factor Authentication (MFA) to applications and services adding an additional layer of defense
- Continuous review and management of third-party service provider
- Baseline security awareness training conducted within the organisation

[redacted]

1.2 Audit Opinion

In accordance with the classification of audit opinion stated in section 2.4 below, audit results indicate a **Reasonable Assurance level** i.e. "*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. 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.	3
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		6

1.3 Acknowledgements and Limitations

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

Our review was focused on specific areas (as detailed in Section 2.1). Our work, unless otherwise indicated, consisted principally of the review and analysis of information provided to us, discussions with staff and management of HIQA, walkthroughs, review of relevant policies and documentation and limited substantive testing (where possible) and may not necessarily disclose all significant matters relating to the current environment within HIQA. 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.

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.

2. Terms of Reference

2.1 Audit Objectives and Scope

The overall objective of this internal audit was to provide the audit committee with reasonable, but not absolute, assurance as to the adequacy and effectiveness of cyber security controls in operation at the network perimeter to protect the organisations internal network and critical applications from a malicious cyber-attack.

This audit was based on the following control objectives related to the cyber security of the HIQA internet facing services:

- Existence, adequacy and operational effectiveness of network security monitoring and detection controls in the following areas:
    - Web filtering controls
    - Mail filtering controls
    - Intrusion detection controls
    - Anti-virus and malicious code detection
- Review the existence and adequacy of authentication controls (on a sample basis) to ensure that remote access to the HIQA network restricts unauthorised access (including third party access).
    - Identify all of the remote access and internet facing services in operation with HIQA.
    - Review the authentication controls for each of solutions identified: -
        - Password
        - Multi factor Authentication
        - IP Restrictions
    - For each of the solutions test to ensure that all remote access is approved, modified and removed in defined manner.
- Existence and adequacy of user awareness training in operation to ensure that all HIQA staff and contractors are made aware of the current cyber-security and remote working threats.
    - Obtain and review that adequacy of the Cyber Security user awareness training program with HIQA.
        - Periodic training
        - Continuous update of current threats
        - Bespoke training for senior management
    - Quantify the level of attendance to HIQA cyber security training
- Existence and adequacy of an incident management process to ensure that threat is contained, source of attack is identified, and remediation controls are implemented to prevent further attacks.
    - Obtain and review the cyber incident management process in place within HIQA
- Existence and adequacy of a security vulnerability management process to ensure that security vulnerabilities are identified and remediated within an appropriate timescale

  - Obtain and review the security vulnerability patch management processes in place with HIQA. At the following levels:
    - Server,
    - Desktop
    - Network devices
  - Review configuration of any centrally managed vulnerability patch management solutions to ensure that HIQA devices are kept up to date and the HIQA has an adequate level of oversight.

- Security vulnerability testing is conducted on a periodic basis for both the internal and external (including client hosting environments) information technology environments. All vulnerabilities are reviewed, risk assessed and where possible remediated.
  - Determine frequency of security vulnerability testing of HIQA internal and external services.
  - Confirm that network security vulnerability tests are being conducted on a periodic basis in line with an appropriate scope.
  - On a sample basis test the remediation process to ensure that all vulnerabilities identified by network security vulnerability tests are reviewed, prioritised and remediated within an adequate timescale.

2.2 Audit Approach and Methodology

Our audit work involves testing whether appropriate key controls exist and, if so, operate effectively. We will evaluate and test the underlying systems and key controls to form an opinion on the control risk in the system. All of our work is performed in accordance with our understanding and interpretation of best practice applicable to HIQA.

Our testing is not designed to provide absolute assurance, and indeed sample-based testing would not provide this, but to provide a reasonable level of assurance that the policies are in place and comply with relevant legislation. Our work will be performed through, observation, documentation review, a verification interviews and independent audit testing

All work carried out will be performed in accordance with an understanding of the proper interpretation of the law and in accordance with best practice within HIQA. Testing is designed to provide reasonable but not absolute assurance that expected controls are in place and work in practice

Work will be completed remotely. Conducting onsite testing will be subject to the feasibility of HIQA being able to provide a safe working environment which adheres to existing government guidelines and Covid-19 related recommended work practices.

2.3 Reporting Arrangements

Draft audit findings were discussed in the form of a “closing meeting” with the relevant key individuals. This meeting involved the discussion of the factual accuracy of 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 report will be presented to the HIQA ARG 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.
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.