Audit and Risk Assurance Committee

10 November 2021

Internal Audit Progress Report 2021-22

Executive Summary

This report summarises the progress so far regarding the delivery of the internal audit plan for 2021/22.

Previous consideration	The Committee reviews the Internal Audit Progress Report at each meeting
Decision	To note
Next steps	The Committee will receive update reports at each meeting on the progress of the Plan.
Strategic priority	All
Risk	All
Financial and resource implications	None as a result of this report
Author	BDO LLP

INTERNAL AUDIT PROGRESS REPORT FOR THE 2021/22 AUDIT PLAN

HEALTH AND CARE PROFESSIONS COUNCIL

CONFIDENTIAL
STATUS - FINAL

NOVEMBER 2021

IDEAS | PEOPLE | TRUST

BDO

1. Internal Audit Progress Report

Introduction

2.1 This report summarises the progress so far regarding the delivery of the internal audit plan for 2020/21. The Audit & Risk Assurance Committee is requested to note this report. We also include in the Appendix, a recently-published BDO article focussing on Data Privacy considerations for the Not for Profit Sector.

Delivery of the plan

2.2 Fieldwork for the Safeguarding Controls audit has concluded with preliminary findings fed back to management. Scoping meetings for the remaining audits have either been held or have been planned.

Changes to the plan

2.3 There are no changes to the plan since our previous update to the Audit & Risk Assurance Committee in September 2021.

External Quality Review

2.4 Our internal audit practice has been subject recently to an external quality assessment (EQA) by the Chartered Institute of Internal Auditors. The global standards of the Institute of Internal Auditors (IIA) requires every internal audit function that aims to comply with its standards to be reviewed, externally, every five years.

2.5 BDO recognises the importance of independent quality assurance and so submitted its Risk and Advisory Services (RAS) team to an External Quality Assurance (EQA) review in April 2021. In summary, their conclusion was that BDO generally conforms to the International Professional Practices Framework (IPPF) and Public Sector Internal Audit Standards (PSIAS). This is the highest of the three grading's awarded by the CIIA.

Assignment title	Output type	Period	Status	Proposed Audit Committee Date
Risk Management	Assurance	Q1	Final Report	September 2021
Safeguarding Controls	Assurance	Q3	Fieldwork Completed	March 2022
Registrations Payment Processes	Assurance	Q3	Scheduled	March 2022
Key Financial Controls	Assurance	Q3	Scheduled	March 2022
Digital Transformation Benefits Realisation	Assurance	Q4	Scheduled	June 2022
Education	Assurance	Q4	Scheduled	June 2022
Follow up	Assurance	Q4	Scheduled	June 2022

Development of Internal Audit performance questionnaire

2.6 We are developing a performance questionnaire to be used to measure the effectiveness of our Internal Audit service to HCPC. We welcome management's and Audit & Risk Assurance Committee's input as to the content of the survey, and whether the survey should be completed per assignment or time period (e.g. quarterly). Questions within the survey will be scored 1-5 and allow narrative commentary against answers. The proposed questions are set out at Appendix 2.

Appendix 1: DATA PRIVACY CONSIDERATIONS FOR THE NOT FOR PROFIT SECTOR

The UK GDPR is a regulation, not a project. Three years on from the UK enshrining GDPR into UK law as the Data Protection Act 2018, many not for profit organisations are reviewing current levels of compliance. Whilst a considerable amount of work was completed across the sector in the lead up to the GDPR 'go-live' date in May 2018, there is a requirement to demonstrate continued compliance with its regulatory requirements. But what does this mean in practice?

This article sets out key considerations for the sector to ensure that you remain up to date with continued data privacy compliance requirements:

1. Has your Article 30 Record of Processing Activity (ROPA) been recently reviewed and updated, to accurately reflect data processing activity? The ROPA forms the foundation of your GDPR governance and compliance, and should be regularly reviewed and updated to reflect changes in data processing activity, and demonstrate accountability and oversight of data processing at your organisation.

2. Have privacy notices been updated to reflect changes in the ROPA? Transparency is a key principle of GDPR, and data subjects have the right to be informed about the collection and use of their personal data. If privacy notices are not regularly reviewed and updated to reflect changes in data processing, then organisations are unlikely to be accurately communicating data processing activity to data subjects.

3. What are the levels of employee awareness of GDPR requirements? Whilst a lot of work was done in 2018 to deliver GDPR awareness training to employees, staff training should be periodically refreshed and updated, to ensure that they are familiar with key internal processes, especially where strict time limits apply, i.e. data breaches and subject access requests. In addition, data protection is a constantly evolving field, so employees need to be aware of relevant recent developments, for example in relation to international data transfers.

4. Do you have full oversight of data protection risk in the supply chain risk? Sharing personal data with third parties, inevitably exposes organisations to risk. This is why it remains crucial for organisations to maintain full oversight of data processors and joint controllers, and crucially, their location to ensure that appropriate data processing provisions are written into contracts, and both parties are clear about their responsibilities in the event of a subject access request or data breach. Recent changes in data protection law including the invalidation of the Privacy Shield, has meant that organisations need to seek an alternative safeguard in relation to transfers of personal data to processors located in the US, so it remains important to be aware of which Non EU/EEA countries you may be sharing personal data with.

5. Do you have full oversight of data processing, which relies on consent or legitimate interest as the lawful basis for processing? Are consent management arrangements in line with GDPR requirements? Remember, individuals have the right to withdraw consent at any time, at which point the data processing should cease. If organisations are relying on consent as the lawful basis for processing then there should be internal infrastructure in place to support this. Have legitimate interest assessments (LIAs) been completed for data processing activity which relies on legitimate interest?

6. Are key data protection policies and procedures regularly reviewed and updated to accurately reflect current processes? To demonstrate continued compliance with GDPR requirements, it is really important to ensure that key policies and procedures are regularly reviewed and updated to ensure that they remain up to date and reflect current practice.

7. Have Data Protection Impact Assessments been embedded into centralised processes? The GDPR requires organisations to embed data protection by design and default, to ensure that data protection risks associated with new projects

and high risk data processing activities are identified and mitigated. Are data protection considerations (and the requirement to complete a DPIA) highlighted as part of the project development process?

8. What insights can you obtain from your data breach register? Organisations are required to maintain a record of all data breaches, regardless of whether or not a breach is sufficiently serious to warrant reporting to the Information Commissioner's Office (ICO) and/or the data subject. But it's also worth noting that the register can also provide useful insights regarding the nature and frequency of data breaches and highlight specific areas where additional controls and/or training may be required to reduce the risk of breaches reoccurring.

The themes highlighted in this article are based on our experience working in the sector and changes in the European data privacy landscape.

Appendix 2: INTERNAL AUDIT PERFORMANCE QUESTIONNAIRE

Below we set out draft questions for our proposed performance questionnaire:

1. Did we make it clear about the function and purpose of the assignment in general? What was good or where could improvements be made in particular?
2. Did the assignment Terms of Reference clearly set out the purpose and objectives of the assignment and explained the methodology and key deadlines?
3. Did we explain what would happen after our visits i.e. were you clear as to what the rest of the process was and what the expected timeline was to be?
4. Was progress communicated to you during the conduct of the assignment? How and when?
5. Did you find the questions we asked were informed and relevant and allowed you to explain the system that you operate? How could we improve this going forwards?
6. Did the team develop and demonstrate a good level of knowledge and understanding of the scope areas reviewed? - please explain.
7. Did the team conduct themselves in a professional and cooperative manner working efficiently with the management team to deliver the assignment's objectives?
8. Did the report provide a fair reflection of the situation of the area reviewed?
9. Were the reported findings and conclusions balanced and do you think the recommendations are proportionate to the identified risk and add value?
10. Please add any comments you would like to make about your experience.

FOR MORE INFORMATION:

SARAH HILLARY

Sarah.hilliary@bdo.co.uk

Document history		Distribution
Final	01/11/2021	HEALTH AND CARE PROFESSIONS COUNCIL

Author: William Jennings
Review: Bill Mitchell