MAZARS

CROYDON

# Final Internal Audit Report

## Hyperion Application

## October 2016

**Distribution:** Executive Director Resources (Final only)

Director Customer and Transformation

Assistant Director of Finance

Accountancy Manager

| Assurance Level | Recommendations Made | |
|---|---|---|
| **Substantial Assurance** | Priority 1 | 0 |
| | Priority 2 | 2 |
| | Priority 3 | 7 |

# Contents

Page

Executive Summary

## 1. Introduction

1.1 Oracle Hyperion is a comprehensive Web-based application used for budget planning, forecasting, analysis and reporting used across the Council. It replaces the use of bespoke Excel spreadsheets. In addition to replacing old processes, Hyperion introduces new functionality such as accessibility and data storage via The Cloud, as well as integration with Microsoft Office as required.

1.2 Full functionality of the Hyperion application was only recently achieved in July of this year when used corporately for budget forecasting for quarter one. As a result, it should be recognised that the processes are still being refined.

1.3 This audit was part of the agreed Internal Audit Plan for 2016/17.

## 2. Key Issues

| Priority 2 Recommendations |
|---|
| The password settings for the application do not lock user accounts after three unsuccessful attempts, or prevent previous user passwords being reused **(Rec 1).** |
| Unsuccessful login attempts are not currently monitored (to identify inappropriate attempts to access the application) **(Rec 2).** |

The Priority 3 recommendations are detailed under item 4 below.

## 3. Actions and Key Findings/Rationale

| Control Area 2: System Security | | | | |
|---|---|---|---|---|
| **Priority** | **Agreed action/s (Rec 1.)** | **Detailed Finding / Rationale** | | |
| 2 | To liaise with Oracle to enhance the logical password controls on the Hyperion application so that:<br>• User accounts are automatically locked after three incorrect password attempts, having to be reset by an administrator; and<br>• The previous 20 passwords by a user cannot be reused (password history). | Password controls should be sufficiently robust to prevent users accessing other users' accounts and gaining inappropriate levels of system access and functionality. This includes automatic controls locking user accounts after failed login attempts and preventing the reuse of passwords (which weakens the strength of password controls).<br>Our review and testing of the password controls in the Hyperion application identified that:<br>• user accounts are not locked out even after six incorrect password attempts; and<br>• when changing passwords, the previous password can be reused (i.e. no password history is enforced).<br>Further investigation by the Accountancy Manager with the product supplier (Oracle) has ascertained that the account is locked after 8 incorrect attempts and that these settings cannot be changed locally.<br>When user accounts are not locked out after a minimal number of unsuccessful password attempts, the system is weak to 'brute force' attacks whereby users or automated computer programs can make unlimited attempts at guessing passwords. This increases the risk that unauthorised access to the system is gained and financial data is compromised. | | |
| **Management Response** | | **Agreed/Disagreed** | **Responsible Officer** | **Deadline** |
| This will be discussed with our Oracle Relationship manager to determine whether future updates to the system can include this functionality. | | Agreed | Accountancy Manager | December 2016 |

| Priority | Agreed action/s (Rec 2). | Detailed Finding / Rationale | | |
|---|---|---|---|---|
| 2 | To liaise with Oracle to ensure that future updates to the system can include the functionality to enable unsuccessful login attempts to be monitored. | In order to detect instances where user accounts are being unsuccessfully logged into on multiple occasions, a periodic review should be performed of user accounts (to provide assurance over the security of the application).<br>A review of unsuccessful login attempts is currently not performed. The priority of this exercise becomes elevated when considered in conjunction with Recommendation 1.<br>Further investigation by the Accountancy manager with the product supplier (Oracle) has ascertained that this functionality is not currently in place.<br>Where unsuccessful login attempts are not monitored, the Council is not able to detect inappropriate attempts to access the system and therefore cannot employ preventative measures (e.g. increasing network or application security). | | |
| **Management Response** | | **Agreed/Disagreed** | **Responsible Officer** | **Deadline** |
| This will be discussed with our Oracle Relationship manager to determine whether future updates to the system can include this functionality. | | Agreed | Systems Accountant | October 2016 |

## 4. Priority 3 Recommendations

| Agreed Action/s | Detailed Finding / Rationale |
|---|---|
| a) On completion of the corporate Information Asset Register, ensure that the Hyperion application is detailed on the register. | Discussion with the Information Manager identified that the corporate Information Asset Register is currently under development.<br>Where applications are not recorded on the Information Asset Register, the Council is not able to properly manage its data and ensure that any legislative / procedure changes to the handling of data are properly applied to all relevant systems.<br>**Response:**<br>Agreed by Information Manager & Interim Complaints Resolution and Information Management Service Manager. |
| b) On a regular basis, conduct a review to confirm that Hyperion users have appropriate system access rights. Furthermore, the Finance Team should also identify inappropriate levels of access during their quarterly budget monitoring processes. | A regular review of the access rights awarded to users is not conducted.<br>If user access rights are not reviewed, there is the risk that staff incorrectly awarded high-level user permissions are not identified.<br>**Response:**<br>Agreed by Accountancy Manager and Systems Accountant.<br>A review process of user access rights was introduced prior to the start of Q2 monitoring and will be part of the regular quarterly monitoring cycle. |
| c) A second member of finance staff should be trained to perform the monthly 'General Ledger to Hyperion' interface data-load to ensure the process is not dependent on a single member of staff. | Whilst testing did not identify any errors or problems with the data-load being performed by the systems administrator, the system administrator is currently the only member of staff to have performed this task. The task should be rotated amongst suitable staff to prevent there being a single point of failure.<br>Where a complicated process relies on a single member of staff, unexpected absences (e.g. sick leave) mean that the process cannot be performed or completed. In this example, this would prevent the budget forecasting abilities of the Council.<br>**Response:**<br>Agreed by Accountancy Manager and Systems Accountant. |
| d) An independent member of staff (Accountancy Manager) should review and sign-off the accuracy and completeness of the monthly interface exercise. | The interface exercise is currently performed by a single officer and not reviewed by any other member of staff. |

| | |
|---|---|
| | When complicated exercises such as this are not independently reviewed, errors may not be identified that lead to the Council using incorrect budget / forecast figures for financial planning.<br><br>**Response:**<br><br>Agreed by Accountancy Manager and Systems Accountant. |
| e) Create a formal change control procedure that should be followed in the event that a change is required for the Hyperion application. | A procedure to manage the change control process for the Hyperion application is not in place.<br><br>Without a pre-agreed procedure, there is the risk that the application is changed inappropriately. Such issues can include not sufficiently or expertly testing changes before making them 'live' and not obtaining sufficient authorisation before implementing a system-wide change.<br><br>**Response:**<br><br>Agreed by Accountancy Manager and Systems Accountant. |
| f) The Council should obtain assurance from Oracle (Hyperion system provider) on an annual basis that disaster recovery exercises are being conducted successfully.<br><br>The Hyperion application should also be added to the Corporate Disaster Recovery Plan. | Oracle are contractually required to back up the Council's data on a daily basis. However, there was no evidence available that this is conducted (or that Oracle regularly test that they are able to recover the data in the event of a loss).<br><br>Relying on contractual commitments without seeking assurance exposes the Council to the risk that data cannot be recovered in the event of an unexpected data loss.<br><br>This risk is reduced in two respects:<br><br>• The majority of the information held on Hyperion (budget and actual spend data) is held on the General Ledger system (which is backed up independently).<br>• The systems administrator manually saves a complete data back up on a monthly basis for additional comfort. However, if assurance is obtained from Oracle, then this task would not be necessary.<br><br>**Response:**<br><br>Agreed by Accountancy Manager and Systems Accountant.<br><br>There is evidence that Oracle back up daily<br><br>The daily back up is downloaded from the Cloud server by the systems administrator and stored off line for I year. |

| | | |
|---|---|---|
| g) | Accountancy should consult with key stakeholders and users of the Hyperion application on an annual basis, evaluating the level of satisfaction with the service provided by Oracle.<br><br>If performance is unsatisfactory, introduce formal contract monitoring of the supplier's performance and processes to enforce the requirements of the contract. | The key stakeholders (systems administrator and accountancy manager) do not monitor the performance of Oracle (e.g. system uptime, response to technical support queries) as they are currently satisfied with the service and issues are very infrequent.<br><br>Whilst formal contract monitoring on a monthly basis may not be proportionate currently, the service should consult with key stakeholders and users of the application on at least an annual basis to confirm that formal contract monitoring is not required.<br><br>Failure to monitor supplier performance when required exposes the Council to the risk that they do not receive the quality of service they are paying for.<br><br>**Response:**<br><br>This recommendation was agreed by Accountancy Manager and Systems Accountant. |

Appendix 1

# TERMS OF REFERENCE

# HYPERION APPLICATION

## 1. INTRODUCTION

1.1 The Hyperion application is a 'Planning and Budgeting Cloud Service (PBCS)' provided by Oracle. Hyperion allows financial planning, budgeting and forecasting across the Council and was introduced to replace the old system (of using excel spreadsheets).

1.2 In addition to replacing old processes, Hyperion introduces new functionality such as accessibility and data storage via the cloud, as well as integration with Microsoft Office when required.

1.3 This audit is part of the Internal Audit Plan for 2016/17 as agreed by the General Purposes and Audit Committee.

## 2. OBJECTIVES AND METHODOLOGY

2.1 The overall audit objective of this audit is to provide an objective independent opinion on the adequacy and effectiveness of the control environment with regards to the Hyperion application.

2.2 In order to achieve the overall objectives, a risk based systems audit approach will be carried out, documenting and evaluating the actual controls against those expected and based on this, undertaking appropriate audit testing.

2.3 The key findings, conclusions and subsequent recommendations arising will be discussed with management at an exit meeting, followed by the circulation of a draft report for consideration, prior to agreement and issue of the final audit report.

## 3. SCOPE

3.1 This audit will examine the Council's arrangements for controlling the Hyperion application:

| Control Areas/Risks | Recommendations Made | | |
|---|---|---|---|
| | Priority 1 (High) | Priority 2 (Medium) | Priority 3 (Low) |
| Application Management and Governance | 0 | 0 | 1 |
| System Security | 0 | 2 | 1 |
| Interface Controls and Processing | 0 | 0 | 2 |
| Data Input | 0 | 0 | 0 |

| | | | |
|---|---|---|---|
| Data Output | 0 | 0 | 0 |
| Change Control | 0 | 0 | 1 |
| System Resilience and Recovery | 0 | 0 | 1 |
| Support Arrangements | 0 | 0 | 1 |

Appendix 2

## DEFINITIONS FOR AUDIT OPINIONS AND RECOMENDATIONS

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

| | | |
|---|---|---|
|  | Full Assurance | There is a sound system of control designed to achieve the system objectives and the controls are consistently applied. |
|  | Substantial Assurance | While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance which may put this achievement at risk. |
|  | Limited Assurance | There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk. |
|  | No Assurance | Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage. |

Priorities assigned to recommendations are based on the following criteria:

| | |
|---|---|
| **Priority 1 (High)** | Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk. |
| **Priority 2 (Medium)** | Control weakness that represent an exposure to risk and require timely action. |
| **Priority 3 (Low)** | Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice. |

Appendix 3

# STATEMENT OF RESPONSIBILITY

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by us should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Our procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our work and to ensure the authenticity of such material. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

**Mazars Public Sector Internal Audit Limited**

**London**

**October 2016**