Appendix 3 - IT Controls Audit Action Plan - updated November 2022

Ref	Action	Objective	Assigned to	Due Date	Update 08/11/2022
Observation 1. Segregation of duties conflicts between Oracle system administration, developer, and finance roles					
1.1	Review Support team role and privilege combinations.	To separate financial reporting duties / system access and the ability to administer system security	Oracle Applications Support Team Manager	30-Nov-22	New Roles configured; Plan to roll them out by end of Nov'22.
1.2	Develop procedure for regular independent review of Oracle security logs	Proactive, regular review of logs of information security events (e.g. login activity, unauthorised access attempts, access provisioning activity)	My Resources Lead / Oracle Applications Support Team Manager	N/A	Completed, mitigated by logging in via Single Sign on
1.3	Develop system administrators access policy	To formally document policy and issue to users with system administrator roles	My Resources Lead / Oracle Applications Support Team Manager	31-Aug-21	Completed
1.4	Review the number of people with system admin accounts	To reduce the number of people with system admin accounts	Oracle Applications Support Team Manager	N/A	Completed
1.5	Develop Business Case to use Oracle Risk Management Cloud	To investigate Oracle Risk Management Cloud to facilitate the use of appropriate formalised and documented controls to monitor system administrator and support team access.	My Resources Lead	TBC	On Hold pending Oracle Value assessment.
1.6	Investigate the use of reports to provide some limited monitoring of system administrator and support team access	To proactively and formally review reports to detect inappropriate or anomalous activity.	My Resources Lead / Oracle Applications Support Team Manager	31-Aug-21	Completed

Observation 2. Oracle system configuration access granted to an excessive number of users, including non-IT staff / end users					
2.1	Undertake a detailed analysis of users roles and privileges	To understand roles and privileges, and where system configuration privileges exist within roles assigned to users outside of the support team.	My Resources Lead/Oracle Applications Support Team Manager/Support Provider	N/A	Completed
2.2	Support Provider to explain the approach used to design role based system access	To understand Oracle best practice and how that was applied to the system during implementation.	Support Provider	N/A	Completed
2.3	Undertake sample testing of users with access to critical Oracle functions that allows them to change system configurations to confirm if they can use configuration privileges.	To confirm the risks of users identified having these elevated privileges and confirm if complimentary controls e.g. security profiles and data roles prevent access via the application.	Oracle Applications Support Team Manager	N/A	Completed
2.4	Remove configuration privileges from users identified in our analysis where it was low impact and simple to address.	To reduce the risks of users changing configurations.	Oracle Applications Support Team Manager	N/A	Completed
2.5	Carry out a risk assessment of more complex role and privilege combinations, with support from our support provider	To assess the risk posed by the privileges, investigate if new custom roles without configuration priviliges can be created and recommend any appropriate actions.	Support Provider	31-Jul-21	Risk assessment completed.
2.6	Implement regular user access review	To ensure access remains appropriate in line with job duties.	My Resources Lead	TBC	To be reviewed once My Resources Governance re-established

Observation 3. Users self-assigning responsibilities without formal management approval					
3.1	Remove access to the IT security manager role from 3rd Party support staff.	To strengthen control. Work requiring the IT Security manager role will be carried out by appropriate members of the Council's Oracle support team.	Oracle Applications Support Team Manager	15-Mar-21	Completed
3.2	Restate the message to users that they must not self-assign roles and must follow the normal user access request process if they require additional responsibilities.	To prevent users self assigning responsibilities without formal management approval.	Oracle Applications Support Team Manager	28-Sep-20	Completed
3.3	Develop a report to identify instances where members of staff have assigned themselves additional responsibilities and any non-compliance.	To monitor users self assigning responsibilities without formal management approval.	Oracle Applications Support Team Manager	30-Jun-21	Completed