Audit Findings Report 2019/20

Appendix B – Update on action relating to Oracle and General IT controls

Officer Action Plan – *Oracle Technical*

No.	Observation	Recommendation	Response
4.1.1 Completed	Our testing of IT General Controls identified the following findings which have been reported in detail to management: • System Administrator accounts with excessive elevated business Responsibilities	A detailed review should be undertaken of all responsibilities in use that are allocated to the Lewisham environment. Access to functions and data should be based on a least privileged principle. The scope of this review should include Lewisham users and responsibilities that have been copied from default responsibilities.	System Administrator accounts with excessive elevated business responsibilities – this level is a prerequisite for system administration. Please see response to those individuals with "IT Security Manager". There are currently 4 named accounts in use, and these are the essential members of the Oracle Systems Administration team, and are required to have this level of access in supporting the system. Note, whilst there are 3 generic accounts within the system (Interface User; Lewisham Buyer; Lewisham Scheduler) These are used internally only within the system processes and are therefore required for specific Cloud processing – these accounts are not available for an individual user to be able to access. The remainder of any generic accounts that were is use during development and implementation have been removed as recommended. Access will be reviewed monthly – Process has been agreed with Evosys. SR is maintained to ensure this process. SR#106237
4.1.2 Completed	End-users with critical IT privileges within Oracle	Access to critical IT security privileges within Oracle should be transferred to IT system administrators who do not perform end-user duties. All security access rights within Oracle granted to end-users should be revoked.	End-users with critical IT privileges within Oracle Lewisham will arrange a 6 monthly review of user access, whereby managers sign off on their staffs role access, including elevated access integral to the service areas'
No.	Observation	Recommendation	Response

			Self-management of the system. This review process is now scheduled for early Feb 21.
4.1.3 Completed	Lack of defined IT processes for Oracle Fusion	Processes should be established for Oracle in BAU and there should be a formal handover to the Oracle Systems Team. As a minimum, formal processes should be established and enforced around: • User Access Management • Access rights review • Change Management	User Access Management • There is a formal process in place for ERP for allocating roles, approved by the group finance manager, director of service & director of financial services or executive director for corporate services. • For HR/Payroll a similar process is in place for allocating roles, approved by Data owners for HR and Payroll respectively. Access rights review: • Lewisham have arranged a 6 monthly review of user access, whereby managers sign off on their staffs role access, including elevated access integral to the service area's self-management of the system nb., any leaver will have all roles revoked automatically by HR on termination. Change Management • Lewisham now have a process to sign off and document the formal process for recording and approving significant changes to the Oracle Cloud system is in place now. Oracle CAB is held weekly to manage Oracle changes.
4.1.4 Completed	Minimal password security within Oracle	Management should enable account lockout controls within Oracle to address the risk of password cracking. Users should be forced to change their passwords a maximum of every 90 days. Password complexity should be introduced.	Lewisham Oracle users use the Council's single sign on (SSO) policy and therefore do not use username/password at sign in. SSO has a complex password and expiry rules, contravention of which will lock out Oracle access.
No.	Observation	Recommendation	Response
			• These are currently: Passwords may not contain the user's AccountName (Account Name) value or entire displayName (Full Name value). Both checks are not case sensitive. • The password contains characters from three of the following categories: o Uppercase letters of European languages (A

			through Z, with diacritic marks, Greek and Cyrillic characters) - Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters) - Base 10 digits (0 through 9) - Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting. - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages. - Enforce Password history; 20 passwords remembered - Maximum password age; 90 days; - Minimum password age; 1 day - Minimum password length; 9 chars - Password must meet complexity requirements; enabled
No.	Observation	Recommendation	Response
4.1.5 In Progress	Audit logging is not proactively monitored within Oracle	Given the criticality of data accessible through Oracle, logs of information security events (i.e., login activity, unauthorised access attempts, access provisioning activity) created by these systems should be proactively, formally reviewed for the purpose of detecting inappropriate or anomalous activity. These reviews should ideally be performed by one or more knowledgeable individuals who are independent of the day-to-day use or administration of these systems.	1) login activity Lewisham AMT (Cloud systems support) will identify requisite report(s) by Sept 2020 and request Internal Audit to review on an interval agreed by them. ***UPDATE:*** *Only standard report available provides data on last date a user has logged in, rather than all login activity.* 2) unauthorised access attempts Lewisham AMT (Cloud systems support) will identify requisite report(s) by Sept 2020 and request Internal Audit to review on an agreed interval ***UPDATE:*** *Unauthorised access is not possible, or the control does not exist at Oracle app level. Access*

			is via single sign-on, linked to Active Directory. If a user is not authenticated on the network then they cannot access Oracle. If they can access Oracle then they must have been 'authorised' via SSO (single sign on via Active Directory) and hence through their network access/credentials. 3) access provisioning activity) There is a formal process in place for ERP for allocating roles, approved by the group finance manager, director of service & director of financial services or executive director for resources & regeneration. For HR/Payroll a similar process has been signed off post HyperCare period (Sept 2020). Both will have the necessary audit trail. ***UPDATE:*** *Processes in place for both Finance and HCM*

General IT Controls

No.	Observation	Recommendation	Response
4.2.1 In progress	Lack of Periodic Third-Party Service Assurance Report Review for Oracle, ResourceLink and Academy.	We recommend management implement a process to periodically (for example annually) obtain a SOC or ISAE 3402 Assurance report. The report should then be formally reviewed, and any ineffective controls / auditor findings assessed for local relevance and impact. Consideration should also be given to identifying any user entity controls specified within the report and ensuring those are implemented locally and operating effectively.	Oracle Cloud: Lewisham will obtain yearly SOC's from Oracle and formally review recommendations, For ERP & HR/Payroll this will commence post HyperCare (Sept 2020) ***UPDATE:*** *This remains in progress and the Director of IT and Digital is considering employing a third party to conduct reviews subject to cost.* ResourceLink: Mitigated, as RL is now an archive system Academy (Thanh Ngo): Regular service assurance is provided by Capita CST, with whom the Council has a support contract for the Academy system. Capita CST provide monthly reports and, in addition, monthly service review meetings are held with them.

4.2.2 Completed	End-users, IT managers and leavers with Security Administration Rights within Academy, ResourceLink and Active Directory	The responsibility of administering security within Academy, ResourceLink and Active Directory should be transferred to IT system administrators who do not perform end-user duties. All security administration rights within Academy, ResourceLink and Active Directory granted to end-users or leavers should be revoked.	ResourceLink : Mitigated as ResourceLink is now a read-only, archive system. Within the system administration there is an added layer of security with only IT system administrators gaining access with a secure password. An option to prevent users from accessing their own record is available. An option exists to create a new security profile. If system was live. Active Directory: The shared service would not be responsible for managing the security within the Academy and ResourceLink applications. The shared service is responsible for managing Active Directory however. The users in the domain admins group is now reviewed regularly by the Enterprise Support team within the shared service. It is true that the Head of Operations has a domain admins account (in addition to a standard account) but this is required for dealing with priority 1 issues that occur outside of business hours (8am to 6pm Monday to Friday) as there is currently no formal out of hours support offered by the shared service.
No.	Observation	Recommendation	Response
4.2.3 In progress	Periodic Employee Acknowledgement of InfoSec Policy Requirements	Management should introduce a process whereby existing employees are required to periodically (at least annually) formally acknowledge that they have read, understand, and will abide by requirements outlined in the organisation's information security policies. Documentation of these acknowledgements should be retained on file for future reference.	Information Governance Team (Tressina Jones): The Council has purchased a new system called Meta Compliance. This monitors, tracks and reports on completion and acceptance of all training and policies and we can include the council's security policy, or any other policy required to meet this audit requirement; i.e. it would ensure that the Council have a periodic employee acknowledgement / acceptance of council policy / procedure in place that is tested regularly. Due to resourcing issues the introduction of new policies/

			training into the system has been put on hold until the service is back to full FTE, at which point the above will be planned and implemented. ***UPDATE:*** *This one is being progress with Information Governance. An update will be provided in the next report.*
4.2.4 In progress	Removing Leavers' Access Rights within Academy and Active Directory	All logical access within financially critical systems belonging to terminated personnel (i.e. "leavers") should be revoked in a timely manner (preferably at time of termination). Security administrators of financially critical applications should be provided with (a) timely, proactive notifications from HR of leaver activity for anticipated terminations and (b) timely, per-occurrence notifications for unanticipated terminations. Security administrators of financially critical applications should then use these notifications to either (a) end-date user accounts associated with anticipated leavers or (b) immediately disable user accounts associated with unanticipated leavers.	Academy : Academy Benefits is accessed via SSO, based on the user's network credentials. Therefore access is cease with immediate effect as soon as AD account is disabled by SICTS, following the completion of the leaver form by the user's line manager. This process is outside the scope of the Benefits Control Team it is reliant on the user's line manager to submit the leaver form in a timely manner for SICTS to complete the process. Therefore remedy would have to come from a review/improvement of the corporate. Leavers' process, not from within Revs & Bens. Active Directory : The leavers' process is currently being reviewed but part of that process is that the account is disabled and should therefore remove access to all systems that use Active Directory for authentication. The shared service does not manage security within applications themselves. ***UPDATE:*** *This is focused at Academy and Active Directory, but the common factor in both is the leavers process (the form) and the effectiveness of it. This is being reviewed as part of the Oracle improvement work.*
4.2.5 Completed	Inadequate Minimum Password Length Enforcement within ResourceLink	The organisation should enable minimum password length restrictions within	ResourceLink: On recommendation password minimum length increased to

		ResourceLink to a value in-line with best practices.	eight characters with a minimum of three character types required.
4.2.6 Completed	Lack of Policies, Processes and Security for Batch Processing	Documented policies and processes should be established and disseminated for batch processing.	Oracle Cloud: There are documented processes in place and the 2 examples provided by the auditor of batch processing in Oracle Cloud have been demonstrated (evidence was emailed separately April 2020) They are 1) 3 1 3 - Oracle - Scheduled process error logs - F59D6451 2) 3 1 2 - Oracle - AP Liability Reconciliation DEC 2019-20 (Cloud). These processes are the responsibility of Lewisham Core Accounting, Financial Services Group. ResourceLink : Responsibility and main contacts for this would be with Lewisham's Payroll Team. This is now mitigated as RL is now an archive read- only system. Academy : Capita CST, with whom the Council has a support contract for the Academy system, are responsible for all Academy batch processing.