Guardians of New Zealand Superannuation

Oracle HCM Implementation (Phase 1) Internal Audit Report
25 February 2022

pwc

Content

Dashboard 1

Executive Summary 2

Detailed Observations 3

Improvement Opportunities 4

Appendices

A. Scope and Approach
B. Summary of Low Risk Rated Observations
C. Risk Rating Matrix

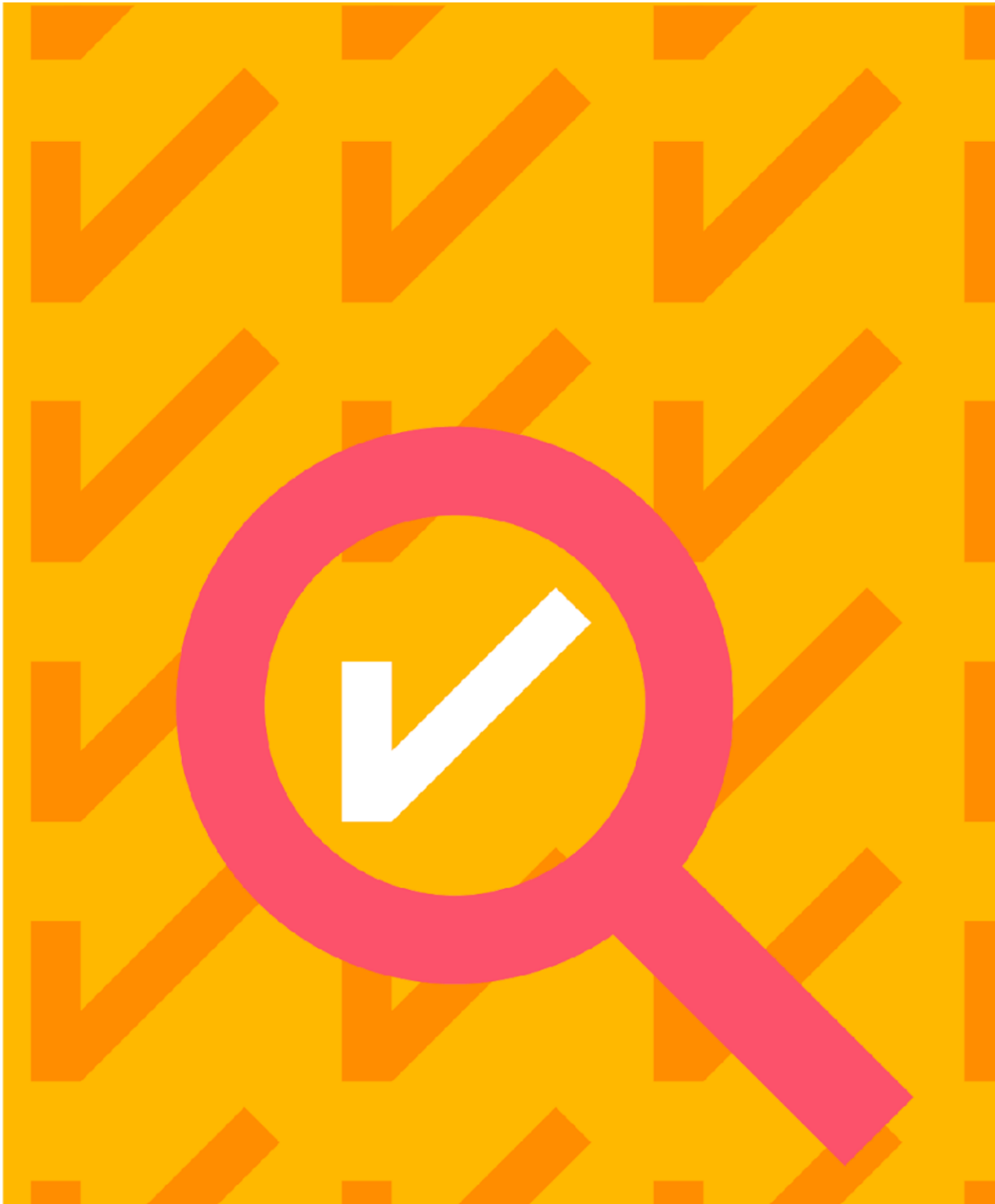
Distribution List

To:

[redacted]

cc:

[redacted]



Garry Sue | Head of Internal Audit | Guardians of New Zealand Superannuation

25 February 2022

Oracle HCM Implementation (Phase 1) Internal Audit Report

Dear Garry

In accordance with our Master Services agreement dated 18 August 2017 and our subsequent Engagement Summary dated 21 September 2021 with its important notices as summarised in Appendix A, we are pleased to provide our final observations and recommendations for the Oracle HCM implementation internal audit. Our work was performed during the period of October to December 2021.

We would like to extend our appreciation to your teams for their support and cooperation throughout this internal audit engagement.

Yours sincerely

| PwC New Zealand | Partner

Inherent limitations: This assignment does not constitute a review, audit, or assurance engagement as defined in the standards issued by the External Reporting Board. Accordingly, this engagement is not an assurance engagement, nor is it intended to, and will not result in, the expression of an assurance, audit or review opinion, or the fulfilling of any statutory audit or other assurance requirement.

Confidential: This report is provided solely for Guardians of New Zealand Superannuation for the purpose for which the services are provided. Unless required by law you shall not provide this report to any third party, publish it on a website or refer to us or the services without our prior written consent.In no event, regardless of whether consent has been provided, shall we assume any responsibility to any third party to whom our report is disclosed or otherwise made available. No copy, extract or quote from our report may be made available to any other person without our prior written consent to theform and content of the disclosure contained within the report.

---

1. Dashboard

Overall Summary

The Oracle Human Capital Management (Oracle HCM) is a software as a service (SaaS) solution implemented to replace legacy systems and consolidate Human Resources (HR) data to support associated business processes and controls. This system integrates with key processes such as payroll and authentication mechanisms such as Active Directory.

This internal audit focused on Phase 1 (Core HR, Recruitment and Onboarding) of four planned phases. From this internal audit of selected aspects of the Oracle HCM system and supporting processes and controls, observations and improvement opportunities have been identified, in line with good practice, to develop and enhance processes to maintain operational consistency, while supporting future maintainability.

Oracle HCM (Phase 1) Key Facts and Statistics

Go live date	# Oracle Cloud modules	Oracle HCM licence period	# Oracle HCM integrations
1 November 2021	2 (Core HR, Recruitment and Onboarding)	5 years from 23 Feb 2021	6 HR* and 2 non-HR** systems * *DataPay, [redacted], Xref, SHL, Careers Website with Insight Creative, [redacted]* ***ServiceNow, Microsoft 365*

Observations Snapshot

#	Category	Observation Title	Rating
3.1	Operating Model	Transition from project to business as usual is ongoing despite Oracle HCM go live	High
3.2	Operating Model / Access	Operational model for application administration is not formalised	High
3.3	Operating Model / Processes	Business continuity management needs to be formalised for Oracle HCM	Moderate
3.4	Access / Security	Oracle HCM access is not adequately segregated	High
3.5	Access / Security	Access management processes are not aligned to organisational TIKA processes	High
3.6	Processes / Controls	Compensating controls in the Oracle HCM application have not been configured or documented	High
3.7	Access / Security	Third party access is not reviewed for appropriateness or regularly monitored	High
3.8	Access / Security	Sign-on controls could be further strengthened	High
3.9	Change Control	Controls for system changes need to be finalised for business-as-usual processes	High
3.10	Testing	Roles and responsibilities for delivering training to testers was not clearly defined	Moderate
3.11	Processes / Configuration	Benefits to be gained through transformation by adoption of Oracle-delivered functionality and processes may be diminished	Moderate
3.12	Support / Maintainability	Responsibility needs to be assigned for configuring new Payroll Calendars	Moderate
3.13	Project Management / Processes	Project Management processes not as rigorous as they could be	Moderate
3.14	Third Party Arrangements	Elevated reliance on support provided by and limited oversight of third parties for Oracle HCM	Moderate
3.15	Third Party Arrangements	Third party contracts management and performance monitoring could be improved, in terms of defining roles and responsibilities and consistency of execution	Moderate
3.16	Testing	Insufficient visibility of testing performed by third parties	Moderate
3.17	Data Migration	Data migration dry runs or mock conversions could not be evidenced	Moderate
3.18	Support / Maintainability	No evidence of a code repository for the storage and control of code related to customisations	Moderate
3.19	Access /Security	Roles not designed as per Guardians' future requirements	Moderate

2. Executive summary

a. Background

Oracle Human Capital Management (Oracle HCM) is delivered by the vendor Oracleunder a software as a service (SaaS) model that supports the Guardians' Human Resources (HR) processes and controls and integrates with key business processessuch as payroll.

The Guardians is implementing Oracle HCM in a phased approach detailed below:

1. Core HR, Recruitment and Onboarding

2. Learning, Performance, Career Development, Goals, Health and Safety

The phasing for the implementation of the remaining modules (Compensation, Benefits, Talent Review, Succession Planning, Workforce Modelling) will be determined at a later stage.

Go live for Phase 1 (Core HR, Recruitment and Onboarding) was completed on 1 November 2021.

The Oracle HCM implementation involved a 'lift and shift' approach, resulting in a higher-than-expected level of configuration and customisation of the solution to fit around the existing business processes and controls operating within the Guardians' environment.

b. Why we did the internal audit

Being a new cloud-based platform that covers a broad range of human resource functionalities, it is important that Oracle HCM can be accessed when required and is properly secured to prevent unauthorised access to information in the system. The Oracle HCM system holds sensitive information of staff and job applicants. A compromise of the Oracle HCM system could result in potential reputational damage orregulatory risks (e.g., privacy breaches) from data loss.

Also, as a SaaS (Software as a Service) solution, it is important that responsibilities during the project and for the ongoing support of the platform between the vendor, support partner, the HR team and the inhouse IT team are clear and fit for purpose. Many of the findings from this review stemmed from the lack of IT involvement or signoff during this IT-led project, that have led to the need for technical design review andremediation.

Inappropriate setup and management processes over the system could impact the following core business activities (November 2021 release):

- Recruitment
- Staff onboarding and termination
- Payroll

c. Key messages

This internal audit identified that the rigour established for the Oracle HCM implementation at the outset has not been maintained. Also, some decisions made during the project contributed to the current state of processes and controls, including exclusion of access management from the project, and changing to a 'lift and shift' approach.

This resulted in a higher-than-expected degree of solution configuration and customisation to fit existing Guardians' processes. Moreover, internal, and external staff challenges and changes have led to project delays and more resources being used than were planned.

In summary, we have identified 8 high, 11 moderate and 10 low risk rated observations. These are captured on the following pages.

Our internal audit of Phase 1 of this Oracle HCM implementation has identified key themes that the Guardians should focus their efforts on to improve in-line with good practice, summarised below. More detailed observations can be found in the following section 3 (Detailed Observations) of this report.

At the onset, we note that the Guardians' Oracle HCM implementation project was well positioned for success due to its limited/defined scope (recruitment, onboarding and Core HR plus payroll and other relevant integrations), the size and structure of the Guardians' organisation (small with a relatively simple structure), and the relative size and composition of the project team (dedicated team members, Subject Matter Experts and engagement of Oracle HCM implementation specialist, [redacted]). However, despite these factors, the Project Go Live was delayed by approximately 15 weeks and this internal audit has identified 29 observations as outlined above. Some of these observations are in line with issues noted by other organisations as they transition into a new Cloud application, but attention is required to address them as recommended.

i) The current operating model, including roles and responsibilities, and transition from project to embedding business as usual processes and controls, are clearly defined

As the Oracle HCM application transitions from project mode to business as usual (BAU), there is a need for a well-defined operating model for day-to-day operation and maintenance of the solution (*observation 3.1*). The following areas can be focused on to tighten the current operating model, including:

2. Executive summary

- Unclear roles and responsibilities for ongoing support of the solution (e.g., for user administration) (*observation 3.2*). Management is in the process of discussing this to arrive at an agreed outcome. Roles and responsibilities should be fit for purpose while respecting data sensitivity. Considerations should include:
  - teams and third-party support such as [redacted], Oracle and other integration partners;
  - how ongoing support will be delivered between the Guardians' HR and IT;
  - for protecting sensitive data, detective controls such as auditing and data security controls can mitigate risk of unauthorised access.
- Processes (e.g., change requests and features management for Oracle quarterly releases) and controls for system changes are being finalised under the business as usual (BAU) post-implementation support model (*observation 3.9*). IT and HR are working on change control requirements for all system changes (e.g., major or minor). Roles and responsibilities between Guardians and third parties such as Oracle and [redacted] who provide support for system changes (i.e., design, development, testing, deployment) should be clearly defined and managed.
- Business continuity management (BCM) requires formalisation (*observation 3.3*). BCM considerations are highly reliant on feedback from [redacted], including guidance on what can be expected from the vendor Oracle for business continuity, including but not limited to:
  - system and data availability and integrity
  - backups management, and
  - disaster recovery.

For example, it is was not clear to the Guardians to what extent backups can be retrieved from the vendor Oracle. To avoid business disruption, ensure the extent of BCM support provided by Oracle and [redacted] is well understood and captured in contractual agreements.

Embedding relevant processes and controls to ensure they are effective, fit for purpose and sustainable in the long term is a work in progress. However, taking note of the above considerations will facilitate a smoother BAU transition for future phases.

ii) High reliance on and limited oversight of activities performed by key third parties, including implementation partner [redacted] and Oracle vendor

Key third parties, such as Oracle, who deliver Oracle HCM as a SaaS, and [redacted], the implementation and support vendor, are heavily relied on (*observation 3.14*). While we have identified that Oracle HCM service organisation (SOC) reports have been reviewed as part of the certification and accreditation process and will be reviewed by management as part of the annual review cycle, we have identified the following:

- SOC reports are not available for [redacted]. The Guardians should instead seek assurance by developing a monitoring process and regularly measuring [redacted]'s performance against defined key performance indicators in line with contractual obligations, including privacy and other legislative requirements. The new Guardians-wide third-party risk management framework will include developing monitoring responsibilities from both a project and BAU perspective, which should be clearly defined and assigned to appropriate Guardians' staff (e.g. the relationship owner).

Outside of the above points, third party contracts are often supplier-driven and therefore not standardised in terms of clauses (e.g., terms and conditions) (*observation 3.15*). Minimum third-party roles and responsibilities have not been clearly defined, creating difficulty in monitoring performance against expectations.

For example, this could include, but is not limited to:

- obtaining comfort over data handling, particularly sensitive data and how it is protected to maintain confidentiality and integrity, ensuring data ownership is clearly defined
- availability of services and related data including backups, restoration testing, business continuity management (for example, how the Guardians are comfortable that their data will be available and recoverable when needed) (note: this is included as part of the Oracle vendor's, rather than [redacted]'s, responsibilities in their cloud contract), and
- defining service level agreement (SLAs) against which supplier performance can be assessed against, including SLA reporting and considerations for non-compliance. However, management have stated the procurement and legal teamsare working to improve existing supplier management processes, including standardising terms and conditions, where possible, for a start.

iii) User access management and security processes and controls require improvement

Oracle HCM captures typically sensitive data. User access management and security are critical to ensuring only appropriate people can access data commensurate with roles to maintain data integrity and confidentiality. The project's approach to role design was to mirror the privileges in the legacy environment. We have identified the following:

- Oracle HCM access is not yet managed in line with the Guardians' access management framework, TIKA (e.g., user access provisioning, deprovisioning and recertification processes) (*observation 3.5)*, although we understand that this is a work in progress. Access is currently managed by the Head of HR Ops outside of TIKA, as security roles are being finalised. In line with good practice, 'auto provisioning' rules are being used, however, management can extend the use of auto provisioning to other roles being manually assigned.

2. Executive summary

- At the time of the review, third parties (e.g., [redacted]), who have privileged access, used generic accounts (*observation 3.7)*. Align with good practice by using named accounts to support traceability of inappropriate activities. Secondly, appropriateness of third-party access is not assessed, access is not revoked in a timely way, and activity auditing is not enabled for monitoring. For example, there is at least one case of a [redacted] user having left the organisation but retaining their Oracle HCM access.

  Ideally, the Guardians should implement measures to restrict access, such as temporary ('just in time' or 'break glass') access, frequent password resets, regular access reviews, and privileged activity monitoring.
- Segregation of duties (SoD) conflicts exist (e.g., the HR Operations team's access enables potential circumvention of processes and/or controls) (*observation 3.4)*. Certain processes (e.g., the ability to administer salaries or change employee assignments) do not require independent approval within Oracle HCM. Moreover, some users can change system configurations and perform user administration outside of their job roles. At a minimum, define a SoD matrix for role assignment for new and existing users. Subsequently conflicts should be identified and appropriately managed as part of ongoing risk management.
- Compensating controls have not been configured (*observation 3.6)*. For example, auditing is not currently enabled. The Guardians should at least enable system audit logging to facilitate exception-based monitoring of unusual activities.
- Staff are currently able to bypass single sign on (SSO) and directly reset their passwords, which can lead to misuse of access by sharing of passwords or the ability to access the application from external networks or devices (*observation 3.8)*. Management has recognised this risk and are working to resolve this, but it remains open.

  The Guardians should consider implementing monitoring controls so such password resets can be reviewed. In the long term, the recommendation is to disable the ability to access the 'chooser page', which we understand is work that is currently underway.
- Oracle-delivered data masking is not being used (the only sanitisation applies to salary changes and removal of attachments, e.g., contracts) to protect sensitive data in non-production environments *(observation 3.5)*. The Guardians should consider applying the same level of access controls and rigour for non-production in line with the production environment.
- A roles matrix defining roles, access rights, and considerations of approvals and segregation of duties, was not defined pre-implementation. Testing has not been performed to validate if provisioned access is in line with the Guardians' expectations *(observation 3.19)*.

iv) Oracle HCM configuration / customisation requires close attention whenimplementing quarterly releases, enhancements, or bug fixes

The Guardians' approach to adapt Oracle HCM to accommodate existing HR processes has led to the following observations:

- benefits to be gained through transformation by adoption of Oracle HCM may bediminished through non-standard use of the application (*observation 3.11)*.
- higher level of configuration and customisation (~231 customisations) than expected, including customised personalisations for the Guardians' look and feel, customised personalisations to limit unnecessary access to functionality and approval rule configuration (*improvement opportunity 4.2*). Definitions for reference:
  - Configuration: no coding required to enable functionality. Configuration involves selecting values from drop down lists, selecting/deselecting checkboxes, entering plain text into fields such as the name or description of the configuration item. e.g., the setup ofbusiness units, departments, jobs, positions.
  - Customisation: coding (e.g., SQL scripts, XML or other coding languages) required to enable functionality, e.g., some personalisations that use SQL to limit user access and some workflow approvals that use SQL to select approvers. Also applies to custom integrations and reports (i.e., not reports that are created by dragging and dropping fields into the report, but reports that are created using SQL scripts for use by downstream systems, e.g., DataPay, ServiceNow).
  - Personalisation: changes made to the appearance of Oracle HCM, e.g., to hide certain fields for all users or update the look and feel such as colour scheme of the application. Personalisation can be configuration (e.g., selecting/deselecting a check box to hide or show afield) or customisation (e.g., using code (e.g., SQL) to limit which userscan see a certain page).
- with a higher level of configuration comes the risk of support issues with each quarterly release of new functionality from Oracle, any enhancements or bug fixes.It is recommended that the Guardians perform an impact assessment for each new release to identify any Oracle HCM (including Oracle Guided Learning) configuration impacts (on functionality, personalisations and approval rules) and regression test the configuration changes for every quarterly release in both test and production (to the extent possible in production), as the Guardians have planned, as part of the quarterly release process *(observation 3.9)*.

2. Executive summary

v) Testing methodology and execution needs more rigour, and roles and responsibilities could be better defined, with formal approvals documented

Testing impacts multiple scope areas, including business processes, configuration management, access management and Oracle HCM integrations, including the critical DataPay payroll system integration. In testing, the volume of user acceptance testing (UAT) and Hypercare defects raised for Phase 1 is higher than what would be expected (*improvement opportunity 4.5*). Some contributing factors are:

- the Guardians having limited visibility over testing performed by third parties, including details of test scripts and results. For example, [redacted] only performed basic unit testing of code for the DataPay component and [redacted] verified any changes made but formal testing was left to the Guardians to complete. Moreover, we identified that [redacted]'s methodology 'Cloud HR to the Point' meant that the Guardians had to incorporate a decision to apply the 'V' model to their testing approach. However, there is the risk that [redacted] were performing testing that wasnot in line with their methodology (*observation 3.16*). The Guardians should ensuremore rigour and transparency in testing performed, along with greater monitoring of [redacted]'s performance can be conducted by the Guardians in future phases.
- the absence of detailed business requirements meant the next best option was to align test cases with evolving business processes to provide a degree of coverage, however this, in combination with resource constraints (i.e., getting time from subject matter experts), meant there was room for improvement of mapping of test cases and coverage of business processes. The Guardians should ensure that detailed business requirements and sufficient resources are available for future testing phases to ensure even better coverage of processes and comprehensive test cases being defined for execution. In some implementations, business users even get involved in earlier phases of testing such as System Testing to allow early identification of issues and to accelerate user adoption, assist with change management and acceptance of delivered functionality and processes.
- unclear roles and responsibilities between the Guardians and [redacted] (*observation 3.10*). An expectations gap in training delivered by [redacted] termed 'train the trainer', which would typically see training delivered to potential instructors or subject matter experts, was not performed, rather it was more technical training for system administrators. For future phases, ensure roles and responsibilities are clearly defined and communicated upfront, minimising potential expectation gaps. Include these in third party contracts, as applicable. Testers should be provided sufficient training to foster familiarity with the system to effectively execute test cases, as applicable. In certain situations, i.e., as part of a deliberate project decision, if test scripts are sufficiently detailed and rigorous, then there may not need to be training for end users prior to UAT to ensure system familiarity.

Outside of the above points, we identified that:

- approvals were often verbally obtained, for example, for the master test strategy, following reviews performed by the Project Governance Board and [redacted] throughout Phase 1. Going forward, the Guardians should document these approvals.

Details on low risk rated observations, are summarised in Appendix B. While of lower risk we feel considering these items will help lift maturity in respect of support and maintainability, training, testing, integration, privacy impact assessment, and business processes and configuration.

These were also shared with management separately in a Low-Risk Issues Log, including agreed action plans. Detailed observations on moderate and above risk rated items can be found in the following section 3 (Detailed Observations) of this report.

Improvement opportunities were also identified from the phase that has already been completed, with lessons to be considered for future projects. These are included in section 4 (Improvement Opportunities).

3. Detailed Observations

3.1. Transition from project to business as usual is ongoing despite Oracle HCM go live	
Category	Operating Model
Risk Rating	**High** (Likelihood: Likely / Impact: Minor)
Observation	Despite Phase 1 go live being completed on 1 November 2021, numerous roadblocks and difficulties still exist in successfully transitioning from project to business as usual (BAU) processes and risk management and implementation of controls. As a result, embedding these processes and controls to ensure they are effective, fit for purpose and sustainable in the long term is a work in progress. For example, user access management controls and security are yet to be fully developed or finalised, let alone embedded into BAU. BAU IT support considerations have not yet been sufficiently covered, including roles and responsibilities between third parties including [redacted] and all other HR integration partners and/or the Guardians HR and/or IT teams. As a result of post-go live transition from project to BAU, the handover to the business (HR and IT) has not been completed. The Project Governance Board decided to have the Oracle HCM project team support through the Oracle 21D release (scheduled for 4 December 2021) and provide support to at least the end of December 2021. To assist with resourcing constraints and have a dedicated Oracle HCM system administrator, the Guardians have hired a HCM system specialist who started mid-December 2021. In the future, the Guardians should ensure all relevant processes and controls have been fully defined and implemented prior to going live to facilitate a smoother transition from project to BAU. Ensure the right support model is in place between internal teams and any third parties, if applicable, including clear definition of roles and responsibilities for BAU processes and controls. Typically, organisations would include the design of the operating model, processes and controls as part of the HCM implementation project so that the design of these aspects would be completed by the end of the design phase for the HCM implementation. Members of the BAU support team would often be part of the project team from the commencement of the project including design and test activities to help accelerate knowledge transfer and prepare the team to accept the ongoing support of the application post go live. For the Guardians a role change meant that the previously identified Oracle HCM System Administrator was not available, and a replacement needed to be recruited.

3. Detailed Observations

Management Agreed Action	1. Processes and controls that were not adequately defined and established at the time of go-live will be rectified as noted in the below observations highlighted in this audit: • Access & Security (refer 3.4, 3.5, 3.7) • Support model (refer 3.2) • Roles and responsibilities (refer 3.3) 2. For future phases of Kaizen, the project team will ensure project tasks are included to: • ensure there is early engagement with Cloud Operations, Service Desk and BAU Support to understand the Operational Readiness requirements so that BAU processes and controls arising from project are adequately defined, documented and implemented prior to go-live. Ensure the right support model is in place between internal teams and any third parties, if applicable, including clear definition of roles and responsibilities for BAU processes and controls. • Representatives of the BAU Support were included in the project activities, further work is needed to ensure that these representatives understand what is expected of them to take back to their teams to ensure BAU support and transition is smooth. **Owner:** [redacted] **Completion Date:** 30 September 2022
3.2. Operational model for application administration is not formalised	
Category	Operating Model / Access Management
Risk Rating	**High** (Likelihood: Likely / Impact: Moderate)
Observation	As the Oracle HCM application transitions from program mode to business as usual (BAU), there is a need for a well-defined operating model for the day-to-day operations and maintenance of the application. Roles and responsibilities relating to the application are not clearly defined. This was particularly the case for user administration as this responsibility typically lies with the IT function, however this is being reconsidered in light of the sensitive data within the Oracle HCM application. Poorly defined roles and responsibilities and ownership of application administration can lead to ineffective management and delays in resolution of issues or result in technical issues where the business takes responsibility for areas that are technical in nature. This could also result in departure from the Guardians' enterprise IT policies and processes.
Management Agreed Action	Roles and responsibilities for the administration of the Oracle HCM between HR, IT, the support partner, the software vendor and integration partners (if necessary) will be clearly defined and documented. **Owner:** [redacted] (with input and agreement from the [redacted])
	Completion Date: 30 June 2022

3. Detailed Observations

3.3. Business continuity management needs to be formalised for Oracle HCM	
Category	Operating Model / Processes
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	Business continuity management specific to Oracle HCM, including business as usual processes and controls, has not been formalised. Management have stated business continuity management considerations are highly reliant on their third-party support vendor [redacted]'s feedback and guidance on what can be expected from the vendor Oracle in terms of business continuity, including but not limited to availability, backups management, and disaster recovery aspects as part of business continuity management for Oracle HCM. For example, it is not clear to what extent backups can be retrieved from the vendor Oracle should the need arise to recover HR data. In addition, the support agreement with [redacted] does not specifically define how they will be involved in business continuity management to support the Guardians from a support arrangement perspective aside from communicating with the vendor Oracle on incidents as needed. The Guardians can look to better define both Oracle and [redacted]'s roles and responsibilities in relation to business continuity management, ensuring these are captured in their contractual agreements where possible. Ensure that the Guardians understand the extent to which the vendor Oracle will provide activities supporting business management continuity, including backups management and disaster recovery, to identify gaps, if any, where controls may need to be implemented or existing controls embedded to address any residual risks to support ongoing availability of Oracle HCM in the event of business disruption. Any discussions and decisions or considerations should also be formally documented.
Management Agreed Action	Business Continuity and Disaster Recovery requirements will be defined for Oracle HCM. This will include: • Documenting a business impact assessment to understand the criticality of system unavailability to the Guardians business objectives. • Defining recovery point and recovery time objectives (i.e., RPO/RTO) • Defining roles and responsibilities between Guardians teams and any third parties e.g., [redacted], Oracle (including response times) • Ensuring third party contracts adequately reflect BCM responsibilities e.g., Contractually define [redacted]'s responsibility for BCP with Oracle • Determining the nature and timing of any restore testing **Owner**: [redacted] (with input and agreement from the [redacted]) **Completion Date**: 30 September 2022

3. Detailed Observations

3.4. Oracle HCM access is not adequately segregated	
Category	Access Management / Security
Risk Rating	**High** (Likelihood: Possible / Impact: Moderate)
Observation	Extensive end to end access has been granted to some members of the HR Operations team, resulting in Segregation of Duties (SoD) conflicts within the team. Whilst the approval of transactions provides a level of mitigation, there are still certain processes that do not require an independent on-system approval such as administering salaries and changing employee assignments. We understand that evidence of off-system approval that is compliant to HR Policy is required and available for all transactions that do not have on-system approval, however this was not tested as part of this review. It is normally expected that these types of transactions would require independent review to ensure that appropriate process have been followed. This issue is further exacerbated by the fact that two HR Operations users (Head of HR Operations, and the Oracle HCM Specialist) also have access to change system configurations and administer users, granting the ability to potentially change the configurable application controls and undermine mitigations for elevated access. The risk due to these conflicts are not mitigated by the approval workflows as they may be overridden by the users with access to the configurations. Moreover, a formal SoD matrix has not been developed to facilitate role assignment to new or existing users. This might result in a higher number of conflicts as the use of the Oracle HCM application evolves. If SoD conflicts are not appropriately identified and/or resolved, this would increase the risk of circumvention of processes and controls.
Management Agreed Action	Roles within Oracle HCM will be assessed to identify and manage SoD conflicts. **Owner**: [redacted] **Completion Date**: 30 April 2022
3.5. Access management processes are not aligned to organisational TIKA processes	
Category	Access Management / Security
Risk Rating	**High** (Likelihood: Possible / Impact: Moderate)
Observation	Access to Oracle HCM is not currently managed within the Guardians' access management framework, TIKA. As a result, the TIKA access provisioning, deprovisioning and recertification processes do not currently apply to Oracle HCM. Documentation is currently being finalised of all system access to be incorporated into the TIKA processes. Until then, the user access management process is being managed by the Head of HR Operations. During the project phase, access provisioning has been managed by the Head of HR Ops, however this again has not been reflected in TIKA. Whilst this is in line with the organisation policy, it is good practice that based on the risk associated with personal employee data, TIKA should be used to control access provision during the project. Not being aligned to the Guardians' standard access management processes results in a risk of user access not being reviewed appropriately and approved in advance of access being provisioned in the system. User access in Oracle HCM is being reviewed on an ad hoc basis by the Head of HR

3. Detailed Observations

	Operations for appropriateness but not formally reviewed and documented as this is a TIKA-initiated process. In the absence of TIKA, we note that only two changes have been made which was requested and documented in ServiceNow and will be part of the handover documentation to TIKA. We do note that the solution design incorporates the use of 'auto provisioning' rules that assign some roles to users based on their job roles. For example, Employee/Contractor access, Line Manager/Hiring Manager access, and the GMHR, and CEO access. This is good practice and management should explore extending the use of auto provisioning rules to other manually assigned roles. Finally, given the sensitivity of data in non-production environments and limited data masking when these are refreshed, the same level of access controls needs to be applied to these environments as well.
Management Agreed Action	Role based access will be defined for Oracle HCM and be updated included in Tika processes (access provisioning/monitoring tool). As part of this we will explore: • Whether Tika should be used to control access during future project stages • Extending the use of auto provisioning rules to other manually assigned roles. • Extending the same level of access controls to non-production environments. **Owner**: [redacted] (with agreement from the [redacted]) **Completion Date**: 30 April 2022
3.6. Compensating controls in the Oracle HCM application have not been configured or documented	
Category	Processes / Controls
Risk Rating	**High** (Likelihood: Possible / Impact: Moderate)
Observation	Formal controls documentation has not been produced as output from the Oracle HCM implementation. We would recommend, and expect, that a risk-based approach is used to design and implement controls and that these are formally documented in alignment with the existing process maps. This would include security, configurable and off-system manual controls. This approach would assist management with being more proactive about mitigating risk and work towards optimising the control environment for efficiency and effectiveness. Key compensating controls, for example, exception monitoring, particularly through use of the auditing functionality have not been set up. However, this is currently being explored with the third-party support vendor [redacted]. As a result, exceptional activity is not reviewed, nor is there the ability to perform a forensic review should the need arise. System auditing logs would enable traceability of inappropriate activities back to the source.

3. Detailed Observations

Management Agreed Action	1. HR will work with Enterprise Risk to develop a risk and controls matrix for HR Oracle HCM processes. **Owner:** [redacted] (with input and agreement from Manager Enterprise Risk) **Completion Date**: 31 May 2022 2. HR will work with IT Security to develop and implement system monitoring controls. This includes exception monitoring through use of system audit functionality, system audit logging to enable identification of inappropriate activities. **Owner:** [redacted] (with input and agreement from [redacted]) **Completion Date**: 30 June 2022
3.7. Third party access is not reviewed for appropriateness or regularly monitored	
Category	Access Management / Security
Risk Rating	**High** (Likelihood: Possible / Impact: Moderate)
Observation	Third party (e.g., [redacted]) privileged access to the Oracle HCM system is not reviewed for appropriateness of access and monitoring of activities, particularly in production. At the time of the review, [redacted] was noted to have been using generic accounts, which is not good practice, and restricts the ability for the Guardians to identify the specific individual who may be responsible for any inappropriate activities performed within the system. Use of any generic user accounts is not in line with the policy and should have been signed off by IT Security, however no evidence of this was noted in the review. Management have stated the intention to use named user accounts going forward. Moreover, third party access is not revoked in a timely manner. There has been at least one case where a [redacted] user had left the organisation, but their Oracle HCM access was not revoked in line with their departure. Additional controls should be in place for external users, such as frequent password resets, regular user access reviews, and temporary (time-bound) access. Also, the same controls should apply for any external user access including any system accounts for integrating into the Oracle HCM application. In addition, rather than administrator access being provisioned permanently, management should consider implementing an emergency access process whereby access to administrators, including the [redacted] users, is only provided as required and for a temporary period. In the period that access is granted, activities in the application should be audited to confirm access is used only for the purpose it was provisioned for.
Management Agreed Action	1. A process for managing access to Oracle HCM by third parties will developed. This will include investigating and implementing improved controls for external party access to the Oracle HCM system. Options to investigate will be in consultation with Cloud Operations/IT Security and is expected to cover periodic access validation, frequent password resets, temporary (timebound) access, specific named user accounts (rather than generic accounts) **Owner:** [redacted] (with input from [redacted]) **Completion Date**: 30 April 2022

3. Detailed Observations

	2. HR will work with IT Security/Cloud Operations to investigate and implement improved controls for external parties to the system. This includes exploring, frequent password resets, temporary timebound access, specific user accounts rather than generic accounts. **Owner:** [redacted] **Completion Date**: 30 June 2022
3.8. Sign-on controls could be further strengthened	
Category	Access Management / Security
Risk Rating	**High** (Likelihood: Likely/ Impact: Moderate)
Observation	As there are external users such as candidates and recruiting agents who are not currently on Active Directory, this requires the need to provide users with the ability to directly enter a user ID and password. As a result of this requirement, the Guardians staff can bypass single sign on (SSO) and reset their passwords directly. This is a known issue that is being actively resolved, but it remains an open risk. This could increase the risk of a user account being misused where passwords do not follow the organisation policy or where accounts could be accessed inappropriately even when the respective accounts are disabled or locked in Active Directory. We would recommend that management consider implementing monitoring controls so that such instances of password resets can be identified, and access restricted until the password is reset by an administrator. In the long term, it would be recommended that this ability to access the 'chooser page' is disabled. In addition, the [redacted] functionality that restricts access to certain functionality and data depending on where a user is logging in from (inside or outside the corporate network) is currently not being used. Whilst this was not discussed during the project, the need for mobile access could pose constraints to using this functionality. However, the functionality can be enabled at a role level so that the roles that provide access to sensitive data and transactions are limited to access from the corporate network or VPN. In case of a Business Continuity event, LBAC can be temporarily disabled to allow external access.
Management Agreed Action	1. We will explore implementing monitoring controls so that such instances of password resets can be identified, and access restricted until the password is reset by an administrator for the external integrations. 2. Location Base Access Control will not be enabled as this function is fulfilled within Microsoft Azure and managed as part of SSO. **Owner:** [redacted] (with input from [redacted]) **Completion Date**: 30 April 2022

3. Detailed Observations

3.9. Controls for system changes need to be finalised for business-as-usual processes	
Category	Change Control
Risk Rating	**High** (Likelihood: Likely / Impact: Moderate)
Observation	Processes and controls for Oracle HCM system changes are still being finalised under the business as usual (BAU) post-implementation support model. Change requests and features management processes (i.e., for Oracle quarterly releases) have been defined in the support model, however these are still in draft. Currently the IT team is working with HR on change control requirements to ensure all system changes, whether major or minor, follow the change control process. The Guardians should finalise the change control process for Oracle HCM specific updates and enhancements to ensure all changes (enhancements or features) are raised via the correct channels, are tested sufficiently and appropriately, and are approved by the right stakeholders prior to work commencing on the change. Moreover, ensure that roles and responsibilities between Guardians and third parties such as Oracle and [redacted] who provide support for changes (i.e., design, development, testing, deployment) for Oracle Cloud HCM are clearly defined and managed.
Management Agreed Action	A change control process will be established between HR, IT and third parties, ensuring the roles and responsibilities of all parties. **Owner:** [redacted] **Completion Date**: 30 April 2022

3.10. Roles and responsibilities for delivering training to testers was not clearly defined	
Category	Testing
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	Prior to entering user acceptance testing (UAT), an expectations gap for training delivery requirements was identified between the Guardians and their implementation partner [redacted]. The Guardians expected that [redacted] would provide 'train the trainer' style training based on what was captured in their Statement of Work, which would entail training someone internally as a trainer, who would then train end users. However, [redacted] only expected to deliver system administrator level (i.e., 'train the admin') training. While there was no dedicated training for testers prior to UAT, we understand that the Test Lead did provide on the day briefings and the project team were available in-situ with the testers while UAT was being conducted, while this was a deliberate project decision it is recommended that this is reviewed moving forward to ensure that all testers have a level of familiarity with the system prior to testing. This expectation gap meant there was the risk that insufficient training was provided to testers, which could lead to ineffective execution of test cases and identification of issues. In the future, the Guardians should: • clearly define roles and responsibilities in training delivery, particularly if reliance is placed on a third party, and ensure sufficient training is provided to testers to ensure they are familiar with the system, and/or any systems supporting management andexecution of testing, such as Azure DevOps in this case to facilitate efficient execution of test cases and supporting activities, for example, expectations of testers, how testers can perform tests and record results, and how to raise bugs arising from testing for resolution.

3. Detailed Observations

Management Agreed Action	Apply learnings from O365 rollout project whereby familiarisation sessions were held with relevant stakeholders to prepare them for UAT. Including the differentiation between functional testing and UAT. This will familiarise testers with the changes and impacts before they do the testing. Project gates need to specify entry and exit points for UAT. This was specified in the test strategy but not followed. In future phases of the project, we will ensure that we define roles and responsibilities in training delivery and ensure clear expectations prior to commencing UAT. This will include determining the system training to be provided to testers. **Owner:** [redacted] **Completion Date**: 31 August 2022 (in time for planning for Phase 2 UAT)
3.11. Benefits to be gained through transformation by adoption of Oracle-delivered functionality and processes may be diminished	
Category	Processes / Configuration
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	A decision was made early on in the project (approved by the Project Sponsor according to the decision log) to move away from the transformation approach (i.e. adoption of the delivered/out-of-the-box Oracle Cloud HCM processes and functionality) that was agreed by the Guardians' Board in the Project Business Case, towards more of a 'lift and shift' approach, whereby Oracle Cloud HCM would be adapted to accommodate the Guardians' existing HR processes, with changes where it made sense. This approach has led to a higher degree of configuration and customisation (~231 customisations) than what was initially intended and could result in diminished benefits for the Guardians as the Oracle Cloud HCM functionality is not being used in the most optimal way (e.g., manager self-service transactions are limited, leaving most with HR). With a higher level of configuration comes the risk of support issues with each quarterly release of new functionality from Oracle. Further, as the co-design process was stopped early in the process, there is a risk that User Adoption may be compromised if there has not been enough focus on employees / managers in the design. What typically works well for other organisations, and our recommendation, is including non-HR users in the design and testing phases of the Project to get their buy-in from the start and throughout the project. (Refer action 3.1 (2)) There is also significant personalisation to achieve the Guardians' look and feel and to limit access to functionality such as screens that are not used (e.g., questionnaires) and fields. For example, access to the My Client Groups springboard is limited to certain security roles. Some personalisations are particularly complex and may require a higher level of technical expertise to support. Approval rules have been configured to meet the Guardians' requirements and some are quite complex. It is noted that some personalisations have been implemented to limit access to functionality that is not used now, but will be enabled during a future phase, and may therefore be removed at a later stage (e.g., Goals Management tile). With a higher level of configuration comes the risk of support issues with each quarterly release of new functionality from Oracle. It is recommended that the Guardians perform an impact assessment for each new release to identify any Oracle HCM (including Oracle Guided Learning – Oracle's contextual help tool) configuration impacts (on functionality, personalisations and approval rules) and regression test the configuration changes for every quarterly release in both test and production (to the extent possible in production). The Guardians should determine how ongoing Oracle HCM changes could be included in the Guardians' existing IT change process.

3. Detailed Observations

Management Agreed Action	The process by which the impact assessment would be undertaken, and the full set of regression testing, established by the project team and overseen by the Test Manager (this team went through 2 quarterly releases during, and immediately after, the project phase) was already completed as part of handover to HR BAU. The Oracle HCM Specialist (who started December 2021) has been trained on the quarterly release process. Agreement is already in place on how to use the existing IT change process for quarterly release management. **Owner:** [redacted] **Completion Date:** Completed.
3.12. Responsibility needs to be assigned for configuring new Payroll Calendars	
Category	Support / Maintainability
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	Pay calendars have been created up until June 2025 as part of the implementation and will be required for each pay period (i.e., fortnight) going forward. The Guardians should ensure that someone in the support structure has responsibility to create pay calendars in Oracle Cloud HCM. Although employees are not paid using Oracle Payroll, this functionality needs to be configured for the payroll integration to the [redacted]-managed DataPay system.
Management Agreed Action	An annual task has been set up as part of HR processes to ensure the payroll calendars are configured on a rolling 12-month basis. **Owner:** [redacted] **Completion Date**: Completed
3.13. Project Management processes not as rigorous as they could be	
Category	Project Management / Processes
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	Prior to the new Project Manager commencing a detailed project plan was in place, however, it was not widely understood or adhered to. The new Project Manager introduced a more detailed Project Plan from August 2021. The level of detail in this new Project Plan is more appropriate, however, the Guardians need to check going forward that all tasks have resources and predecessors allocated. Change requests do not appear to have considered timeline / resource impact. For example, CR001 (historical data migration), CR002 ([redacted]), CR006 (historical data migration in production), CR007 (additional notifications for Core HR), CR009 (additional notifications for Core HR), CR010 (OGL support), CR013 (additional refinements identified in UAT), CR015 (21C analysis) included extra scope and did not appear to have

3. Detailed Observations

	changed the project timeline, eventually compounding and leading to schedule delays, covered by subsequent change requests. Going forward, change requests should include an impact assessment that covers timeline and resources. As was observed in the internal project review, there has been some confusion regarding the waterfall vs. agile implementation approach. This observation is included here for completeness. Guardians should work with [redacted] in planning the next phase to clarify if waterfall, agile or a hybrid approach should be used. The risk/issue management process could be more rigorous. It was noted that some risks were missing owners and/or risk responses, some seem to be closed that would be relevant to the next phase, potentially because risks are being tracked by phase. Several risks were realised (i.e., became issues) but they do not appear to be tracked as issues. Approximately 40% of the risks in the log provided were realised as issues, indicating that the risk management process could be more effective. Also, the Potential Risks to Benefits Realisation in the Benefits Management Plan are missing likelihood, level of impact, owner, etc. Recommend these be included in the updated version and the risks tracked as part of the overall risk/issue process. The decision process could also be more rigorous. Some decisions were closed without an actual decision recorded. Also, some significant decisions seem to have been made by individuals rather than the Project Board. A decision framework should be adhered to help identify decisions that should go to the Project Board such as the decision regarding the implementation approach and the degree of transformation to implement. Also, a more rigorous decision process may help to formalise decisions made and reduce the re-litigation of decisions which has been previously observed in the internal project review. Overall, more rigour and compliance with project management processes is recommended going forward to introduce a higher level of control and certainty for future phases and thereby reduce the risk of delays in future phases.
Management Agreed Action	For future phases of the project, we will ensure more rigour is adopted in the project management processes by the project team to ensure adherence to the Project Management and Governance Frameworks put in place. We will also clarify the roles and responsibilities on the project. **Owner:** [redacted] **Completion Date**: 31 May 2022

3. Detailed Observations

3.14. Elevated reliance on support provided by and limited oversight of third parties for Oracle HCM	
Category	Third Party Arrangements
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	Oracle HCM is delivered as a Software as a Service (SaaS). This is advantageous as end users, such as the Guardians, do not need to acquire expensive hardware and other infrastructure to be able to host the solution. Instead, the Guardians rely on third party service providers such as the vendor Oracle (owner of Oracle HCM) and [redacted] HRM (an external support partner) to provide ongoing support for Oracle HCM. For Oracle, there are service organisation controls (SOC) reports available, including SOC 1 Type II, SOC 2 Type II and SOC 3, that provide details on the design and operating effectiveness of controls such as IT general controls, security, user access management, change controls, confidentiality, availability and integrity, backups management and disaster recovery procedures to name a few. The Guardians obtains limited third-party assurance from the vendor [redacted]. There is reliance on [redacted] to provide ongoing support in the year following implementation arising from a project decision. However, the support agreement with [redacted] has limited service level agreements (SLAs) that they will be measured against to provide support services. In the absence of a readily available SOC report for [redacted], ensure that regular reporting is in place to monitor [redacted]'s performance against any SLAs and the Guardians can obtain assurance over any third-party risks associated with exposure to [redacted]. We did note, however, that SOC reports for Oracle HCM were reviewed as part of the IT certification and accreditation process completed prior to go live. Going forward, the intention is to perform these reviews as part of the annual review cycle, as indicated by the Guardians' IT Security Manager. This will ensure that there is ongoing monitoring of Oracle vendor-provided services to ensure that the Guardians is comfortable with the control environment and that any residual risks are being identified and addressed timely through existing controls within the Guardians' own internal controls environment. At a minimum, the timing, form and content of these reviews should include: • An assessment of the continued availability of the Oracle HCM application and data hosted. • Consideration of how Oracle HCM would perform with changes in increased system usage volumes and acceptable recovery timeframes from system outages. • Performance against Key Performance Indicators (or similar) as set out in the relevant service agreements.
Management Agreed Action	HR will undertake periodic reviews of [redacted] and Oracle HCM supplier relationships in accordance with the third party monitoring requirements in the Procurement and Outsourcing policy. This will include ensure are meeting our service expectations and assessing the risks we are exposed to through the third party relationship are within the Guardians tolerance for risk. Where necessary, service expectations with the third parties will be clarified and updated into the SLA with the third party. **Owner:** [redacted] **Completion Date:** 31 October 2022

3. Detailed Observations

3.15. Third party contracts management and performance monitoring could be improved, in terms of defining roles and responsibilities and consistency of execution	
Category	Third Party Arrangements
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	Although there is a Guardians procurement framework in place under which supplier management sits, there is currently inconsistency in the approach taken for supplier contracting at both a project and business as usual level. Responsibility for managing a specific third-party contract is devolved to the natural owners of those contracts. However, in certain cases, ownership of a supplier contract has not been clearly defined. For example, it is not clear who owns the relationship with the third-party supplier Oracle (e.g., if it sits with HR, IT, and/or finance). Management have stated that this is a work in progress and relationship owners will be better defined in the future as third-party risk management practices are overhauled. As such, there is currently high reliance on institutional knowledge and key individuals, often without the benefit of fit-for-purpose processes and guidance and templates to drive consistent, repeatable, good practice. In the third-party contracts reviewed, contract variability was identified, with inconsistencies in terms and conditions, and the absence of or limited key performance indicators. At a minimum, the Guardians should look to standardise new and existing contracts with third parties, where possible and if appropriate, using a fit-for-purpose procurement management framework to ensure supplier management practices to drive effective monitoring of supplier performance. In addition, ensure that roles and responsibilities of these third parties are clearly defined, and contracts are owned by the appropriate Guardians role. From our understanding, the Guardians' legal team has introduced standardised terms and conditions for contracts as of September 2021, which will look to drive consistency within contracts as a starting point. However, this will not address inconsistencies or omissions in baseline requirements, including roles and responsibilities and key performance indicators, that suppliers should be assessed against for the Guardians to obtain assurance that third parties are meeting their contractual, including performance, obligations. Moreover, third party contracts are not standardised, and key performance indicators have not been clearly defined or are absent from contracts. Moreover, management has stated the minimum baseline for supplier roles and responsibilities have not been clearly defined in several HR contracts, partially driven by supplier-provided contracts, rather than templates used by the Guardians. As a result, monitoring of third-party performance is difficult to achieve. From a project perspective, roles, and responsibilities for who should be monitoring these contracts was unclear therefore monitoring was not performed consistently or at all for all third parties involved in the Oracle HCM implementation. For future projects, the Guardians should ensure that roles and responsibilities for third party monitoring should be agreed upfront, key performance indicators and third-party roles and responsibilities clearly defined within contracts. Regular monitoring should be performed by all these third parties, for example, during regular meetings and reporting reviewed by appropriate Guardians staff to ensure performance against key performance indicators, which are defined in contracts, is being adhered to. Reporting formatting should be agreed upfront, with the Guardians comfortable with the contents reported, and with any updates made to reports provided during the support arrangement.

3. Detailed Observations

Management Agreed Action	The Guardians have a formal procurement and outsourcing framework. A standard contracts template has also been recently developed by the Legal Team. While we may request suppliers to adopt our preferred contract terms, it may not always be possible, e.g., large multi-national suppliers will often not deviate from their own standard contracts. Also, at the time of the project all contracts were reviewed by the Legal team, consistent with internal processes. For any new or existing contracts due for renewal, we will explore the extent contract arrangements can be standardised. Also, as part of contract negotiations we will ensure key performance indicators and third-party roles and responsibilities are clearly defined. **Owner:** [redacted] **Completion Date:** Ongoing at time of new or existing contract renewals.
3.16. Insufficient visibility over testing performed by third parties	
Category	Testing
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	The Guardians had limited visibility over testing performed by third parties, including details of test scripts and results. For example, [redacted] only performed basic unit testing of code for the DataPay component and [redacted] verified any changes made but formal testing was left to the Guardians to complete. Moreover, we identified that [redacted]'s methodology 'Cloud HR to the Point' meant that the Guardians had to incorporate a decision to apply the 'V' model to their testing approach. However, there is the risk that [redacted] were performing testing that was not in line with their methodology. A higher degree of clarity needs to be provided by third parties involved in delivering changes and/or performing testing for Oracle HCM or any of its integrations. For instance, this could include vendors providing evidence of test scripts and results in test exit reports and documentation verifying successful completion of testing. Insufficient testing in the early stages of the project can lead to defects in later stages. As a rule, the later a defect is found in a project, the harder it is or longer it takes to resolve. For future phases, the Guardians should ensure that sufficient comfort and clarity is obtained from all third parties delivering changes into the Guardians' environment and/or performing testing, and that activities performed by third parties are verified with documented evidence and are in line with the Guardians' expectations and master test strategy.
Management Agreed Action	For future phases we will ensure that the third parties provide proof of testing, evidence of what has been tested and the results before it is handed over to Guardians for our testing. Azure DevOps will be used to manage defects and refinements to prevent confusion when tracking and managing changes and testing; this will bring more structure to the process. **Owner:** [redacted] **Completion Date:** 31 May 2022

3. Detailed Observations

3.17. Data migration dry runs or mock conversions could not be evidenced	
Category	Data Migration
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	There was a comprehensive data migration report following the data migration to production with details of the success and failure of each data load, and prior to that there was one data migration dry run in the test environment to test that the data could be migrated successfully ahead of the migration to production. Typically, there would be two to three dry runs including a final dress rehearsal (whereby the whole production migration is rehearsed). This also gives the project team the opportunity to perform testing (ST, SIT, UAT) with real data. The use of dry runs helps to minimise the number of data migration issues in the migration to production and the risk of data issues in production once transactions are performed with the real data. It is noted that Guardians also executed Production Verification Testing (PVT) following the data migration to production, helping to minimise data issues in production post go live.
Management Agreed Action	We note that dry runs of data migration were undertaken on the project. The problems encountered were less about data migration and more about the lack of a clear data strategy. For future phases of this project, we will ensure that the data strategy we are going to use for testing and the implications of using this data and the access to it are well understood and documented in the planning and requirements phase of the project. The strategy will specify the agreed criteria for how we will treat sensitive data, with appropriate security and NDAs if required. It will also specify the data types including those which should be hashed or where dummy data is more appropriate. We will ensure that adequate (e.g., two or three) dry runs or mock conversions are done before moving to production. **Owner:** [redacted] **Completion Date:** 30 April 2022
3.18. No evidence of a code repository for the storage and control of code related to customisations	
Category	Support / Maintainability
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	There is no evidence of a code repository for the storage and control of code related to Oracle HCM customisations. These customisations may include custom integrations, reports, personalisations and/or workflow. The customisations are documented in the designs prepared by [redacted], however, it is not clear where that documentation resides for ongoing support and maintenance and who is responsible for that documentation going forward. Guardians should agree a process and method for storing, controlling and maintaining the code related to the Oracle HCM customisations to ensure that the code is supportable going forward.

3. Detailed Observations

Management Agreed Action1.	1. We will work with [redacted] to agree a process and method for storing, controlling and maintaining the code and related documentation for theOracle HCM customisations. The repository will be independent to the Oracle Services Cloud environment and documentation should be written that any Oracle HCM implementation partner could support Guardians. **Owner:** [redacted] **Completion Date**: 30 April 2022
3.19. Roles not designed as per Guardians' future requirements	
Category	Access Management/Security
Risk Rating	**Moderate** (Likelihood: Possible / Impact: Minor)
Observation	In our review, we note that there was limited design due diligence on the roles in the application and how these were provisioned to the users. The principle followed was to mirror the access in Oracle to what the users had in the legacy application. A roles matrix was not developed pre-implementation that clearly outlined roles, their associated access rights, implications on approvals and specific considerations around segregation of duties. Role provisioning was approved by the Head of HR Ops based on the limited information provided by the implementation partner. Furthermore, there was no evidence of unit testing performed by [redacted] to verify if access rights configured for each Oracle HCM role was in line with expectations (i.e., no testing done to validate what can and cannot be accessed). Finally, we understand there was no design conversation on how the copies of seeded Oracle roles would be created, e.g., full hierarchy or only top-level roles copied and the impact this might have on the future functionality released by Oracle. If system access is not in line with the future Oracle HCM processes or commensurate with the users' business roles, this may lead to segregation of duties or excessive or inappropriate access within the system.
Management Agreed Action	In future project phases we will ensure: • That this be included in future state mapping, part of requirements gathering. • There is a thorough understanding during creation of roles from seeded Oracle roles e.g., copying full hierarchy roles vs top-level roles; and • Unit testing is performed by [redacted] to verify if access rights configured for each Oracle HCM role was in line with expectations. **Owner:** [redacted] **Completion Date**: 30 April 2022

4. Improvement Opportunities

From this internal audit, improvement opportunities were also identified from the phase that has already been completed, with lessons to be considered for future projects. Refer to the following table for details.

4.1. Project was delayed	
Category	Project Management
The project went live approximately 15 weeks behind schedule. The go live date was originally planned as 20 July 2021, with an eventual go live date of 1 November 2021. This observation has been well documented in the mid project Internal Review and is included here for completeness. The recommendation is that the Guardians work closely with [redacted] to plan future phases. Any future planning should not only consider [redacted] implementation activities but also any Guardians activities (e.g., Change Management, Business Readiness, etc.) and third party project activities/dependencies.	
4.2. Design process not as rigorous as it could be	
Category	Processes / Configuration
[redacted]'s lead functional/technical resource seems to be highly skilled / experienced with implementing Oracle HCM from the design documentation that was reviewed. However, [redacted]'s approach to design is unclear from the documentation reviewed, including the [redacted] statement of work. This lack of clarity regarding the design process may have contributed to a higher level of configuration and a higher number of defects and enhancement requests for Phase 1. We recommend that the Guardians work with [redacted] to firm up and align on the approach prior to the next phase to reduce the risk of defects and enhancement requests in future phases.	
4.3. Resource constraints during project	
Category	Operating Model
It has been observed that there were resource constraints with the Business Owner performing multiple roles therefore taking their time away from the project. This observation has been well documented in the mid project Internal Review and has been included here for completeness. We recommend that resource requirements are considered as part of the planning process for future phases.	

4. Improvement Opportunities

4.4. [redacted] resource changes at critical stage of project	
Category	Operating Model / Third Party Arrangements
There was a change in [redacted] Project Manager at a critical point in the project, i.e., just prior to go live. Although [redacted] consulted with the Guardians and this change was agreed, it is recommended to have named key resources/roles in supplier contracts where possible and require agreement between the Guardians and the supplier before changing key resources to limit this risk in future. That said, it is recognised that resignations by third party resources cannot be controlled.	

4.5. User acceptance testing processes could be improved	
Category	Testing
User stories were initially developed as part of the user acceptance testing (UAT) plan to support the definition of test cases and mapping to associated business processes in the absence of detailed business requirements. However, documentation was not completed, and not all business processes were covered due to resource or time constraints from the subject matter experts involved in the Oracle HCM implementation. The Guardians should ensure that for future projects, potential time and resources constraints are identified and addressed to improve UAT processes and support execution of test scripts. This will assist in identification of bugs to be resolved. In some implementations, business users even get involved in earlier phases of testing such as System Testing to allow early identification of issues and to accelerate user adoption, assist with change management and acceptance of delivered functionality and processes. Moreover, full end to end UAT could not be completed due to the absence of test environments for Oracle HCM integrations with internal or external systems (for example, the Guardians' Azure Active Directory and the payroll system, Data Pay, managed by [redacted]). These limitations were identified during the project and impacted the extent of testing. If limitations are identified during a project, the Guardians should ensure they are identified upfront and factored into any testing strategies, ensuring contingency processes are established to perform limited testing to the extent that it is possible. We understand some of these limitations were documented in the master test strategy to acknowledge that not all possible scenarios could be tested due to technical, environmental or resource constraints. During the project, many UAT and Hypercare defects have been raised. Rigorous testing was performed by the Guardians' subject matter experts, contributing to the identification of a large number of defects. The Guardians should review whether these defects relate to areas tested during System Test and UAT (for Hypercare defects) as this may be linked to insufficient testing during those phases. For future project phases, the Guardians should implement additional fields or tags in Azure DevOps to track the root cause of defects and additional categories to track functional areas. Moreover, ensure UAT scripts are system tested prior to commencement of UAT, and that more formal system testing by [redacted] is performed prior to SIT and UAT. In some implementations, business users even get involved in earlier phases of testing such as System Testing to allow early identification of issues and to accelerate user adoption and acceptance. The Guardians have stated that a 'shift left' testing approach will be adopted for requirements design and analysis in Phase 2 delivery.	

4. Improvement Opportunities

4.6. Automated testing options can be considered if practical	
Category	Testing
Automated testing is not currently being utilised by the Guardians for executing test cases (particularly regression testing) in Oracle Cloud HCM, but potential options are being explored by the Guardians Test Lead.	

4.7. Inconsistent use of the term 'Team' rather than 'Department'	
Category	Processes / Configuration
In the [redacted] configuration document, it appears that in some places the field label 'Department' has been replaced with the field label 'Team', but in some places it remains as 'Department' (e.g., Hire Employee). It is unclear if this inconsistency is intended. Recommend that the Guardians review this design if the inconsistency is unintended.	

Appendices

Appendix A – Scope and Approach

We set out below the scope of work completed:

a. Scope

The objective of the assignment was to undertake an internal audit of selected aspects of the Oracle HCM system and supporting processes, highlighting improvement opportunities/weaknesses and recommendations for improvement.

The internal audit started with a desktop assessment of key design elements of phase 1 (Core HR, Recruitment and Onboarding, Payroll integration), by reference to design documentation provided by the project team. We understand the Guardians project team has tight timelines through to go-live on 1 November 2021 and has limited availability. The purpose of the first part of the internal audit was to help identify any significant red flags from a desktop review that the Guardians need to be aware of before go-live. Following go-live, the internal audit focused on the implementation of controls and supporting processes.

Other phases and areas of focus may be added to scope if requested by the Guardians and agreed in writing.

The scope of the internal audit focused on how the Oracle HCM system has been designed to support 'fit for Guardians' internal controls leveraging good practice where relevant. This included:

A) Desktop Assessment Pre-Implementation

HR process design, including security:

- The design of key HR processes, and how this supported quality information
- Consideration of automated controls to be configured within the system and how this supported the designed business rules, including identifying whether there were further opportunities for improvement
- Understanding how the project has understood how the core HR configuration impacts downstream dependencies for later phases/functionalities of the setup
- User access design, including segregation of duties and privileged access (including any employee self-service).
- Authentication/access security (password security, user sign-on etc.).

Project Development Controls

- How data was migrated accurately and completely from legacy systems to Oracle HCM.

B) Post Implementation, Implementation Assessment

HR process implementations, including security:

The implementation of key HR processes, and how this supported quality information

- Consideration of automated controls actually configured within the system and how this supported the designed business rules, including identifying whether there are further opportunities for improvement
- User access implementation in accordance with design, including segregation of duties and privileged access (including any employee self-service).
- The implementation of authentication/access security (password security, user sign-on etc.).

Business as Usual Processes and Risks:

- Access management (e.g., provisioning) and monitoring/ Privileged Access management
- Interface processing confidentiality and integrity (accuracy and completeness) between Oracle HCM and other systems such as [redacted]* and [redacted]payroll or the design of manual data update processes
- Third party IT support arrangements adequacy of contractual arrangements/ clarity of roles and responsibilities between Oracle/other key third party support providers and the Guardians
- Clarity of roles and responsibility for maintaining and operating Oracle HCM as applicable to a SaaS environment. This focused on:
  - Back-up and restore expectations including periodic testing
  - Software change management including pre/post testing
  - Business continuity management considerations
  - Third party risk management monitoring.
- Process Continuity/resilience / contingency arrangements etc.

Other considerations

- The extent to which a privacy impact assessment was performed.
- The impact customisations may have on the future maintainability of Oracle HCM when standard Oracle patches or feature updates are released.

**No direct integration from Oracle HCM to [redacted]. DataPay integrates with [redacted].*

Appendices

b. Approach

As requested, the scope of work was performed in at least two main tranches:

Desktop Assessment Prior to go-live:

- A desktop assessment of business process and other relevant documentation
- Limited interviews with the project team/management and other relevant contacts to confirm our understanding.

Post go-live process and controls implementation:

- An observation and walkthrough of business processes and controls as implemented
- Observations of system settings, configurations, or onscreen walkthroughs
- Reading key documents as relevant to the scope.

c. Our responsibilities and limitations

This assignment does not constitute a review, audit, or assurance engagement as defined in the standards issued by the External Reporting Board. Accordingly, this engagement is not an assurance engagement, nor is it intended to, and will not result in, the expression of an assurance, audit or review opinion, or the fulfilling of any statutory audit or other assurance requirement.

Our report will be prepared for the sole benefit of the Guardians for the purpose set out above. Our report is not intended for general circulation or publication (including on an internet website) and should not be reproduced or used for any purpose other than set out above, without our prior ·written consent. Even if such consent is provided, we will accept no responsibility or liability to any third party in respect of the contents of our report. In addition, we will not accept any responsibility or liability for losses incurred by you or any other party as a result of the circulation, reproduction or use of our report contrary to the provisions of this paragraph.

The procedures we will perform may not detect all cases of financial fraud, processing errors or suspicious transactions, even if material. This is because there are inherent limitations with data analytic procedures. Our follow-up will be on a sample basis, and frauds could occur in ways that have not been anticipated or are otherwise outside the scope of the procedures performed.

d. Our responsibilities and limitations

Management remains responsible for the appropriate implementation and of an adequate internal control system. An effective internal control structure reduces the likelihood that errors, irregularities or illegal acts will occur and remain undetected; however, it does not eliminate that possibility. Accordingly, while we cannot guarantee that errors, irregularities or illegal acts, if present, will be detected,we will assist management in designing our internal audit procedures, however it is management's responsibility to determine whether those procedures are sufficient for their purposes.

PwC has not been engaged to, and we will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee or otherwise engage in any activity that in the judgment of PwC would be inappropriate in the capacity for performing internal audit assignments.

e. Inherent limitations

We shall use reasonable skill and care in the provision of the services set out in this letter. It is important to recognise there are inherent limitations in the internal auditing process. For example, internal audits are generally based on the concept of selective testing of the area being examined and are, therefore, subject to the limitation that material errors and irregularities and illegal acts having a direct and material financial impact, if they exist, may not be detected. Also, because of the nature of irregularities, including attempts at concealment through collusion and forgery, an internal audit may not detect a material irregularity. We will, however, inform management with respect to any illegal acts or material errors and irregularities that come to our attention during this internal audit.

All services will be rendered in good faith, by and under the supervision of qualified staff in accordance with the terms and conditions set forth in this letter.

PwC makes no other representation or warranty regarding either the services to be provided or any deliverables; in particular, and without limitation of the foregoing, any express or implied warranties of fitness for a particular purpose.

Appendices

Appendix B - Summary of Low Risk Rated Observations

Essential to address during future project phases:

Support and maintainability:

- Configuration documentation was missing details on Grade Rates due to sensitive data (e.g., salary details). The Guardians need to ensure support can be provided for Grade Rates following issues and configuration design can be accessed by support resources as needed. Secondly, configuration documentation was missing dashboards and reports, which should be obtained from [redacted], and had comments to be resolved for support purposes.
- Configuration documentation of the [redacted] integration was not available for our review that detailed how the integration is enabled (e.g., no details of whether options to capture PII Data and Send PII Data are enabled or not). These details should be documented for support purposes.

Future improvement opportunity:

Access management:

- Off system processes for user account creation.

Testing:

- Formal approvals not obtained for Oracle HCM master test strategy
- Automated testing options can be considered if practical to reduce time spent on manually testing each quarterly release

Privacy impact assessment:

- Approvals for the Oracle HCM certification and accreditation and privacy impact assessment were not formally documented, and privacy impact assessment could be updated for completeness (i.e., sections had incomplete information or required clarification).

Business processes or configuration:

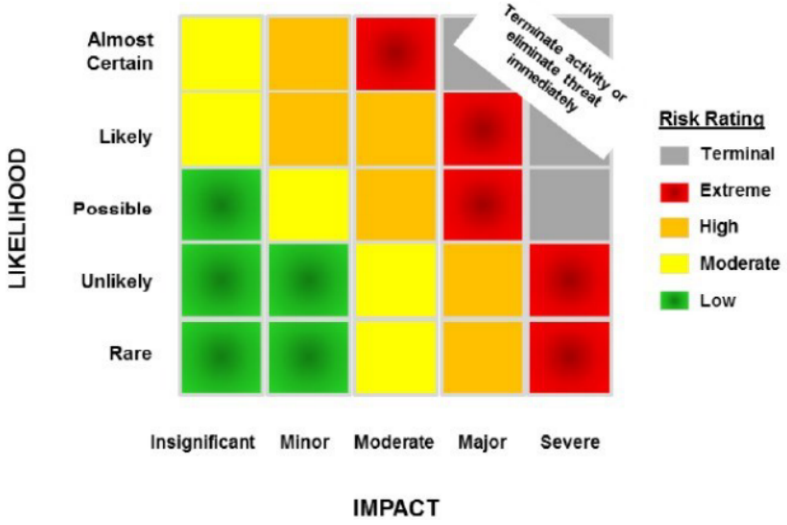
- From the config documents, the Administrator Profile Value [redacted] has not been enabled for Guardians. This function can be enabled to limit the Position List of Values to approved positions only for user friendliness.
- CREATE Job Requisition process has up to five levels of reviewer / approver for a requisition.
- Quality of design documentation may impact application support.

Appendices

Appendix C – Risk Rating Matrix

The risk rating framework from the Guardians' Risk Management Policy was used to apply risk ratings based on an assessment of likelihood and impact for each of the detailed observations.

LIKELIHOOD	Description
Almost Certain	The event is expected to occur in most circumstances (95% chance of occurring in next 12 months or in 19 out of every 20 years)
Likely	The event will probably occur at some time (50% chance in next 12 months or in 10 out of every 20 years)
Possible	The event may occur at some time (25% chance in the next 12 months or in 5 out of every 20 years)
Unlikely	The event is unlikely to occur (10% chance in the next 12 months or in only 2 out of every 20 years)
Rare	The event will occur only in exceptional circumstances (4% chance or only once every 25 years)



Business Risks		
	Unintended profit or loss impacts	**Processes**
Severe	$20m - $30m	Failure of project of between $20m - $30m. More than 10 instances of fundamental process failure leading to complete breakdown of operations
Major	$10m - $20m	Failure[1] of project of between $10m and $20m Qualified audit report Custodian Normal operational errors >400 errors Custodian Major errors >24 pa Organisational errors reported to the Audit Committee > 24 pa
Moderate	$5m – $10m	Failure of project of $5m - 10m Any OAG ESCO audit grade "Poor" Restatement of financial accounts or Fund performance Custodian Normal operational errors >300 errors Custodian Major errors >12 pa Organisational errors reported to the Audit Committee > 12 pa
Minor	$1m - $5m	Failure of Project of $1m - 5m
Insignificant	-	-

[1] Failure of a project means any of the following: (1) No project benefits will be realised; no project success measures will be met; and/or the project will be stopped.

Thank you