City of Nedlands

Agenda

Audit & Risk Committee Meeting

9 November 2020

ATTENTION

This Agenda has yet to be dealt with by the Committee.

The Administration Recommendations, shown at the beginning of each item, have yet to be considered by the Committee and are not to be interpreted as being the position of either the Committee or Council.

The Minutes of the meeting held to discuss this Agenda should be read to ascertain the decision of the Committee.

Before acting on any recommendation of the Committee a check must also be made in the Ordinary Council Minutes following the Committee Meeting to ensure that Council did not make a decision at variance to the Committee Recommendation.

Mark Goodlet
Chief Executive Officer
30 October 2020

Table of Contents

City of Nedlands

Notice of a meeting of the Audit & Risk Committee to be held on Monday 9 November 2020 at 5.30 pm online via teams. Committee Members and the public are permitted to attend in person in the Council Chamber, at 71 Stirling Highway, Nedlands.

Audit & Risk Committee Agenda

Declaration of Opening

The Presiding Member will declare the meeting open at 5.30 pm and will draw attention to the disclaimer below.

Present and Apologies and Leave of Absence (Previously Approved)

Leave of Absence **(Previously Approved)**	None at distribution of agenda.
Apologies	None at distribution of agenda.

Disclaimer

Members of the public who attend Council meetings should not act immediately on anything they hear at the meetings, without first seeking clarification of Council's position. For example by reference to the confirmed Minutes of Council meeting. Members of the public are also advised to wait for written advice from the Council prior to taking action on any matter that they may have before Council.

Any plans or documents in agendas and minutes may be subject to copyright. The express permission of the copyright owner must be obtained before copying any copyright material.

1. Public Question Time

A member of the public wishing to ask a question should register that interest by notification in writing to the CEO in advance, setting out the text or substance of the question. Questions tabled at the meeting may be unable to be answered due to the requirement for technical research and will therefore be answered directly afterwards.

Questions must relate to a matter contained within the agenda of this meeting.

2. Addresses By Members of the Public (only for items listed on the agenda)

Addresses by members of the public who have completed Public Address Session Forms will be invited to be made at this point.

3. Disclosures of Financial and/or Proximity Interest

The Presiding Member to remind Councillors and Staff of the requirements of Section 5.65 of the Local Government Act to disclose any interest during the meeting when the matter is discussed.

A declaration under this section requires that the nature of the interest must be disclosed. Consequently a member who has made a declaration must not preside, participate in, or be present during any discussion or decision making procedure relating to the matter the subject of the declaration.

However, other members may allow participation of the declarant if the member further discloses the extent of the interest. Any such declarant who wishes to participate in the meeting on the matter, shall leave the meeting, after making their declaration and request to participate, while other members consider and decide upon whether the interest is trivial or insignificant or is common to a significant number of electors or ratepayers.

4. Disclosures of Interests Affecting Impartiality

The Presiding Member to remind Councillors and Staff of the requirements of Council's Code of Conduct in accordance with Section 5.103 of the *Local Government Act*.

Councillors and staff are required, in addition to declaring any financial interests to declare any interest that may affect their impartiality in considering a matter. This declaration does not restrict any right to participate in or be present during the decision-making procedure.

The following pro forma declaration is provided to assist in making the disclosure.

"With regard to the matter in item x ….. I disclose that I have an association with the applicant (or person seeking a decision). This association is ….. (nature of the interest).

As a consequence, there may be a perception that my impartiality on the matter may be affected. I declare that I will consider this matter on its merits and vote accordingly."

The member or employee is encouraged to disclose the nature of the association.

5. Declarations by Members That They Have Not Given Due Consideration to Papers

Members who have not read the business papers to make declarations at this point.

6. Confirmation of Minutes

6.1 Audit & Risk Committee Meeting 5 October 2020

The minutes of the Audit & Risk Committee held 5 October are to be confirmed.

7. Matters for Which the Meeting May Be Closed

Council, in accordance with Standing Orders and for the convenience of the public, is to identify any matter which is to be discussed behind closed doors at this meeting, and that matter is to be deferred for consideration as the last item of this meeting.

There are no matters for which the meeting may be closed.

8. Items for Discussion

Note: Regulation 11(da) of the *Local Government (Administration) Regulations 1996* requires written reasons for each decision made at the meeting that is significantly different from the relevant written recommendation of a committee or an employee as defined in section 5.70, but not a decision to only note the matter or to return the recommendation for further consideration.

8.1 Internal Audit Action Log

Committee	9 November 2020
Applicant	City of Nedlands
Employee Disclosure under *section 5.70 Local Government Act 1995*	Nil.
Director	Lorraine Driscoll – Director Corporate & Strategy
Attachments	1. Internal Audit Actions Log – Main; and 2. Internal Audit Actions Log – Archive.
Confidential Attachments	Nil.

Executive Summary

The attached Internal Audit Actions Log contains details of the matters raised by the Auditors during the City's Internal Audit program. The list apportions information detailing the Log Reference, Dates – Open, Due and Closed, Business, Audit Status, Name and Action, Owner, Original and Revised Due Dates, Action, Owner and Status Comments.

The recently updated Internal Audit Actions Log is presented to the Audit and Risk Committee members for their information.

Recommendation to Committee

The Audit and Risk Committee receives the Internal Audit Actions Log.

Discussion/Overview

An audit is a process through which internal control effectiveness is examined and assessed. The objective is to provide an audit for compliance with relevant management policies and procedures. Each internal audit undertaken results in actions being recommended to the City's Administration. These actions are monitored for completion using the Internal Audit Actions Log.

The attached list contains details of the Actions raised and outcomes.

The recently updated Internal Audit Actions Log is presented to the Audit and Risk Committee members for their information. We have recently updated the log to a more optimised process. All past items are under the Archive tab. The log will be managed on one page which is the Main sheet of the register.

Key Relevant Previous Council Decisions:

Nil

Consultation

Nil.

Strategic Implications

As part of the measures identified within the Community Strategic Plan for great governance and civic leadership, ongoing management of internal audit items assists towards this goal. This register has improved our ability to identify and manage both audit items and potential risk.

Who benefits?

All (specify who) will benefit from a more streamlined method of capture and simpler method of filtering closed and open items.

Does it involve a tolerable risk?

This reduces the City's exposure to financial risks as it provides a method of management by measuring the City's actions and outcomes.

Budget/Financial Implications

Nil.

Any actions requiring expenditure that are not allocated to an existing budget item will be considered by Council during budget deliberations.

Main Audit Log

Audit Register 2020/21									
		Date					Audit		Status Comments
ID	**Open**	**Due**	**Closed**	**Business**	**Status**	**Name**	**Action**	**Owner**	**Status Comments**
1	Dec-15	Nov-20		Business Systems	Closed	Business Continuity Management Review	**Business Continuity Management Review** Workshop and update to current plan and then produce new plan	Manager Business Systems	**28 Oct: Closed** **5 Oct:** Status Not Changed **23 Sep 20:** Workshop has been carried out, updated plan has been received and updated. The plan it self now required sign off by EMT to be completed. **3Aug20:** Both strategy and presentation have been drafted and await executive endorsement. **Jun20:** Manager Business Systems is going to develop a Digital Stategy by Aug 2020 which will address the matters raised here. Further, a strategic plan will be developed by Oct 2020. **Sept19:** The IT Strategic Plan will be developed once all recommendations made in Final IT Audit Report has been addressed and the relevant policies, procedures and plans have been created. **Feb19:** All policy, procedures and plans will be developed and adopted in line with the final IT audit report to ensure all recommendations are included. **Nov18:** IT Strategic Plan to be formulated following development of corporate strategy.
2	Dec-15	Nov-20		Business Systems	Closed	IT General Controls	**Formalisation of IT Strategic Plan (3.3.1)** Due to changes to IT infrastructure, development of IT Strategic Plan is crucial to ensure business strategy and IT decisions are evaluated in alignment.	Manager Business Systems	**28 Oct: Closed** **15 Oct:** Presented to Managers and all have agreed in it direction and proposed actions **5 Oct:** Status Not Changed **3Aug20:** Both strategy and presentation have been drafted and await executive endorsement. **Jun20:** Manager Business Systems is going to develop a Digital Stategy by Aug 2020 which will address the matters raised here. Further, a strategic plan will be developed by Oct 2020. **Sept19:** The IT Strategic Plan will be developed once all recommendations made in Final IT Audit Report has been addressed and the relevant policies, procedures and plans have been created. **Feb19:** All policy, procedures and plans will be developed and adopted in line with the final IT audit report to ensure all recommendations are included. **Nov18**: IT Strategic Plan to be formulated following development of corporate strategy.
3	Dec-16	May-20		Finance	Closed	Control Self-Assessments	**Fraud Management Policy and Procedures (1)** Create a formal fraud management policy and procedure based on relevant industry standards.	Manager Financial Service	**28 Oct: Closed** **5 Oct:** No Change; awaiting approval **18Aug20:** No change; awaiting approval **Jun20:** Fraud and Corruption Policy and Fraud and Corruption Investigation and Reporting Procedure have been established. These documents are awaiting for EMT review and approval. **Sept19:** The City was audited by OAG as a part of their Performance Audit - Fraud Management Prevention in Local Government. Based on the outcome of the audit, the City is progressing to complete the full documentation of the Fraud & Corruption Framework and Relevant Policies & Procedures consistent with the OAG's findings and requirements. **Feb 19:** The policy has been reviewed by the Governance Officer. We are now progressing to complete the full documentation of the Fraud & Corruption Framework and Procedures consistent with the OAG's approach and requirements under their current audit. **Nov18:** The drafted policy is awaiting review by the Governance Officer

4	Nov-17	Jul-20		Finance	ork in progr	Payroll Review	**Review, update and implement documented payroll policy and procedures (pt 3)** Develop and document the Payroll Policy and update procdures to include: -Changes to payroll data -Tax file number declarations -Termination payments -Fortnightly payroll processing -Terminating employees payroll processing -Payroll month end reporting.	Manager Financial Service	**28 Oct closed** - Redundant New platform and service comming **5 Oct:** Awaiting Validation **18Aug20:** The audit actions are still outstanding. This is being raised again in the current Payroll Audit which has just been completed. **Jun20:** The Payroll Policy awaiting for the EMT review and approval. Once approved, the policy will be implemented. **Feb20:** Combined Payroll Policy and Procedure was presented to EMT for the approval. However, the recommendation was made to create a separate Policy and Porcedural document. Accordingly, a sperate Payroll Policy has been created and is awaiting for the EMT review and approval. **Nov19:** Payroll policy and procedures have been combined in a procedural document with the new legislation requirements incorporated and awaiting EMT approval. **Sept19:** Procedural document was finalised and was awaiting for the adoption. However, due to implementation of new Legislation the procedures needs to be amended and updated. Further, few relevant
5	Jan-19	Oct-20		Finance	ork in progr	Accounts Payable and Purchasing	**Purchasing Policy - Contract Variations (pt 3.3)** Develop monitoring controls to ensure that deviations to the guidelines around contract variations are detected and mitigated.	Manager Business Systems	**9 Nov:** Still in progress **5 Oct:** Still in progress **3Aug20:** - Currently in progress **Jun20:** The Procurement Coordinator is in the process of reviewing the exisiting controls and update them to enhance the monitoring process around contract variations. **Feb20:** The City is in the process of recruiting Purchasing and Tenders Coordinator. Existing Monitoring controls will be reviewed, finalised and managed by the appointed Purchasing and Tenders Coordinator. Nov19: Monitioring controls to detect contract varaiations will be managed via exception reporting. Currently, the reporting is being developed. **Jun19:** The Purchasing of Goods and Services Policy has been updated with the contract variations clauses. The monitoring controls will be updated as part of the purchasing procedures and process which will be rolled out once the policy is approved by the Council.
6	Jan-19	Oct-20	Aug-24	Business Systems	Closed	Accounts Payable and Purchasing	**Tender Process - Risk Assessment (pt 7)** Develop a risk assessment process to identify potential risks as part of tender process.	Manager Business Systems	9 Nov: Awaiting Validation 5 Oct: Signed off by EMT awaiting Validation 3Aug20: - This has been completed. Will send evidence to Internal Auditor to close out item. Jun20: The Procurement Coordinator is in the process of developing Risk Assessment Process. Once developed the Risk Assessment Porcess along with relevant documents will be approved and roll out within the City. Feb20: The City is in the process of recuriting Purchasing and Tenders Coordinator. The Risk Assessment process will be developed and mainted by the appointed Purchasing and Tenders Coordinator. Nov19: The Risk Assessment process was going to be developed by Purchasing and Tenders Coordinator. The Purchasing and Tenders Coordinator has resigned from the City and the development of the Risk Assessment process will be completed by the replacement officer. Jun19: To be completed after approval of policy by Council as part of the updated procedures and processes.
7	Jun-19	Dec-20		Business Systems	ork in progr	IT Policy review	Develop Privacy Policy and also policy to cover Data Breach Notifications (4.2.1)	Manager Business Systems	**9 Nov:** Cyber Security Policy Awaiting EMT Endorsement **5 Oct:** Still in Progress **3Aug20:** Currently work in progress. **Jun20:** The IT Department is in the process of creating Privacy Policy and to test it. Once developed and tested, the policy will be approved and implemented.

8	Jun-19	Nov-20	Business Systems	ork in progr	IT Policy review	Item #1 Review and update BCP. Carry out testing of the BCP to assess for appropriateness.	Manager Business Systems	**28 Oct** Ongoing **5 Oct:** Completed going to EMT for Sign Off **3Aug:** Remaining action is to carry out testing by re-creating a complete shutdown. The BCP has now been reviewed and the current BCP has been updated. A series of two workshop and a complete re-write will commence ofter that workshop. **20 Jun :** The review has been conducted by the Internal Auditors on Business Continuity Management Area as part of 2nd year Internal Audit Function. The review process is in progress but the BCP document has been updated to incorporate certain recommendations made as a part of Internal Audit Review. Once, the review is completed and the Final recommendations are received, the BCP document will be finalised and the testing will be conducted.
9	Jun-19	Aug-31	Business Systems	Closed	IT Policy review	Item #2 To consider update of the Business Information Systems document covering critical functions to increase effectiveness and usability of the document as per suggestions outlined in report.	Manager Business Systems	**28 Oct: Closed** **5 Oct:** Awaiting validation **3Aug20:** An entire suite of policies, procedures and governance have been developed and now awaiting validation.
10	Jun-19	Aug-31	Business Systems	Closed	IT Policy review	Item #6 Update Business Systems and Applications - System Application Change Management to ensure greater clarity around protocols for changes made by third parties.	Manager Business Systems	**9 Nov:** New Interface to JIRA according to ITIL service management - Awaiting Validation **5 Oct:** New interface being developed around (Request/Incident/Problem/Change/Release Management) **20 Sep:** In progress **3Aug :** The adoption of ITIL Service Management has been designed to use within our Service Desk Solution (JIRA). Once new workflow has been tested it will be adopted. The existing system will manage existing requests and close that interface. All new requests will be managed via the ITIL Service desk version which will manage Request, Incidence, Problems, Change, Release Management.
11	Jun-19	Oct-20	Business Systems	Closed	IT Policy review	Item #16 Change Control form - to update form to provide greater clarity around Go/No Go decision.	Manager Business Systems	**5 Oct: Repeat of item 10 (Closed)** **3Aug20:** IT Governance Framework has been defined and is currently waiting on EMT endorsement **Jun20:** The IT Department is in the process of changing form. Once updated the form will be approved and implemented.

CLOSED AUDIT ITEMS

Item ID	Log Referen	Audit	Audit Action	Original Due D	Revised Date	Action Owner	Completed - p	Status Comments	Validation comments
	2015Dec	Purchasing Card and Credit Card Control Assessment	**Include Card Cancellation process in the procedure (5)** Add card cancellation process to credit card procedure.	Dec-16	Sep-18		**Closed**	**Jan19: Validated via Accounts Payable & Purchasing audit** Nov18: Card cancellation process has been included in the procedure.	N/A
	2015Dec	Purchasing Card and Credit Card Control Assessment	**Formalise credit card financial delegations and update procedure (5)** A delegation process for use of credit cards belonging to a different card holder to be investigated and implemented.	Dec-16	Dec-18		**Closed**	**Jan19: Validated via Accounts Payable & Purchasing audit** Nov 18: Recommendation of replacing a delegation process with a control whereby an application by the card user and approval by the cardholder for each transaction.	N/A
	2015Dec	Project Management	**Project Management Information (3.4.1)** Develop a standard practice policy for storing project file folders and applying version control over key doucmentation.	Nov-15	Apr-18		**Closed**	**Jan19: Validation requires passage of time and review of internal practices in following standard.** Nov18: This solution became avaliable in December 2017.	Validated August 2020.
2	2015Dec	IT General Controls	**Backup and restoration testing (4.1)** Review the tapes backup process and determine if this process is still necessary due to the online replicaton of data.	Dec-15	Mar-19	Director Corporate & Strategy	**Closed**	**Feb19: Tapes back-up process is no longer relevant due to the City's online replication of data.** Nov18: Backup and recovery processes are being reviewed and will be tested in line with the Business Continuity requirments.	N/A
4	2015Dec	IT General Controls	**Change Management Procedures (4.2)** Develop change request form with sign-off when changes are made to IT infrastructure, systems and applications.	Dec-15	Dec-18	Director Corporate & Strategy	**Closed**	**Feb19: Documented has been approved and implemented.** Nov18: This policy has been developed and is awaiting approval by the Executive.	Reviewed during IT Policy review

CLOSED AUDIT ITEMS

6	2016Nov	Control Self-Assessments	**Accounts Receivable Policy and Procedures (1)** Develop Accounts Receivable policy and update current procedures.	Jul-18	Dec-18	Manager Financial Services	**Closed**	**Feb 19: The policy has been created and approved by the Director Corporate & Strategy and pending EMT approval**. **Procedures have been updated.** Nov18: The drafted policy is awaiting review by the Governance Officer	Will be reviewed during planned Revenue Audit.
9	2017Nov	Payroll Review	**Improve leave processing process (pt 4)** Fix the rejected system leave requests to enable accurate updates.	Late 2018	N/A	Manager Financial Services	**Closed**	Jun19: This has been fixed.	Validated during Payroll Audit July 2020.
12	2017Dec	Financial Applications Control	**Improve application security management (pt 3)** Authority (Civica) password policies be implemented with access managed, monitored and reviewed to ensure only authorised individuals are granted access based on business needs.	Jun-18	Dec-18	Director Corporate & Strategy	**Closed**	**Feb19:Access to Authority is only granted to staff based on application approved by divisional and HR manager and for other individuals is approved by divisional manager. Authority Password policies are defined by Active Directory policies which enforce Complex passwords. Authorised users are only those that have an active Active Directory account along with a request for specific access from their manager. Once a user leaves the organisation, full access is removed.** Nov18: Project review and	Access is granted at the active directory domain level . If staff are removed from active directory, access privileges at the application (Authority level) are also blocked.

CLOSED AUDIT ITEMS

16	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy (pt 2.1)** Form of quotation to be included in Policy for Council approval. Suggested wording, “verbal and written quotations to include name of person and name of firm providing quotation, contact details pricing including GST, scope of works / details.	Apr-19	Manager Financial Services	**Closed**	**Jun 19: The audit action has been completed and the Council Purchasing of Goods and Services Policy has been updated to incorporate the Audit Recommendations. Futher, the Policy has been approved by the EMT and will be presented to Council for approval in June 19 OCM.**	Validated
17	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy (pt 2.2)** Consider adjusting the thresholds to enable minor purchases to require verbal quotation (i.e. up to $1k) with at least two written quotations if greater than $5k and more stringent requirements for purchases greater than $40k.	Mar-19	Director Corporate & Strategy	**Closed**	**Jun 19: The audit action has been completed and the Council Purchasing of Goods and Services Policy has been updated to incorporate the Audit Recommendations. Futher, the Policy has been approved by the EMT and will be presented to Council for approval in June 19 OCM.** Feb19:The City will take this recommendation under consideration and assess the impact upon operational efficiencies vs risk - will liaise with Audit team.	Validated
18	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy (pt 2.3)** Policy to include criteria and requirements for approval as sole source supplier.	Apr-19	Manager Financial Services	Closed	**Jun 19: The audit action has been completed and the Council Purchasing of Goods and Services Policy has been updated to incorporate the Audit Recommendations. Futher, the Policy has been approved by the EMT and will be presented to Council for approval in June 19 OCM.**	Management will develop procedure for documentation and approval of when sole source suppliers are used.

CLOSED AUDIT ITEMS

19	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy - Contract Variations (pt 3.1)** Include policy requirements around contract variations within the Purchasing Policy for Council approval.	Apr-19	Manager Financial Services	**Closed**	**Jun 19: The audit action has been completed and the Council Purchasing of Goods and Services Policy has been updated to incorporate the Audit Recommendations. Futher, the Policy has been approved by the EMT and will be presented to Council for approval in June 19 OCM.**	Validated
22	2019Jan	Accounts Payable and Purchasin	**Delegations of Authority - Award of Tender (pt 4)** Align wording re: delegations of authority to ensure consistency through all formal documentation.	Apr-19	Manager Financial Services	**Closed**	**Jun 19: The audit action has been exectued and the Council Purchasing of Goods and Services Policy has been updated to incorporate the Audit Recommendations. Futher, the Citys Purchasing Procedure Manual and the Register of Delegations will be amended once the Policy is approved.**	Validated
29	2019Jan	Accounts Payable and Purchasin	**Conflict of Interest Acknowledgement (pt 9)** Develop a separate form for panel members to sign prior to receipt of the tender documentation.	Feb-19	Manager Financial Services	Completed - pending validation	**Feb19: Completed and implemented**	Pls send form for validation.
31	2019Jan	Accounts Payable and Purchasin	**Access to ABA File (pt 11)** Restrict access to the ABA file to only those that required.	Jan-19	Manager Financial Services	**Closed**	**Feb19: Completed and implemented**	Validated during Payroll Audit July 2020.
32	2019Jan	Accounts Payable and Purchasin	**Vendor Masterfile Creation/Updates (pt 12)** New/changes to supplier details should be checked after input into Authority.	Feb-19	Manager Financial Services	**Closed**	**Feb19: Completed and implemented**	Validated Aug 2020

CLOSED AUDIT ITEMS

7	2016Nov	Control Self-Assessments -Accounts Receivable	**Excessive Number of Users with Access to Accounts Receivable Modules (pt 3)** Review current user access and allocate relevant and appropriate access for staff based on roles and responsibilities**.**	Dec-18	~~Dec-18~~ ~~Apr-19~~ Jul-19	Director Corporate & Strategy	**Closed**	**Sept19: The matter has been addressed and the City wide User access to the Accounts Receivable Module has been reviewed and updated based on roles and responsibilities.**	Will be reviewed during planned Revenue Audit.
10	2017Dec	Financial Applications Control	**Improve application governance and management (1)** Develop policies and procedures to support the management and governance of the authority application e.g. information security, data management, IT asset management, IT risk management and change management.	Jun-18	~~Aug-18~~ ~~Aug-19~~ Dec -19	Director Corporate & Strategy	Closed	Feb19: IT Policies have been reviewed and developed as required.	Further actions have been reported in the IT Policy Audit.
11	2017Dec	Financial Applications Control	**Improve application contract management (pt 2)** Authority (Civica) service level agreement is out of date and does not include any reference to confidentiality or security requirements.	Jun-18	~~Mar-19~~ Aug-19	Director Corporate & Strategy	Closed	**Sept19: The matter has been addressed with CIvia and no further action is required based on the comments provided in June 2019**	Closed Aug19 reporting; to be formally addressed following outcome of ERP decision
14	2017Dec	Financial Applications Control	**Improve application controls (pt 5)** Implement data verification and input controls to Authority system, with automated transactional calculations and reconciliation where possible.	Jun-18	~~Jun-19~~ Dec-19	Director Corporate & Strategy	Closed	**Jun 19: The Ctiy is still negotating with CIVICA and will try to address the recomendation with them.**	Closed Aug19 reporting; to be formally addressed following outcome of ERP decision
15	2019Jan	Accounts Payable and Purchasin	**Procurement Role (pt 1)** Consider changes to the roles and responsibilities of the Purchasing and Tenders Co-ordinator:	Dec-19		Director Corporate & Strategy	Closed	**Oct19: Roles & Responsibilitiies have been updated and reporting lines changed.**	Actioned Oct19
23	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy - Anti Avoidance (pt 5.1)** Develop monitoring controls re: supplier spend for potential breach of the $150k threshold at least once a year.	Feb-19	Sep-19	Manager Financial Services	Closed	**Nov19: reports have been developed.**	Sighted evidence.

CLOSED AUDIT ITEMS

24	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy - Anti Avoidance (pt 5.2)** Conduct spend analysis: • current spend by category; • to identify opportunities to achieve cost savings; • review length of existing contracts by service type to determine most appropriate duration upon renewal etc.	Jul-19	Sep-19	Manager Financial Services	Closed	**Nov19: reports have been developed.**	Sighted evidence.
25	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy - Quotations (pt 6.1)** Provide City wide training for staff re: market testing and evaluation of tenders.	May-19	Sep-19	Manager Financial Services	Closed	**Oct19: Training has been conducted.**	Training June 25/26 2019.
26	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy - Quotations (pt 6.2)** Develope procedures for the checks to be performed by officers when approving POs.	Mar-19	Sep-19	Manager Financial Services	Closed	**Oct19: Training has been conducted.**	Sighted training material.
30	2019Jan	Accounts Payable and Purchasin	**Segregation of Duties - Finance System Access Privileges (pt 10)** Conduct a full review of all staff with Authority access.	Jun-19	Sep-19	Director Corporate & Strategy	**Closed**	**Sept19: The matter has been addressed and the City wide User access to the Authority System has been reviewed and updated based on roles and responsibilities.**	Full review has been ocnducted. New issue raised regarding review of Payroll access by HR staff.
33	2019Jan	Accounts Payable and Purchasin	**Technical Check - Supplier Invoices (pt 13)** Formal handovers should be conducted for new contract owners.	Apr-19	Sep-19	Director Corporate & Strategy	Closed	**Oct19: Handovers by departing employees are not part of the Exit checklist.**	Sighted new checklist.
28	2019Jan	Accounts Payable and Purchasin	**Tender Process - Assessment for Financial Capability (pt 8)** Develop and implement risk-based matrix to evaluate the potential supplier for financial capability.	Jun-19	Sep-19	Manager Financial Services	Closed	**Oct19: Risk matrix being used to determine extent of due diligence for evaluation of financial capability of suppliers.**	Sighted improved process for evaluation of suppliers for supplier strength.
20	2019Jan	Accounts Payable and Purchasin	**Purchasing Policy - Contract Variations (pt 3.2)** Provide staff training to 'contract owners' to ensure they are aware of the requirements around contract variations.	Apr-19	Oct-19	Manager Financial Services	Closed	**Oct19: Training has been conducted.**	Sighted email to staff.

8.2 Review Report against the Officer of Auditor General's Report on Local Government Information Technology

Committee	9 November 2020
Applicant	City of Nedlands
Employee Disclosure under *section 5.70 Local Government Act 1995*	Nil.
Director	Lorraine Driscoll – Director Corporate & Strategyt
Attachments	1. Area of Focus based on OAG Report – 25 June 2020
Confidential Attachments	Nil.

Executive Summary

The objective of this report is to provide the Risk and Audit Committee with background information on the OAG's (Office of Auditor General) report on Local Government IT. The Business Systems business unit has reviewed the City's IT processes and practices, using the OAG report as a guideline.

We have assessed the City's IT maturity level to be around the "Defined (3)" and moving towards "Managed and Measurable (4)". This was an exercise in preparation and discovery. It is important to be prepared for future audits, be they internal, external or by the OAG. By understanding how the City is positioned against the OAG findings, we will be in a better position to improve and provide the safety and security of the City's business systems.

Recommendation to Committee

The Audit and Risk Committee;

1. **Reviews the report on the City's position in respect to the criteria defined in the Office of Auditor General's report dated 25 June 2020; and**

2. **Endorses the work undertaken by Administration and outlined in this report.**

Discussion/Overview

This report identifies the practices required in the 14 areas that the OAG reviewed across 10 local government entities. The OAG found significant gaps in meeting the good practice standard across several control areas. Only 4 of the local governments demonstrated that they were effective, or partially effective, in at least 7 of the 14 areas.

The OAG's conclusion was that local governments should understand and assess their risks unique to their business activities and environment that would inform their strategy and to assess their controls against good business practice standards.

Using both International Organisation for Standardisation (ISO) standards and Information Technology Infrastructure Library (ITIL), Administration has carried out an assessment and believes the City is in a good position. Some minor gaps have been identified, which will be address in on-going work to continually improve the City's processes.

Strategic Implications

How well does it fit with our strategic direction?

The processes and practices highlighted will better enable Business Systems in the delivery of Information Communication Technology Services. As well as meeting our compliance and demonstrating our governance practices.

Who benefits?

The City of Nedlands Administration and Council will benefit from a better awareness within the organisation. The Business Systems business unit will be better able to carry out its role in the supply and support of ICT Services.

Does it involve a tolerable risk?

This review of the City's processes against the report by the OAG helps to reduce risk by ensuring the City's process meet the standards outlined in the report.

Do we have the information we need?

Yes, the report informed us of areas to be aware of and of what has been discovered by the OAG in their work with other Local Governments.

Budget/Financial Implications

Can we afford it?

There are no costs associated with this report.

Item 8.2 - Attachment 1

City of Nedlands

Review based on WA Officer of the Auditor General’s findings reported about Local Government Entities

Table of Contents

Executive Summary

On the 25th June 2020, the Western Australian Office of the Auditor General (OAG) released the first local government Information Systems Audit report since the proclamation of the Local Government Amendment (Auditing) Act 2017. The report summarises the results of the 2019 cycle of information systems audit at 10 local government entities.

These audits our a fundamental part of the financial audits. They help to assure that the financial information generated by information systems is accurate, reliable, and recorded. While local governments will differ in the size and scale, they should have effective controls to manage information systems.

The report was given in 2 parts:

1. Information systems – security gap analysis, and
2. General computer controls and capability assessment of local government entities

The result of the security gap analysis was benchmarked against a globally recognised standard. The standard provides a set of controls which entities can easily implement to protect critical information from internal and external threats. These standards usefully guide how the City of Nedlands can address these potential weaknesses.

It was identified that Local government entities' information systems are integral for delivering key public services. However, most entities do not have a holistic view of activities that pose risks to their information systems. Entities should have visibility over their systems and take a strategic approach to address these risks.

There are both international and local frameworks which will enable these practices. Department of Local Government Sports and Cultural Industries (DLGSC) has produced a WA ICT Strategic Framework as a guide. Using that framework and the practices around The Open Group Architecture Framework (TOGAF) we have created our own.

The City of Nedlands was not one of these councils, but as a precaution and good practice this report is the results from carrying out our own audit against the same parameters. Using the AOG's report we made a check list to review and confirm our position against these standards.

In carrying out this review we have seen no evidence to indicate that we are exposed in any perspective. This has been an old scout exercise of being prepared.

Information Security Policies

Introduction

The objective of this report is to carry out a gap analysis between what the OAG has been looking at and where the City of Nedlands is positioned. The goal is to assess our information security controls to see if we meet the requirements of International Security Standard 28002 (AS ISO/IEC 27002:2015). This standard provides the framework and controls to ensure IT environments preserved the confidentiality, integrity, and availability of information. Most of these controls are globally recognised as good practices and require minimal effort to implement.

Background

The City of Nedlands hold information, including confidential information about people and the community, which is fundamental to our operations and should be protected from external and internal threats. As our IT systems and computing environment become~~s~~ more interconnected, the amount of information grows, along with the number and diversity of threats. Effective information security involves managing people, processes, and technology to preserver the confidentiality, integrity, and availability of information.

At the City of Nedlands, we are using the information security standards to develop sound practices around our controls. These standards have 14 areas with each area containing various controls that can be tailored to our needs and complexity.

	Information security aspects of business continuity management		Operations Security
	Physical and environmental security		Information Security Incident Management
	Human resources security		Compliance
	Information security policies		Organisation of information security
	Access control		Supplier relationships
	System acquisition, development and maintenance		Asset management
	Communications Security		Cryptography

Figure 1 - 14 Areas of Assessment

This report is to validate our overall rating for each area:

- Determined which controls were applicable,
- Assessed and gave individual controls a score,
- Consolidated those scores to calculate our overall result which considered the number of effective controls, and
- Scores over 80 percent indicate that we have effective controls, 61-80 percent indicate partially effective and below 61 percent as ineffective.

What the AOG found

The AOG found significant gaps in meeting the good practice standard across several control areas. Only 4 of the councils demonstrated that they were effective, or partially effective in at least 7 of the 14 areas.

Each council has its unique security requirements based on their business needs. However, most councils have not assessed and identified their security requirements. Generally, security requirements can be identified through:

- Assessing risk, considering the overall business strategy and objectives including vulnerabilities and threats to assets,
- Understanding legal, statutory, and contractual requirements that apply to the entity and its contractors and service providers, and
- Understanding the set of principles, objectives, and business requirements for information handling to support operations.

The AOG found issues around:

- Security policies did not provide direction and support for information security,
- Poor controls risked network and operations security,
- Most entities had business continuity strategies, but few had tested them,
- Poor access management controls resulted in inappropriate access
- Entities risked not effectively responding to security incidents,
- Information was at risk du~~r~~e to inadequate supplier management controls
- Physical and environmental security could be improved
- Information security controls were not considered over the lifecycle of information systems, and
- Inadequate human resource security controls could threaten information security.

AOG Recommendations

Local governments should:

1. Understand and assess the risk unique to their business activities and environment to inform their strategy for information security management,
2. Assess their controls against good business practice standards to identify gaps and develop plans to improve information security. Entities can seek further guidance from other good practice standards. i.e.:
    a. The Australian Cyber Security Centre maintains the Australian Government Information Security Manual to assist entities in protecting their information and systems.
    b. The National Institute of Standards and Technology publishes NIST Cybersecurity Framework to help organisations improve the management of cybersecurity risks.
    c. Implement processes to continuously monitor and improve information security controls to ensure that they meet entity needs.

Under section 7.12A of the Local Government Act 1995, the 10 audited entities must prepare an action plan addressing significant matters relevant to their council for submission to the Minister for Local Government within 3 months of the report being tabled in parliament and for publication on the council's website. This action plan should address the points above if they relate to their council.

This last action I believe would be a major security breach as it would be telegraphing security issues that are open and how they are being addressed.

Conclusion

Based on the report by the AOG, Business Systems has carried out its own audit around the identified criteria. What has been found is that we are in good shape and moving to a better position regarding any future IT Audit.

In the areas identified we are in a good position of maturity based on the rating scale and criteria of 0-5. Working across the six defined areas of:

1. Information Security,
2. Business Continuity,
3. Management of IT Risk,
4. IT Operations,
5. Change Control, and
6. Physical Security

We have assessed our positing to be around the “Defined (3)” and moving towards “Managed and Measurable (4)”. This was an exercise in preparation and discovery. Preparing for any future audit be it internal, external or the OAG. In defining our position, we are in a better position to improve and provide the safety and security expected of Business Systems within the City of Nedlands.

Introduction

Capability Maturity Models (CMMs) are a way to assess how well-developed and capable our City's IT controls are. The model provides a benchmark for organisations performance and a means for comparing results from year to year, and across organisations.

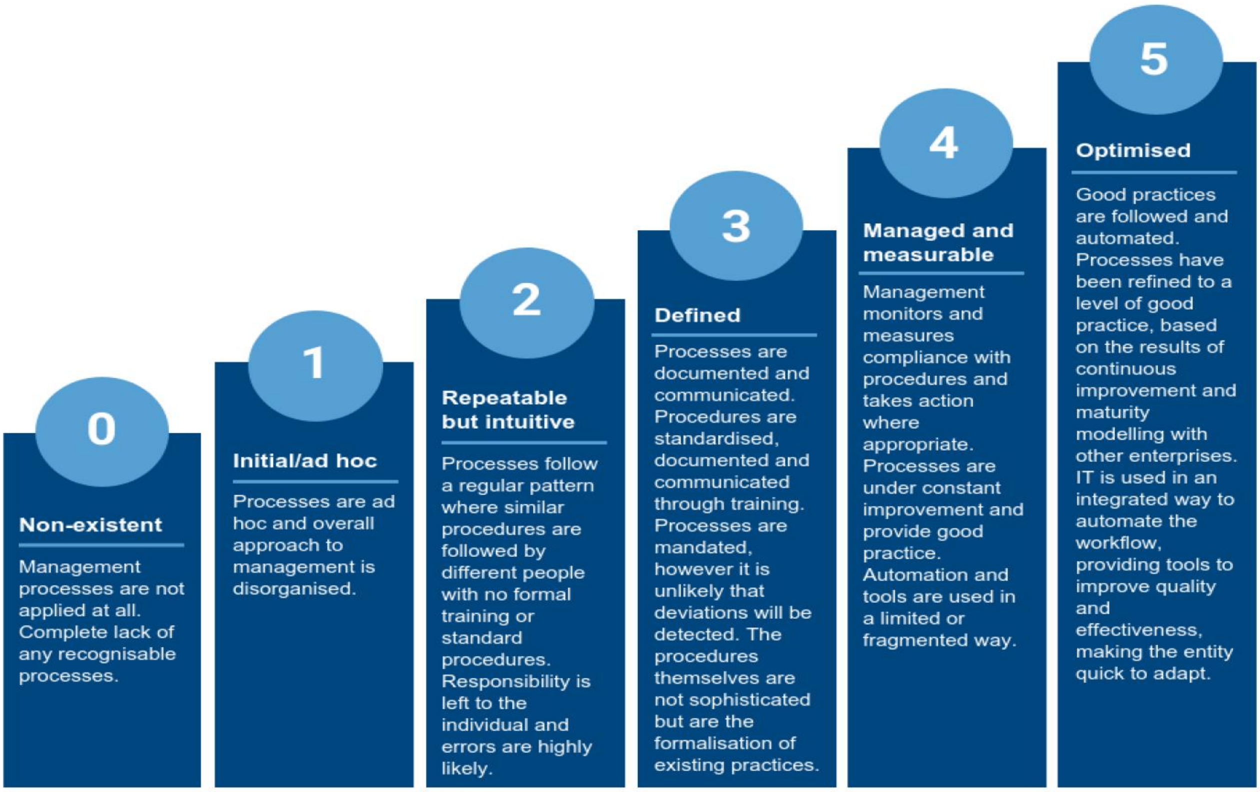
The model the AOG has developed uses accepted industry good practice as the basis for assessment. That assessment of General Computer Controls (GCCs) maturity is influenced by various factors including:

- Business objectives of the City
- Level of dependence on IT
- Technological sophistication of computer systems, and
- Value of information managed by the City.

They focused on Six categories to determine the maturity of the councils control environments:

	Description	Score		Description	Score
	Information Security	3 going 4		IT Operations	3 going 4
	Business Continutiy	4		Change Control	2 goiong 3
	Management of IT Risk	3 going 4		Physical Security	3 going 4

Table 1 - Six categories in Determining IT Maturity



0 Non-existent
Management processes are not applied at all. Complete lack of any recognisable processes.

1 Initial/ad hoc
Processes are ad hoc and overall approach to management is disorganised.

2 Repeatable but intuitive
Processes follow a regular pattern where similar procedures are followed by different people with no formal training or standard procedures. Responsibility is left to the individual and errors are highly likely.

3 Defined
Processes are documented and communicated. Procedures are standardised, documented and communicated through training. Processes are mandated, however it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed and measurable
Management monitors and measures compliance with procedures and takes action where appropriate. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised
Good practices are followed and automated. Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the entity quick to adapt.

Figure 2 - Rating scale and criteria for the CMM

Policies & Procedures

These are some of the questions and area we should be addressing.

- What are our policies outlining our approach for managing information security objectives?
- Do they contain guidance for key areas?

They should include:

- roles and responsibilities for information security management
- access management
- protection from malware or malicious code
- use of IT assets and technical vulnerability management.

We need to take a strategic approach to information security by understanding the risks and implementing policies to govern security.

- What is our policy or a management approach on cryptography controls?

A lack of direction for our cryptography controls increases the risk that the confidentiality and integrity of information held by the City of Nedlands and we could be compromised.

- Do we have a good process to check compliance with security requirements?

For example, performing periodic internal reviews to ensure controls are working as expected. Without processes to detect policy breaches and non-compliance, we cannot determine if these controls are operating effectively.

City of Nedlands review against the OAG Report

Based upon the OAG's report, these were the areas we reviewed and either validated or identified as an issue to be addressed to meet good practices around the ISO standards. Our responses to each question are highlighted in Green.

Information Security Policies

- What are our policies outlining our approach for managing information security objectives?
- Do they contain guidance for key areas?
  - These include:
    - roles and responsibilities for information security management. ***Yes***
    - access management. ***Yes***

New User and User Deactivation details are communicated via Jira helpdesk to manage user accessing systems/network, AD groups and permissions, new user permission details are captured for the Finance system (Authority) user roles & responsibilities permissions.

- protection from malware or malicious code
  - *We do not have a policy for malware protection. Cyber Security Policy/Procedure needs to be created. This is being addressed in our Cyber-Security Assessment currently being undertaken by Rajan Sharma*
- Use of IT assets
  - *IT Asset Policy/procedure needs to be this is being created by Nalin Dias as part of his work.*
- technical vulnerability management
  - *This is being addressed in our Cyber-Security Assessment currently being undertaken by Rajan Sharma*

We need to take a strategic approach to information security by understanding the risks and implementing appropriate policies for the governance of security.

City's Acceptable Use of Electronic Equipment, Security and Media Policy covers:

- *offensive material via internet (search, access, social media); information security obligation,*
- *information intellectual property obligation,*
- *right to monitor and audit,*
- *acceptable use of information systems (systems/network/email/telephone/internet),*
- *appropriate use of Internet/social media, email,*
- *user accounts and passwords,*
- *software and licensing,*
- *remote access and working from offsites,*
- *unauthorised hardware and software install and use,*
- *incident reporting – monitoring and reporting breaches and inappropriate use of internet and email,*
- *information assets/resources (databases/servers/communication equipment).*

This is a current piece of work being undertaken by Nalin Dias.

This policy will require an acknowledgement and acceptance sign for each employee.

- What is our policy or a management approach on the use of cryptography controls?
  - *No cryptography controls are in place except SSL certification for web information trust. Cyber Security Policy/Procedure needs to be created. This requires further investigation and development.*

Any lack of direction for our cryptography controls increases the risk that the confidentiality and integrity of information held by the City of Nedlands and we could be compromised.

- Do we have a good process to check compliance with security requirements?
  - *Not at this stage but is being incorporated with our work with the cyber-security assessment being carried out by Rajan Sharma and will add to our Cyber Security Policy/Procedure.*

We have multiple systems that scan for security and compliance, the security requirements need to be better defined within a policy.

For example, performing periodic internal reviews to ensure controls are working as expected. Without processes to detect policy breaches and non-compliance, we cannot determine if these controls are operating effectively.

Network and Operational Security

- What are our practices to manage operational security?
  - *Regular network security control checks – firewall reports, virus scanning, email scanning, network port scanning using Nessus network monitoring and reporting tool.*
  - *Operational practices are Daily/Monthly Scans along with keeping all systems up to date. From a compliance point of view, we log most event log data into Azure Monitor along with all Office 365 events. Firewalls are handled by Fortianalyzer.*

Without good practices, we are at greater risk that internal and external threats will compromise our systems.

What are our controls over network and operations security?

They should include:

- Do we have adequate change management processes?
  - *Currently being adopted and implemented in Jira helpdesk, this is following ITIL service management practices*
- Do we have enough coverage in our network security appliances?
  - ***Yes***
- How long do we retain our firewall events?
  - What sort of account are we using to administer the firewalls?
    - *We retain our firewall events for 1.5 years in total as well as local account administers firewall logs*
  - What are our processes to assess and remediate security weaknesses?

            - *We have the following in place - Annual security audit reviews run by internal IT staff*
        - What controls do we have to observe and review network activities?
            - *We have - Nessus network vulnerability scanner. These include*
                - *Fortianalyzer for all web traffic from any gateway*
                - *Aruba Wi-Fi Logging*
                - *FortiGate Firewalls for each site*
                - *Microsoft Defender ATP desktops (Azure Security Centre)*
        - What is our data backup plans?
            - *VMWare has an automated backup testing feature in place. Data is automatically tested for integrity using Veeam surebackup.*
            - *Backup and Replicated data are application aware indexed whole virtual machine data. Business Backups Continuity Policy will cover the backup process etc. Data is automatically tested for integrity using Veeam surebackup*
            - *Backup and Replicated data are application aware indexed whole virtual machine data.*
- And do they reflect current IT infrastructure. ***Yes***
- When was the last time we tested the integrity of data on backups?
    - *Once every month. SureBackup does this automatically but we test once a month.*
- Do we have adequate segregation of networks? *Yes, via VLANs*
    - *External facing servers are in a DMZ zone where only key ports are allowed.*
    - *All traffic to the internet is inspected including SSL traffic except for defined exceptions*
    - *External facing servers are in a DMZ zone where only key ports are allowed.*
    - *All traffic to the internet is inspected including SSL traffic except for defined exceptions*
    - *Only ports 80 and 443 are allowed – all others are blocked unless exceptions are needed i.e. Civica FTP access.*
    - Do we have anti-malware controls installed on our key servers? ***Yes***

Business Continuity Strategies and IT Service Continuity

There needs to be a clear distinction between Business Continuity and Information Service Continuity. Once clearly identified we need to establish both our **IT Service Continuity (ITSC)** plan and the **IT Disaster Recovery (ITDR)** plan that is in support of the **Business Continuity Plan (BCP)**.

*Both plans need to be clearly established and tested on a regular basis. I am recommending six months overlap with each plan being on an annual basis. The development of the ITDR plan depends solely on the **Business Impact Statements (BIA)** that define critical needs and time frames that the Business Services team need to meet.*

A great demonstration of our ability within a disaster was during the time we had to work from home. Within a matter of two days we were operational from home with all staff. This was due to our early adoption of the cloud, Office365 and Microsoft Teams.

Access Management Controls

- What are the processes to manage access to systems and networks?
  - *New user, user deactivation and permission granting are communicated via Jira helpdesk to manage user accessing systems/network and any permission authorisation. Also, AD groups and permissions are in place manage security. New user permission (roles & responsibilities) is communicated to setup the Finance system (Authority) for all users via Jira helpdesk.*

Some of the weaknesses may include:

- Former staff still having access to systems.
- Do we have a practice of review of accounts? *Yes*
- What are they and when do they get carried out?
  - *Active Directory is cleaned up regularly as per user termination information via Jira helpdesk, and as per HR and BU Manager email communication to IT. Authority users cannot be deleted due to the attached transactions.*
- Is there a record of these events?
  - ***Yes** – in SharePoint & Jira*
- What is the process to request and authorise access to our systems?
  - *via Jira helpdesk*
- What are the password and authentication controls?
  - *This is managed via Jira helpdesk, in Active Directory (AD) and Windows, Authority user setup interface. I would Say 99% is Single Sign On (SSO) via AD for end users*
- What are the processes to review user access and privileges?
  - *We use AD report, Authority report. We really do not have a great way of reporting other than PowerShell. Sharegate does to permission reporting but Jon did not have the report to review yet. This will be a part of cyber security policy/procedure and DRP*

Security Incidents

Are there appropriate plans to manage information security incidents?

- *No there is no incident response policy or procedure. Currently these are managed via SharePoint – IT enquiries & complaints/internal comms & memos, and Jira helpdesk, this will be part of cyber security policy and procedure.*

What are our response plans to address these incidences?

- *This will form part of Cyber Security Policy/Procedure and part of DRP*

What are the programs and procedures for detecting security incidents?

- *Firewall reports, SharePoint reports, Authority access reports. Internal scanning through Nessus Vulnerability Scanner and internal remediation. Fortianalyzer for all web traffic from any gateway, Symantec Endpoint protection for Servers, Microsoft Defender ATP desktops (Azure Security Centre) & Microsoft Advanced Threat Protection*

What is our policy and procedures to handle forensic evidence to effectively manage security incidents?

- *We do not have a policy regarding Forensic evidence directly. In such a case is the retention of logs over a period. We do this, but do not have a policy. Need to have a policy for security breach protection. This should come under Cyber Security Policy/Procedure. How IT treats digital forensic evidence such as server and firewall and AD logs/file logs etc. This is an area of future development.*
- *We have a policy/procedure around* ***e-Discovery*** *which is a* ***Forensic discovery tool,*** *this is controlled and strictly managed and documented when used as per our defined policy.*

Supplier Management Controls

What documentation do we have around information security risks associated with the use of suppliers or contractors? I

- *Currently we do not have NDA's (Non-Disclosure Agreement)   for 3rd Party contractors. This is an area worth exploring further to see if there is a need.*

We need to understand our vendors and their security posture, services, and systems is vital in maintaining effective information security controls. Without these controls there is an increased risk that entity information is exposed to unauthorised access and disclosure.

Physical and Environmental Security

What are the controls around our physical and environmental area?

These should include:

- *We have formally defined the roles and responsibilities for managing the server room, physical access controls.*

- *NextDC is Gated, secure complex. Depot is Swipe card access only for approved users(logged) and Admin building has rubbish in front of the rack (but no sensitive equipment)*

For example, fire suppression systems are they installed in our technology rooms?

- *No to Depot/Admin buildings,*

What has access to the server rooms, and is that access monitored?

- *Staff card access logs to server room at the Depot. NextDC has camera and visiting request system. Outstation CCTV cameras are in place for site visit recording.*

Information Security Controls Over the Lifecycle of Information Systems

What are the practices for managing our information and IT assets over the lifecycle of information systems?

- *Information Management handle information, IT assets are captured and depreciated and eventually disposed but no policy is available.*

What plans and procedures do we have to manage the acquisition, maintenance, disposal and re-use of IT and information assets?

- *There is no IT Asset Policy/Procedure exists. IT HW/SW acquisition form/maintenance, Project charter, and not in our approved policies/procedures. Jira does not track assets. AssetFinda does track assets but I.T. equipment is not included. Change management is part of this process.*
- *Business case document. Disposal/re-use - IT Asset Disposal Policy, Jira helpdesk system setup to track/manage IT assets or AssetFinda to capture/manage IT assets*

Have we a clear understanding of all our assets that process information?

- *Not really. Authority system asset reporting only captures assets above $5000 for depreciation purpose by Finance team. Jira helpdesk system setup to track/manage IT assets or AssetFinda to capture/manage IT assets. IT Assets Policy/Procedure and an Asset Map/Register is required.*

Are there appropriately protected and the information on the assets cannot be inappropriately accessed, even after disposal.

- *MFD contract has a clause to securely disposing city machines and wipe hard drives after decommissioning. Hardware disposal policy has a similar clause. IT Asset Policy/Procedure to have disposal criteria.*

What are the policies and processes for classify information based on its value, legal requirements, criticality, and sensitivity?

- *No policy or process is in place atm. Information Management Policy to be created to classify information based on the above criteria. Agree, need to classify documents based on document value – top secret, general etc*

Human Resource Security Controls

Do we have the necessary policies and process to manage information security risks when staff are hired or terminated?

- *There is no policy or procedure though, that says HR and Manager/Director will approve access. There needs to be a policy behind this. Agree, new Information Security Policy/procedure needs to be created to highlight user activation/deactivation.*
- *Jira helpdesk user creation/termination process is in place,*

Weaknesses we need to check for could include:

- Requirements for background checks before employing staff and contractors, -
  - *For staff this occurs. Not for Contractors. For contractors we need to create NDA and a background check Policy/Procedure*

- Confidentiality and non-disclosure agreements not required for new staff,
  - *I believe this was in the works or is live for staff. Not done for contractors. Same as above – NDA (non-disclosure agreement) is required*

- Induction and ongoing programs to inform staff and contractors of their information security responsibilities.
  - *For staff this is done. Not for contractors. There is no Contractor Register that we utilise with a yearly audit or repeat of induction. A Contractor Register with a policy/procedure is required*
  - *Staff need to understand their responsibilities for information security. Security of information needs to be managed properly when staff leave our organisation.*
  - *More work needs to be done. Need to do more Phishing tests and more staff education. Information Security Policy/Procedure needs to be created. Staff and contractor NDA.*

Management of IT risks

What are the policies and procedures for managing IT risks?

- *Procurement and risk - Project charter and Busines case document. Tender & quote process, Annual IT audit – internal/external,*

Some common weakness to look for included:

- A lack of risk management policies,
  - ***Yes**, we have an Integrated Risk Management Framework, policies, and procedures as well as a comprehensive Risk Register. This has been developed around the Information Security Manual 2020 principles and currently being updated to 2020 version.*
- In adequate processes to review and report risks to senior management,
  - *Jira helpdesk to be aligned/modelled against ITIL standard to highlight risks. IT Risk Register / Policy/Procedure needs to be created.*
- No risk registers for ongoing monitoring.
  - *IT Risk register/treatment plan for IT needs to be created. A Risk register has now been created with a policy and Integrated Risk Management Framework. This has been completed for Business systems and will now be rolled out to the City. Business Systems will work with each area in assisting and managing the risk register with each of the risk owners in each area. This will be a regular rolling bi-monthly exercise across the city.*

We need to be able to identify, assess, and treat risks affecting key business objectives. We should be aware of the nature of risks associated with IT and have appropriate risk management policies and practices with good risk assessments, registers, and treatment plans. We need to be able to identify and treated incidents within reasonable timeframes to meet our business objectives.

IT operations

- What are the requirements for our IT service levels?
    - *Business Systems and Applications - ICT Service Level Agreement (SLA) Policy needs to be reviewed as it does not match ITIL framework and has silly timeframes with no PROBLEM (everything is an incident)*
- Have we allocated sufficient resources to meet these requirements?
    - *Jira helpdesk to align/model against ITL standards to understand resource requirements. Depends on projects and staff capability. Also, the current SLA does not have the coverage to meet our requirements. Need a review of the current IT SLA Policy – Request -> incident -> Problem -> Change (each criterion above should have its own SLA).*
    - *This is currently underway and will be adopted once built. Next Business Systems will run a workshop around the ITIL Service Management practices.*

IT operations include day-to-day tasks designed to keep services running, while maintaining data integrity and the resiliency of IT infrastructure.

Do we have any formalised procedures and monitoring controls to ensure processes are working as intended?

- *Monitoring controls - Jira helpdesk to be aligned/modelled against ITIL standards to generate reports against processors. Also Depends on what the process is. Are we also talking about monitoring System stability/uptime? IT Operations dashboard is not in place to monitor all system. Investigate systems for centralised view of all systems where possible*

Weakness we may find could include:

- inadequate processes to review and report risks to senior management,
    - *IT Risk Register/Policy/Procedure needs to be created*
- An asset registers to track and monitor IT equipment,
    - *Currently we have SharePoint hardware management/annual license & renewals, AssetFinda, Authority/SharePoint or Jira helpdesk to be aligned/modelled against ITIL standards to capture and report IT assets. These are not up to standard and needs to be reviewed or created - IT Asset Register/Policy/Procedure.*
- Adequate processes to ensure compliance with software licensing agreements,
    - *Current processors - SharePoint annual license & renewals/software management, Jira helpdesk to be aligned/modelled against ITIL standards to capture and report software assets. These are not up to standard and needs to be reviewed or created. There is no Contractor SLA Register is in place. IT Vendor SLA Policy/Procedure needs to be created*
- Do we have adequate service level agreements with our vendors?
    - *some vendor contract details with SLAs are in the SharePoint under contractor & vendor register. Jira helpdesk can be aligned/modelled against ITIL standards to*

capture and report vendor SLAs. None are documented in a register. A Contractor SLA Register needs created. IT Vendor SLA Policy/Procedure needs to be created

- What are the contract management practices that gives us the oversight of our vendors?
  - *SharePoint some vendor contract details with SLAs are in the SharePoint under contractor & vendor register. Also, in annual license & renewal register, Jira helpdesk can be aligned/modelled against ITIL standards to capture and report vendor SLAs. Need to create - Contractor/Vendor SLA Register, IT Vendor SLA Policy/Procedure*
- Are the retention and management of event logs adequate for our needs?
  - *We do retain many logs on premise and in Azure – but it is not a defined policy to determine for how long or what is kept. Information Security Policy/Procedure needs to be created. This will be in the Information Security Policy/Procedure that needs to be created.*
- Are adequate reviews of access to see that there are no inappropriate accesses being made.
  - *Tools in place for reporting - AD, Authority, SharePoint & Firewall reporting*

Change control

What are the controls around processes to implement changes in their IT systems and infrastructure?

- *Emails and Jira helpdesk service calls*

Is there a record of these changes, authorisation, and testing?

- *Developed a Change Control Form under IT controlled documents and it is yet to get approved.*

Weaknesses that could potentially create an issue included:

- Are adequate reviews of access to see that there are no inappropriate accesses being made.
  - *Current - Firewall report, Code of conduct, system log files, AD and Authority access permission reports. Weekly review of Firewall Reports – Azure AD has reports unusual activity. This will be a part of Information Security Policy/Procedure.*

There is a lack of a formal system of change management. This increases the risk that changes, including those that may be harmful to systems and information, could be implemented without assessment.

- *Agree*

There are currently no records of changes made to critical systems. This would make it difficult to investigate incidents that may have been caused by changes. Current - Firewall reports, system log files, AD and Authority access permission reports. I think this is more regarding not having a change request system will not then show why something occurred. Logs will show information, but not why they change occurred.

- *Need a Change Control Policy/Procedure – there is a policy in place but needs reviewing.*

What formal policies and procedures do we have to ensure changes, risk assessed, tested, sufficiently documented, and authorised prior to being implemented.

- *We have an Integrated Risk management Framework as well as policies, procedures and register.*

Physical Security

What are the controls to protect their IT systems and infrastructure against environmental hazards and unauthorised access to server rooms?

- *CCTV and staff access card register & reports,*

Do we regularly monitor our assets for improper access?

- *NextDC has logs on all entry events. Depot has logs on all room entry events. This is a part of Information Security Policy/Procedure*

Do we log all access to IT secured areas?

- *100% of the time - admin building does not have anything special other than switches. So other rooms are logged. NextDC and Depot – Yes 100%. Everywhere else is 0%*

Appendix 1 – Technical Vulnerabilities

Vulnerabilities are flaws in operating systems, devices, and applications that attackers could exploit to gain unauthorised access to systems and information. Local government entities should have continuous monitoring processes to understand security weaknesses and gaps in their systems, devices, and applications. Vendors generally provide patches to address flaws in applications and systems. Entities should implement processes and assign responsibilities to identify and treat these flaws.

The following table outlines guiding principles entities should address vulnerabilities. This is not intended to be an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre.

Principle	Our expectation
Stocktake of assets	Entities should have visibility of all their ICT assets on the network including servers, workstations, printers, software applications, IoT and other network devices (switches, routers, firewalls).
Our Response	
Identify vulnerabilities	Regular vulnerability scans must be performed to identify security weaknesses. Where it is impossible to scan all assets at once, entities should prioritise and group assets to scan them in stages. Scans should be regular (e.g. continuous or monthly) as extended time gaps between scans leave the systems exposed for longer periods.
Our Response	
Understand the exposure	Each vulnerability poses a threat but some are more severe than others. Vulnerabilities generally have a severity rating based on impact and how easily they can be exploited. Entities should perform risk assessments to understand the exposure and act.
Our Response	
Test and patch vulnerabilities	Entities should test patches before deploying them to live production systems. Ideally vulnerabilities should be patched ASAP, in line with their severity and impact levels. Entities should define appropriate timeframes to patch vulnerabilities based on their severity.
Our Response	
Apply mitigating controls if patching is not possible	Sometimes, vulnerabilities cannot be addressed as they could affect the operations of a system (usually legacy systems), or a patch may not yet be available. Based on a risk assessment, mitigating controls should be applied with considerations to: • virtual patches • segregating or isolating unpatched systems • upgrading systems that no longer receive security updates.
Our Response	
Don't forget the network devices – and printers	Network devices such as firewalls, routers and switches - and printers - are equally important. Vulnerability management processes must include them. Entities should regularly update the firmware and software for these devices.
Our Response	
Verify the patches	Entities should establish a process to verify that patches have successfully fixed the vulnerabilities. Some patches may fail to install or could require further configuration to address the weakness. Running another scan after applying patches can identify and report such instances.

Our Response	

8.3 Moore Australia – Payroll Internal Audit Report

Committee	9 November 2020
Applicant	City of Nedlands
Employee Disclosure under *section 5.70 Local Government Act 1995*	Nil.
Director	Lorraine Driscoll – Director Corporate & Strategy
Attachments	1. Moore Australia – Agenda Paper; 2. City of Nedlands Payroll Audit (FINAL) (16 October 2020); and 3. City of Nedlands Potential Internal Audit Topics.
Confidential Attachments	Nil.

Executive Summary

The objective of this report is to deliver the Risk and Audit Committee with background information on the Moore Australia (Internal Auditor's) Payroll Report and a copy of the final report for endorsement.

Recommendation to Committee

The Audit & Risk Committee:

1. **reviews the Final Payroll Internal Audit;**

2. **endorses the Report; and**

3. **receives the Potential Internal Audit Topics report.**

Discussion/Overview

This report identified five key observations and recommendations (three High and two Medium). The procedural recommendations have now been adopted, of the two technical one has been adopted. The other is being address with the work on obtaining a new business platform and an RFT for a payroll service.

In relation to the Detailed Observations and Recommendations, management has agreed will all recommendations. The actions where possible have been taken now or will be taken in the coming months. Many of the other issues should be covered and reviewed once the new platform is in place.

Strategic Implications

How well does it fit with our strategic direction?

The processes and practices highlighted will better inform implementation of the new platform. This will bring us more in line with current technology offerings and provide better performance and automation.

Who benefits?

The City will benefit from an understanding that our current practices are well founded, the areas identified have been addressed or will be addressed further once the new platform is in place.

Finance and Business Systems business units have benefitted from this report. It has made staff aware of issues that needed to be addressed. This will better prepare us for implementing a new solution.

Does it involve a tolerable risk?

This report reduces financial risk by highlighting areas that can be improved or easily rectified.

Do we have the information we need?

Yes, the report informed us to act upon, and where needed clarify and correctly move forward with how we manage payroll.

Budget/Financial Implications

Can we afford it?

There is an approved budget to obtain this service to prepare for our external audit.

MOORE

Audit and Risk Committee Agenda Paper

Subject	Internal Audit
Prepared	2 November 2020
Attendance	Director Assurance Advisory - Michelle Shafizadeh Associate Director - Duy Vo

1. Purpose

To provide an update on the status of the internal audit to the Audit and Risk Committee.

2. Status Update

Payroll Report

The Final Internal Audit Report Payroll Report was provided to Management on 16 October 2020. A copy is provided as Appendix 1.

Strategic Internal Audit Plan

A draft Strategic Internal Audit Plan is being prepared for the years ending 30 June 2021 to 2023. The audit topic of revenue has been agreed with Management. Moore Australia are currently liaising with Management to determine additional proposed audit topics.

A list of potential audit topics was provided to Management on 28 October 2020 for their consideration. A copy of the list is provided in Appendix 2.

Internal Audit Recommendations

A selection of internal audit recommendations has been validated since the last Audit and Risk Committee meeting held on 5 October 2020.

The status of internal audit recommendations on 2 November 2020 is set out below:

Status	Number	Percentage
Not implemented by Management	**5**	**45%**
Completed by Management but not verified by internal audit	**0**	**0**
Verified by internal audit and recommended to the Audit and Risk Committee to be removed from the Internal Audit Log.	**6**	**55%**
Total number of recommendations on 2 November 2020	**11**	**100%**

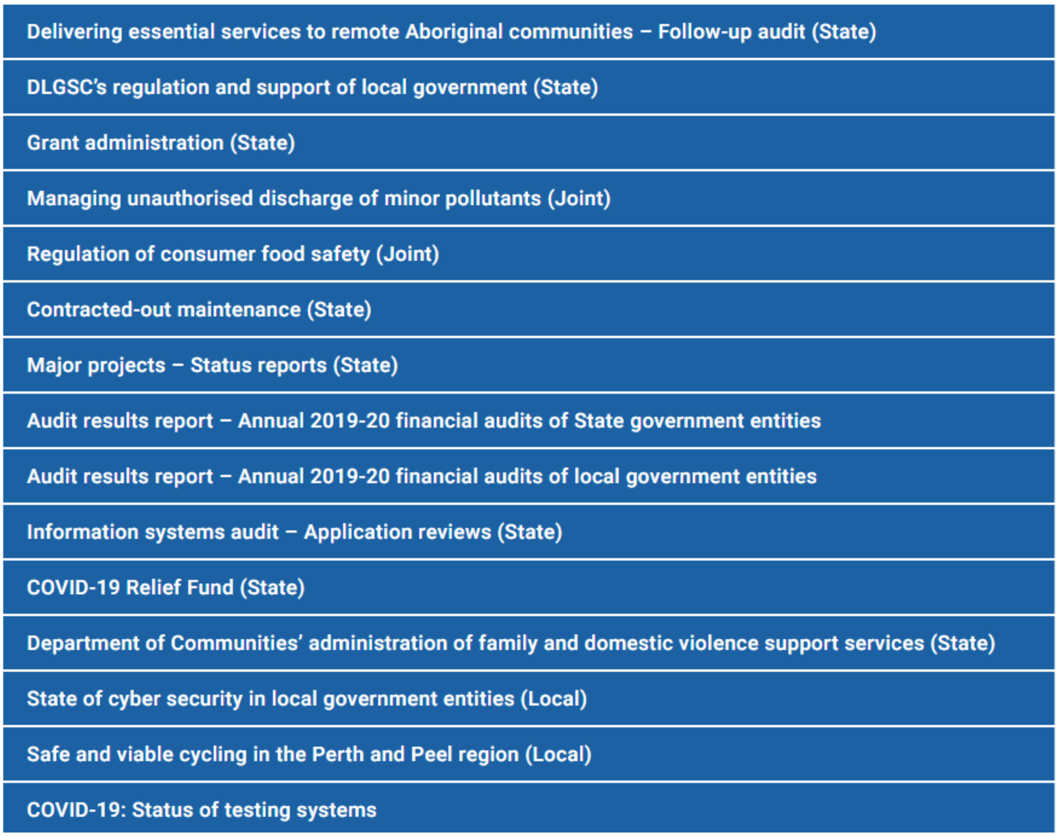
3. Office of the Auditor General

A role of internal audit is to help Management to identify where risks are and to identify the controls and treatment actions which are in place to mitigate those risks, or to report the lack of these controls and treatment actions.

A risk for all Local Governments is the risk the Auditor General will perform performance audit and report the findings to Parliament which depending on the results, may identify significant un-identified risks and affect the credibility of the Local Government with Parliament, the community and other stakeholders. Moore Australia like to assist our clients to be “audit ready” to reduce their credibility risk.

Set out below is an extract from the Office of the Auditor General website on 28 October 2020 which identifies the current performance audits in progress and future performance audit program. Currently there are no future performance audits identified. These topics can be used to identify where there may be gaps within your Local Government and where work needs to be performed to reduce your risks, including credibility risk. It is our proposed approach to include these within our Audit and Risk Committee papers for your information only.

Commenced Audits



Delivering essential services to remote Aboriginal communities – Follow-up audit (State)
DLGSC’s regulation and support of local government (State)
Grant administration (State)
Managing unauthorised discharge of minor pollutants (Joint)
Regulation of consumer food safety (Joint)
Contracted-out maintenance (State)
Major projects – Status reports (State)
Audit results report – Annual 2019-20 financial audits of State government entities
Audit results report – Annual 2019-20 financial audits of local government entities
Information systems audit – Application reviews (State)
COVID-19 Relief Fund (State)
Department of Communities’ administration of family and domestic violence support services (State)
State of cyber security in local government entities (Local)
Safe and viable cycling in the Perth and Peel region (Local)
COVID-19: Status of testing systems

4. Publications

There are no publications we have identified we believe may be of interest to the Audit and Risk Committee.

5. Questions

Michelle Shafizadeh and Duy Vo are available to answer any questions that you may have at the meeting.

MOORE

PAYROLL INTERNAL AUDIT

City of Nedlands

16 October 2020

www.moore-australia.com.au

TABLE OF CONTENTS

1. Engagement Overview

1.1. Scope of Services

The Audit Plan for Year 2 approved by the CEO and endorsed by the Audit & Risk Committee on 2 September 2019, considered the following areas to be of priority for internal audit in FY 2019/20:

1. Accounts Receivables End to End Process Review
2. Business Continuity Review (Completed March 2020)
3. Payroll Audit

1.2. Audit Scope

The agreed scope for Payroll Internal Audit is as follows:

- Review of the City's payroll policies and procedures;
- Assessment of segregation of duties regarding payroll and Human Resources (HR) roles and responsibilities;
- Review of the adequacy and effectiveness of controls within payroll processing i.e. fortnightly payroll, termination payments, new employees, payroll reconciliations and employer obligations; and
- Review the controls over employee master file and employee payroll records.

2. Executive Summary

2.1 Background

The City’s payroll function consists of a Payroll Officer who reports directly to the Manager, Financial Services. The Payroll Officer is responsible for data entry of timesheets and all payroll processing tasks involved in paying employees. The Payroll module is part of the Authority system; there is currently no separate HR module. The set-up of employee master file details are also the responsibility of the Payroll Officer based on documentation provided by HR. Two SharePoint folders have been set up for the exclusive use by Payroll and HR for communication and document exchange purposes.

There are currently two staff in HR, reporting through to the HR Manager. There are a total of 176 permanent and 15 casual staff. Total payroll expenditure was $13,439,591 as per the Payroll Summary Report for FY 2019/2020.

2.2 Overall Results

The review has highlighted that the Authority Payroll system is out-dated and does not contain system controls and interfaces normally expected of a contemporary payroll system. The current deployment of the Authority HR system does not interface with Payroll Authority and is limited in its functionality as it is only used for Position Management purposes. As a result, there are numerous workarounds and labour-intensive procedures associated with payroll processing.

Notwithstanding the system limitations, the City’s payroll processes are well controlled due to the recent improvements implemented by the incumbent Payroll Officer to manage and control document exchange between HR and Payroll. The Payroll Officer has also developed control procedures using Excel to document pay changes from the previous pay cycle to the current pay cycle. The Excel spreadsheet provides a structured process for the Payroll Officer to ensure the changes required have been input correctly and reconcile back to the Payroll system i.e. total employee numbers; change in total gross salary.

Our review of the end to end payroll processes, however, indicated the lack of a robust detailed check at the supervisory level. This presents a segregation of duties risk as the current Payroll Officer is responsible for creating employee master file details in Payroll system as well as complete payroll processing and payroll reconciliation responsibilities. Fraud risk is significantly increased in this scenario. The review of system access privileges by IT also revealed weaknesses in the approach that was taken to assess access for appropriateness and adequate segregation of duties.

It is our understanding there are plans to move Payroll into HR. Due to the size of the HR function, there will be options to segregate certain tasks to ensure that the person performing the main payroll duties are not involved in employee master file responsibilities.

Our sample testing of 25 employee pays which included existing, new and terminating employees, to the best of our knowledge, did not detect any inappropriate payments. We also reviewed the processes around leave management and found the City to be pro-active in ensuring staff with 8 or more weeks of annual leave are on leave plans to reduce the City’s leave liability. Payroll reconciliations appear to be performed accurately, on time and independently reviewed. The limited samples that we tested means that fraud or misconduct could still have occurred as our testing was not tailored to identify this.

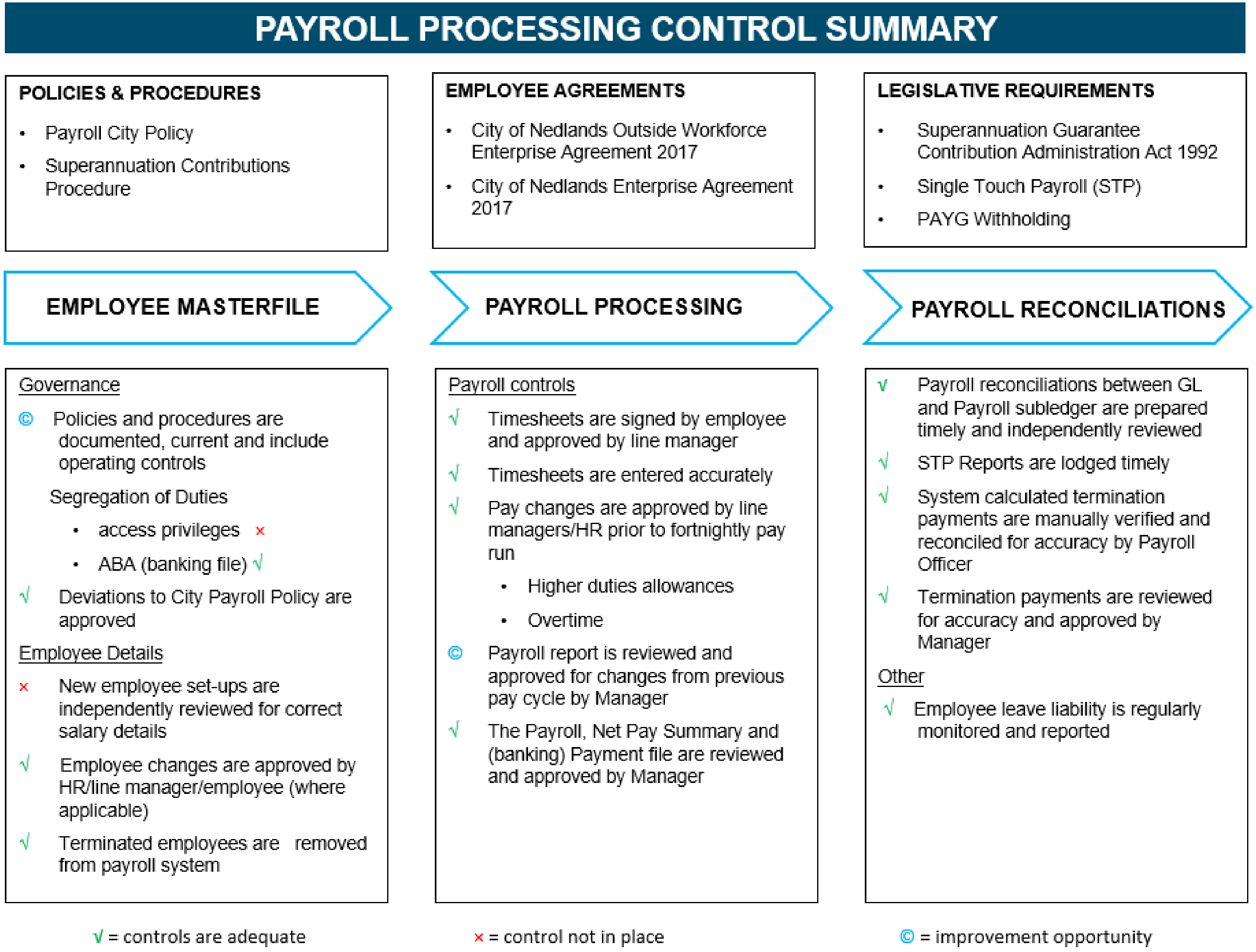
Please refer to 2.3 Key Observations and Recommendations.

2. Executive Summary

2.3 Key Observations and Recommendations

NO	OBSERVATIONS	RECOMMENDATIONS	RATING
1	**Lack of Segregation of Duties** Payroll Officer has numerous incompatible system responsibilities which enable full access to create, change and delete employee master file details as well as perform payroll processes. This presents an increased risk undetected of fraud or error. Refer to page 7 for further details.	Set-up of new employee salary details in Payroll system should be performed by someone other than the Payroll Officer. Employee master file details should be independently reviewed post set-up. Consider workflow approval for new employee set-ups as a future state consideration.	H
2	**Lack of Segregation of Duties – System Access** Review of system access privileges for Payroll and HR was not adequate to ensure that critical and sensitive transactions have been appropriately assigned. This presents an increased risk of undetected fraud or error. Refer to page 8 for further details.	IT to conduct an initial and regular review of system access in conjunction with the business to ensure critical and sensitive transactions are segregated via user role profiles.	H
3	**Lack of Independent Review of Payroll Reports** The supervisory review procedures of the payroll report does not entail a detailed review back to supporting documentation for all high-risk transactions i.e. first salary payment for new employee. This presents an increased risk of undetected fraud or error. Refer to page 9 for further details.	The supervisory review procedures should include a detailed review of high-risk transactions.	H
4	**Lack of Current Payroll Procedures** Existing documented payroll procedures do not reflect current practices and do not contain operating controls which need to be performed. This presents a risk that payments to employees are not authorised, or not in accordance with award conditions. There is also a risk the payroll controls are reliant upon staff continuity. Refer to page 10 for further details.	Develop comprehensive payroll procedures including interfaces between HR and Payroll. The key roles and responsibilities associated with the Payroll and HR function should be described including the required operating controls.	M
5	**System Limitations** The current functionality of the Payroll and HR systems within Authority requires numerous manual processes. This presents an increased risk of undetected fraud or error. Refer to page 11 for further details.	We recommend the City's planned digital strategy as part of the Strategic Plan for 2020 – 2023 consider the system constraints identified in this review.	M

3. Payroll Procedures



PAYROLL PROCESSING CONTROL SUMMARY

POLICIES & PROCEDURES

- Payroll City Policy
- Superannuation Contributions Procedure

EMPLOYEE AGREEMENTS

- City of Nedlands Outside Workforce Enterprise Agreement 2017
- City of Nedlands Enterprise Agreement 2017

LEGISLATIVE REQUIREMENTS

- Superannuation Guarantee Contribution Administration Act 1992
- Single Touch Payroll (STP)
- PAYG Withholding

EMPLOYEE MASTERFILE

Governance

© Policies and procedures are documented, current and include operating controls

Segregation of Duties

- access privileges ×
- ABA (banking file) √

√ Deviations to City Payroll Policy are approved

Employee Details

× New employee set-ups are independently reviewed for correct salary details

√ Employee changes are approved by HR/line manager/employee (where applicable)

√ Terminated employees are removed from payroll system

PAYROLL PROCESSING

Payroll controls

√ Timesheets are signed by employee and approved by line manager

√ Timesheets are entered accurately

√ Pay changes are approved by line managers/HR prior to fortnightly pay run

- Higher duties allowances
- Overtime

© Payroll report is reviewed and approved for changes from previous pay cycle by Manager

√ The Payroll, Net Pay Summary and (banking) Payment file are reviewed and approved by Manager

PAYROLL RECONCILIATIONS

√ Payroll reconciliations between GL and Payroll subledger are prepared timely and independently reviewed

√ STP Reports are lodged timely

√ System calculated termination payments are manually verified and reconciled for accuracy by Payroll Officer

√ Termination payments are reviewed for accuracy and approved by Manager

Other

√ Employee leave liability is regularly monitored and reported

√ = controls are adequate × = control not in place © = improvement opportunity

4. Details of Observations and Recommendations

<table>
<tr><th>NO</th><th>OBSERVATION</th><th>POTENTIAL RISKS</th><th>RATING</th><th>RECOMMENDAITON</th><th>AGREED MANAGEMENT ACTION</th><th>ACTION OWNER & DUE DATE</th></tr>
<tr><td>1</td><td colspan="6"><b>Segregation of duties</b></td></tr>
<tr><td></td><td>The Payroll Officer is currently responsible for all the data entry into the Payroll System including creation of the employee master file without an independent detailed review process.

The following table illustrates all the key updates that are done as part of their role to prepare the payroll for the fortnightly pay cycle:

<table>
<tr><th></th><th>Transaction type</th></tr>
<tr><td>1</td><td>Employee creation</td></tr>
<tr><td>2</td><td>Employee termination</td></tr>
<tr><td>3</td><td>Update employee banking details</td></tr>
<tr><td>4</td><td>Update of employee level / salary</td></tr>
<tr><td>5</td><td>Input of timesheets for employee hours (including overtime)</td></tr>
<tr><td>6</td><td>Input of higher duties allowances</td></tr>
<tr><td>7</td><td>Input of employee leave</td></tr>
</table>

<b>Compensating control:</b>
Payroll can only set up new employees if Human Resources (HR) attaches a position number to the new employee via Position Management functionality within Authority.</td><td><i>Increased risk of undetected fraud or error</i></td><td>●</td><td>1. The set-up of salary details for new employees should be performed by someone other than the Payroll Officer.</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>2. Creations and changes to employee master file details impacting on salaries and/or employee level, should be independently reviewed after the changes have been made. There should be evidence of review by way of signature or initials.</td><td>This will be addressed in the new ERP system as the audit trail in the current format cannot be independently checked for changes made.</td><td>Manager responsible for Payroll.
June 2022</td></tr>
<tr><td></td><td></td><td></td><td></td><td>3. <b>Future state recommendation</b>
New employee set-ups or changes to employee master file data could be set up with workflow approval to ensure that there is an independent review process.</td><td>Will be considered under the new ERP system or via SharePoint in due course.</td><td>Manager responsible for Payroll.
June 2022</td></tr>
</table>

NO	OBSERVATION	POTENTIAL RISKS	RATING	RECOMMENDATION	AGREED MANAGEMENT ACTION	ACTION OWNER & DUE DATE
2	**Segregation of duties – System Access Privileges**					
	We reviewed the system access privileges for the following: • Payroll system (Authority); • Human Resources (HR) (Authority); • SharePoint folders used by Payroll, HR; and • ABA file (csv folder). Our findings are as follows: a) Critical and sensitive transactions have not been identified to ensure that those transactions are only assigned based on a ‘need to know’ basis due to job role. b) The system access review performed by IT in September/October 2019 did not involve consultation with the business to understand the nature of the transactions. There is a risk that the existing profiles assigned to staff are not appropriate. Examples: • Manager, Financial Services has access to Position Management, a key control which should be restricted to HR staff. • Two HR staff have 59 transactions in the Payroll module based on an access report provided by IT of their privileges under Human Resources Business Partner role profile. Our review of the access to SharePoint folders set-up specifically for HR and Payroll indicated that they are restricted to HR and Payroll staff. The csv folder is not accessible by the Payroll Officer.	*Increased risk of undetected fraud or error*	●	1. The access to Position Management should be removed from the Manager, Financial Services as soon as practicable. 2. Critical and sensitive transactions associated with Payroll module should be identified to ensure those specific transactions are only assigned to Payroll staff. 3. Following completion of recommendation #2, any critical or sensitive transactions that are part of the Human Resources Business Partner profile should be removed.	Agreed Agreed Agreed	Manager Business Systems September 2020 Manager Business Systems October 2020 Manager Business Systems November 2020

NO	OBSERVATION	POTENTIAL RISKS	RATING	RECOMMENDAITON	AGREED MANAGEMENT ACTION	ACTION OWNER & DUE DATE
3	**Review of Payroll Reports (fortnightly pay run)**					
	The review of payroll processes indicated the Payroll Officer has implemented robust controls and self-checks in place which help ensure the required changes for the pay cycle are input into the Payroll system accurately. The assessment of the payroll review processes performed by Manager; Financial Services indicated a more detailed check is required especially for new employees that are being paid for the first time. During the walkthrough with the Manager, Financial Services, it was confirmed that new employee salary details are not checked back to the employment contract to ensure it has been set-up correctly by the Payroll Officer. This check is critical as the new employee salary details have been set-up in the Payroll System by the Payroll Officer. We have confirmed that HR also does not perform a review of employee Masterfile details after initial notification to Payroll. Our sample testing of 10 new employees to the best of our knowledge, did not reveal any discrepancies. Our review of 3 fortnightly pay run cycles indicated the Final payroll reports (titled Pay Edit Listing) were signed off as approved by Manager, Financial Services.	*Increased risk of undetected fraud or error*	●	1. For new employees being paid for the first time, the Manager, Financial Services should perform a detailed check of system details back to employment contract either at the point of employee master file creation (refer point 1) or as part of the payroll review process.	Agreed that the check is required. The Manager responsible for Payroll will check to the Offer Letter signed by the CEO and staff.	Manager Financial Service September 2020
				2. **Future state recommendation** The feasibility of a “payroll change” report should be considered to ensure that all changes from current pay to previous pay are reported in a manner to facilitate an efficient review process.	To be considered in the new ERP system	Manager Business Systems June 2022

NO	OBSERVATION	POTENTIAL RISKS	RATING	RECOMMENDAITON	AGREED MANAGEMENT ACTION	ACTION OWNER & DUE DATE
4	**Payroll Procedures**					
	For better governance and to also assist with the smooth transition of the Payroll function over to HR, it is recommended that the current documented payroll procedures, "Pre-Payroll Preparation" are updated to reflect current practices and include details of operational controls which should be performed. Our review of the document, Pre-Payroll Preparation documentation indicates it is an explanation of the menu screens and does not include the SharePoint folders and controls that have been recently implemented by the Payroll Officer. Other gaps in the current procedural documentation include: • Employee master file set-up • Payroll review controls • Payroll reconciliation tasks • Calculation of redundancy and termination payments • Leave entitlements as it relates to pay processing • Access privileges to HR/Payroll SharePoint folders • Recordkeeping of payroll files and data	*An increased risk that payroll controls may not be performed as required or is reliant upon staff continuity.*	●	Develop documented approved comprehensive Payroll Procedures which include all the key roles and responsibilities of the Payroll and/or HR function including operating and supervisory controls. We recommend the procedures include a visual graphic of the payroll processes to help to identify the workflow ensuring key controls are performed by the appropriate resource and at the right time. This will help ensure segregation of duties is maintained between critical HR and Payroll through system access privileges.	Approved payroll procedures will be updated to include the operating and supervisory controls. Agreed but will be documented in a payroll process document.	Manager Financial Services December 2020 Manager Financial Services December 2020

NO	OBSERVATION	POTENTIAL RISKS	RATING	RECOMMENDAITON	AGREED MANAGEMENT ACTION	ACTION OWNER & DUE DATE
5	**System Limitations**					
	During the course of our review, we have observed some shortcomings of the current Payroll and HR system functionality. Examples identified include: • Insufficient controls which separate creation of employee salary data from pay processing tasks; • Document exchange between HR and Payroll is reliant on SharePoint folders which are not integrated with Authority; and • Inaccurate sick leave balances; the system reports sick leave balances incorrectly. A manual review of an employee's sick leave history at the time of termination must be performed to ensure they have earned the sick leave taken. • Timesheets are also manually input into the Payroll system by the Payroll Officer. This is a time-consuming activity and prone to human error for the employee, their approving supervisory/line manager and Payroll.	*This presents an in inefficient process including increased risk of undetected fraud or error.*	●	We understand the City is developing a digital strategy as part of the Strategic Plan for 2020 – 2023. It is recommended the shortcomings noted in this review are considered as part of the future state requirements.	Agreed	Manager Business Systems December 2021

4. Details of Observations and Recommendations

Classification of Review Observations

The following classification has been used to assist Management with prioritising internal audit findings according to their relative significance and in consideration of their impact to the business process.

🔴 Issue represents a weakness which will/may have an adverse effect on the ability to achieve business objectives. Requires immediate management action. Includes risk of breaches to legislative requirements if not addressed.

🟡 Issue represents a weakness which may become more serious if not addressed. Requires management action within a reasonable time period.

🟢 Issue represents an opportunity for improvement. Management should consider cost benefit analysis within a reasonable time period.

Note: The rating assessment as detailed above is our assessment based on the circumstances surrounding the procedures performed. They are intended to be read in the context of our rating assessment to the organisation as a whole. They are provided solely to assist you understand the nature of the matters raised and to prioritise any remedial action.

5. Other

5.1. Disclaimers

Liability limited by a scheme approved under Professional Standards Legislation.

This information has been prepared for use by you subject to the terms of our engagement that include confidentiality conditions limiting the extent to which this document may be disclosed to individuals and the purposes for which it may be used. Please refer to Moore Australia (WA) Pty Ltd's terms of engagement.

Moore Australia (WA) Pty Ltd reserves the right to change, amend or update our findings and this report, should additional information become available.

Statements contained in this report are given in good faith, and in the belief that they are not false, misleading or incomplete. however, in the preparation of this report Moore Australia (WA) Pty Ltd has relied upon the information provided to us which we understand to be reliable, complete and not misleading.

Moore Australia (WA) Pty Ltd does not warrant or imply, nor should it be construed, that it has conducted an audit, or verification of the information provided to us which we have relied upon, however we have no reason to believe that any of the information provided, is false or materially incorrect.

The statements provided in this report are given in good faith

Moore Australia (WA) Pty Ltd trading as agent – ABN 99433 544 961, an independent member of Moore Global Network Limited - members in principal cities throughout the world.

5.2. Independence

Moore Australia (WA) Pty Ltd does not provide external audit services to City of Nedlands. Prior to accepting this engagement, Moore Australia (WA) Pty Ltd assessed that its independence is not impaired. At the date of this report, Moore Australia (WA) Pty Ltd does not have any relationship that would impair its independence in relation to this report.

CONTACT US

Level 15, 2 The Esplanade,
Perth WA 6000

T +61 8 9225 5355

F +61 8 9225 6181

E perth@moore-australia.com.au

www.moore-australia.com.au

MOORE

HELPING YOU THRIVE IN A CHANGING WORLD

MOORE

City of Nedlands Potential Internal Audit Topics

Financial	Information Management and Technology	Community and Development Services
• Budget & Forecasting • Cash & Investments Management • Credit Card Management • Financial Management • Financial Reporting & Governance • Grants Applications/ payments and acquittals • Infrastructure assets maintenance and replacement- strategies and inspection programs • Major Capital Projects • Non-Rates Revenue Management • Payroll (October 2020) • Procurement and Tendering • Accounts Payable (January 2019) • Rates Invoicing & Collection • Supplier Master file Management • Timely Payment of Suppliers	• Application Systems Reviews • Cybersecurity Information Management Strategy • Information Technology Strategy • Information Security • Information Technology- General Controls Review • Records Management • Review of IT Policies (June 2019) • User Access Controls •	• Access and Inclusion • Asbestos Management • Building licence application and approval process • Cats & Dogs Registration • Closed-Circuit Television • Community Development • Community Grants Management • Environmental Regulation • Grants Management • Homelessness Management • Native Flora and Fauna Management • Public Health Management • Urban Planning • Waste Management

Corporate Administration

- Asset Management
- Audit and Risk Committee Effectiveness
- Business Continuity (June 2020)
- Customer Services
- Conflict of Interest, Gifts, Benefits and Hospitality
- Contract Management
- Corporate Business Plan Corporate Governance
- Emergency Management
- Financial Transaction Analysis
- Fleet Management
- Fraud and Misconduct
- Governance
- Human Resources (recruitment, performance management and terminations):
- Legislative compliance
- Long Term Financial Planning
- Occupational Health & Safety
- Post Implementation Review of Financial and Non-financial Systems
- Post Project Reviews
- Public Interest Disclosure
- Risk Management
- Systems of Insight Review (assessing the improvements from previous data analytics work)
- Training and Development
- Verifying Employee Identify and Credentials

Please Note:

- Moore Australia have not performed a risk assessment or liaised with any stakeholders to identify the above potential internal audit topics.
- Potential internal audit topics have been identified from our experience with Local and State Government, the private sector and better practice principles.
- The items marked as green have previously been performed by Moore Australia
- The items marked as red should in our opinion be performed regularly and if they have not, then we believe they should be strongly considered.

8.4 Financial Audit for Year Ended 30 June 2020 – Update on Issues and Status of the Audit

Committee	9 November 2020
Applicant	City of Nedlands
Employee Disclosure under *section 5.70 Local Government Act 1995*	Nil.
Director	Lorraine Driscoll – Director Corporate & Strategy
Attachments	1. Update from Auditors, KPMG on the status of the audit; 2. Update from the Auditor General on the status of the audit; and 3. Update from the Department of Local Government Sport and Cultural Industries on the proposed amendments to the Financial Management Regulations.
Confidential Attachments	Nil.

Executive Summary

The objective of this report is to provide the Audit and Risk Committee with an update on the issues and status of the financial audit for the year ended 30 June 2020.

There have been some delays in the audit process arising from shortcomings of the City's accounting system reporting capabilities, changes to accounting standards which have come into effect from 1 July 2019 and further proposed amendments to the Local Government Financial Management Regulations.

Recommendation to Committee

The Audit and Risk Committee notes and reviews the issues and status of the financial audit for the year ended 30 June 2020.

Discussion/Overview

The Auditor General (AG) has been the auditor for the City since the financial year 2019. The 2019 financials were audited by Macri Partners as contractors of the AG and 2020 financials are being audited by KPMG as contractors of the AG.

The relevant legislative requirements are as follows:

The City is to submit the annual financial report to the auditor by 30 September 2020 as required by the LGA S 6.4(3).

The audit report is to be completed (signed and sent out) by 31 December 2020 as required by the LGA S 7.9.

The annual report to be accepted by Council no later than 31 December 2020. If the auditor's report is not available in time for the annual report to be accepted by 31 December 2020, the annual report is to be accepted by the local government no later than 2 months after the auditor's report becomes available. This is in accordance with the LGA S 5.54.

A general meeting of electors is to be held once every financial year and within 56 days of Council accepting the annual report as required by the LGA S 5.27. However this requirement has been suspended for the declared COVID-19 emergency period.

The audit of the 2020 financials was planned to be completed by end of October 2020 and presented to the Committee at the meeting on 9 November 2020. However there have been some delays in the audit process arising from shortcomings of the City's accounting system reporting capabilities, changes to accounting standards which have come into effect from 1 July 2019 and further proposed amendments to the Local Government Financial Management Regulations.

The completion date of the audit is not ascertained yet and is likely to be delayed until the regulation amendments are gazetted.

The tabled report is presented to the Committee for their information and consideration.

Strategic Implications

How well does it fit with our strategic direction?

The Annual Financial Report, reports on the previous years financial activity which will allow the City to predict where funds need to be spent the following year to align with the strategic direction.

Who benefits?

The City of Nedlands community benefits from the Annual Financial Report, as it is a public document that they can view, to see how the City of Nedlands has allocated funds.

Does it involve a tolerable risk?

The risk of delay is tolerable as it is highly likely that deadlines will be met.

Do we have the information we need?

At the present time, there is some uncertainty surrounding the date of the regulation amendments to be gazetted which will affect the date of completion of the audit.

Budget/Financial Implications

Can we afford it?

There are no costs associated with this report.

8.4 - Attachment 1

KPMG

Office of the Auditor General
Serving the Public Interest

City of Nedlands

Audit Status Update
For the year ended 30 June 2020

Audit update

Office of the Auditor General
Serving the Public Interest

Financial statement audit status

- Controls testing completed and management letter prepared for controls testing findings. Draft management letter with City of Nedlands for comment
- Transactional testing in progress
- Treasury, PPE and Infrastructure testing finalised other than the vested land, leased property matters noted and final consideration of fair values
- General IT Controls testing completed. Draft management letter with City of Nedlands IT for review
- Prior year management letter status being finalised

Key audit findings (to date)

- IT system

Due to system limitations, management were unable to extract transactional data form Authority in a timely manner. Once extracted the data required modification to ensure it was in a usable format

Civica (Authority vendor) have permanent access to the IT system with the ability to make system changes. Whilst access to the system is logged at a network level, the logging of the changes processed at the Authority level does not allow monitoring of the changes that are made

Key matters outstanding

- Resolution of vested land & buildings accounting

Proposed changes to Local Government regulations (which are anticipated to be gazetted by November 2020) for 30 June 2020 require vested land & buildings to be accounted for in accordance with AASB 16 *Leases*, which is generally at zero cost. Management have identified the value associated with vested land. They are undertaking a process to identify the value associated with the vested buildings

- Leases

Management are calculating the right of use asset and lease liability relating to a commercial lease. The property is sub-leased to an external party which requires additional accounting considerations

- Finalisation of remaining audit procedures
- Finalisation of review of financial statement disclosures
- Final partner and OAG review of the audit workpapers and financial statements

Completed audits

Roads to Recovery grant acquittal completed on 30 October 2020

Punitha Perumal
Assistant Director,
Office of the Auditor General
+61 8 6557 7544
Punitha.Perumal@audit.wa.gov.au

Matthew Beevers
Engagement Partner
+61 8 9263 7228
+61 411 155 987
mbeevers@kpmg.com.au

John Ward
Engagement Director
+61 8 9263 7246
+61 424 047 710
jmward@kpmg.com.au

kpmg.com.au

kpmg.com.au/app

Download on the App Store

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Dear Mayors, Presidents and Chief Executive Officers

YOUR 2019-20 FINANCIAL AUDIT

I am writing to provide an update on the status of the Office of the Auditor General's (OAG) financial audit program for the local government sector.

Broadly, across the sector, financial statements were due to us at the end of September, as our teams finished State sector audits, with December 2020 the original date for audit finalisation.

As you will be aware from various information sources, there were significant changes to the Australian Accounting Standards for 30 June 2020. Some of these changes have implications for the financial reporting of assets by local governments.

We understand the Department of Local Government, Sport and Cultural Industries is still working to formalise necessary changes to the Local Government (Financial Management) Regulations 1996 (FM Regulations). They provided an initial LG Alert on 18 September 2020 and we understand they are drafting an additional alert.

As a consequence, the local government sector continues to seek urgent guidance on changes the Department is now proposing to the FM Regulations that will apply retrospectively to reporting requirements on certain classes of assets for the 2019-20 financial year.

We understand the regulatory changes are awaiting consideration and approval by Executive Council and no gazettal date had been confirmed.

We continue to receive a large number of enquiries from the local government sector on this matter, but are limited on the advice we can offer given the uncertainty surrounding the final form of the amendments and the fact we are not responsible for managing the process. This has created a significant impost on our financial audit work for this year's local government financial audit cycle. We request your patience with this matter.

We will endeavour to complete your audit to schedule, but ask for some flexibility and understanding, as any changes which are gazetted will require auditing. As we are fast approaching year end, it is inevitable that some bottlenecks will occur in this regard. Some exit meetings with audit committees and council meetings will need rescheduling, as we are not in a position to issue any opinions without amended regulations.

Please contact your OAG audit engagement leader should you wish to discuss this matter further or if you have questions around the documentation your entity needs to prepare for the audit. Thank you for your understanding during this time.

We look forward to working with you over coming months.

Yours sincerely

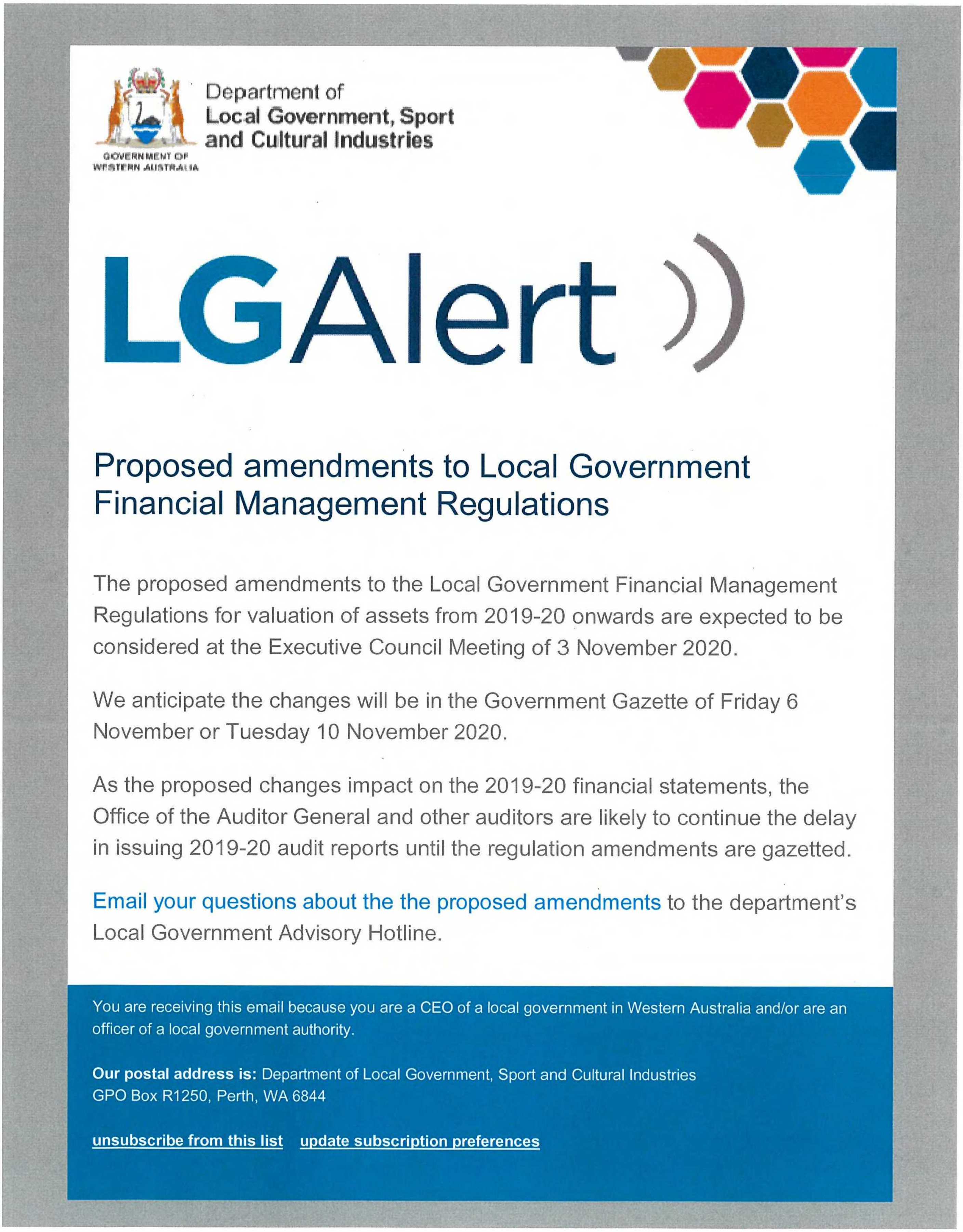
CAROLINE SPENCER
AUDITOR GENERAL
27 October 2020

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respect to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

OAG
Office of the Auditor General
Serving the Public Interest

The information contained in this email is confidential and is not for distribution without the author's prior consent.

From: Department of Local Government, Sport and Cultural Industries <newsletter@dlgsc.wa.gov.au>
Sent: Tuesday, 27 October 2020 4:40 PM
To: Council <council@nedlands.wa.gov.au>
Subject: Proposed amendments to Local Government Financial Management Regulations



GOVERNMENT OF WESTERN AUSTRALIA

Department of
Local Government, Sport
and Cultural Industries

LGAlert

Proposed amendments to Local Government Financial Management Regulations

The proposed amendments to the Local Government Financial Management Regulations for valuation of assets from 2019-20 onwards are expected to be considered at the Executive Council Meeting of 3 November 2020.

We anticipate the changes will be in the Government Gazette of Friday 6 November or Tuesday 10 November 2020.

As the proposed changes impact on the 2019-20 financial statements, the Office of the Auditor General and other auditors are likely to continue the delay in issuing 2019-20 audit reports until the regulation amendments are gazetted.

Email your questions about the the proposed amendments to the department's Local Government Advisory Hotline.

You are receiving this email because you are a CEO of a local government in Western Australia and/or are an officer of a local government authority.

Our postal address is: Department of Local Government, Sport and Cultural Industries
GPO Box R1250, Perth, WA 6844

unsubscribe from this list update subscription preferences

8.5 Audit & Risk Committee Dates for 2021

Committee	9 November 2020
Applicant	City of Nedlands
Employee Disclosure under *section 5.70 Local Government Act 1995*	Nil.
Director	Lorraine Driscoll – Director Corporate & Strategy
Attachments	Nil.
Confidential Attachments	Nil.

Executive Summary

This report seeks the Audit & Risk Committee's approval to set the Committee dates for 2021.

Recommendation to Committee

The Audit & Risk Committee agrees to the following Audit & Risk Committee Meeting Dates for the year 2021:

1. **Monday, 15 February 2021;**

2. **Monday, 14 June 2021;**

3. **Monday, 20 September 2021; and**

4. **Monday, 08 November 2021.**

Note: these dates are subject to change and extra meetings may be scheduled if the need arises.

Discussion/Overview

For the Audit and Risk Committee to fulfill its duty to the Council, it must meet several times a year.

In scheduling the meetings for 2021 around key financial and auditing dates the Audit & Risk Committee will be allowing Administration to plan reports around these dates and provide timely information to the Committee.

Key Relevant Previous Council Decisions:

There are no relevant previous Council decisions to consider.

Consultation

Nil.

Strategic Implications

How well does it fit with our strategic direction?

Scheduling the Audit and Risk Committee meetings for 2021 around key financial and auditing dates will manage the City of Nedlands' risk, which fits with the strategic direction.

Who benefits?

The Audit & Risk Committee members benefit from the dates for 2021 being set at the end of this calendar year. The organisation also benefits from having a schedule of meetings that enables it to ensure financial deadlines are met.

Does it involve a tolerable risk?

There is no risk associated with the recommendation.

Do we have the information we need?

All required information has been provided to the Committee.

Budget/Financial Implications

This does not have any financial implications

9. Reports by the Chief Executive Officer

There are no reports by the Chief Executive Officer.

10. Urgent Business Approved By the Presiding Member or By Decision

Any urgent business to be considered at this point.

11. Confidential Items

There are no confidential items.

12. Date of next meeting

The next meeting of the Audit & Risk Committee is to be confirmed.

Declaration of Closure

There being no further business, the Presiding Member will declare the meeting closed.