



City of Nedlands

Agenda

Audit & Risk Committee Meeting

22 February 2018

Dear Committee Member

The next meeting of the Audit & Risk Committee will be held on Monday, 22 February 2018 in the Meeting Room at the City of Nedlands Council Administration Building located at 71 Stirling Highway, Nedlands commencing at 5.30pm.

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.

Martyn Glover
Acting Chief Executive Officer
14 February 2018

Table of Contents

Declaration of Opening	3
Present and Apologies and Leave of Absence (Previously Approved)	3
1. Public Question Time	3
2. Addresses By Members of the Public (only for items listed on the agenda).....	4
3. Disclosures of Financial Interest	4
4. Disclosures of Interests Affecting Impartiality.....	4
5. Declarations by Members That They Have Not Given Due Consideration to Papers.....	4
6. Confirmation of Minutes	5
6.1 Audit & Risk Committee Meeting 27 November 2017	5
7. Items for Discussion.....	5
7.1 2017 Compliance Audit Report	6
7.2 Internal Audits	8
7.3 BDO Audit – Financial Application Control Review	11
7.4 Regulation 17	12
9. Confidential Items	16
10. Date of next meeting	16
Declaration of Closure	16

City of Nedlands

Notice of a meeting of the Audit & Risk Committee to be held in the Meeting Room at the City of Nedlands on Monday 22 February 2018 at 5:30pm.

Audit & Risk Committee Agenda

Declaration of Opening

The Presiding Member will declare the meeting open at 5:30pm and will draw attention to the disclaimer below.

(NOTE: Council at its meeting on 24 August 2004 resolved that should the meeting time reach 11.00 p.m. the meeting is to consider an adjournment motion to reconvene the next day).

Present and Apologies and Leave of Absence (Previously Approved)

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

Apologies Mr P Setchell Community Member

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 direct 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 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). 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 27 November 2017

The minutes of the Audit & Risk Committee held 27 November 2017 are to be confirmed.

7. 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.

7.1 2017 Compliance Audit Report

Owner	City of Nedlands
Officer	Stacey Gibson – PA to Director Corporate & Strategy
Director	Lorraine Driscoll – Director Corporate & Strategy
Director Signature	
Disclosure of Interest	No officer involved in the preparation of this report had any interest which required it to be declared in accordance with the provisions of the Local Government Act (1995).
Attachments	1. Compliance Audit Return 2017

Executive Summary

The 2017 Compliance Audit Return is an annual return that is required to be reviewed and adopted by Council prior to submission to the Department of Local Government by 31 March 2018. The Audit and Risk Committee are required to review the return and is to submit results for that review to Council.

Recommendation to Audit & Risk Committee

Committee recommend that Council adopts the 2017 Compliance Audit Return.

Discussion/Overview

Local governments are required to complete the annual Compliance Audit Return. The attached return for the City of Nedlands is for the period 1 January 2017 to 31 December 2017. It is required to be considered and adopted by Council, and submitted to the Department of Local Government by 31 March 2018. The Audit and Risk Committee is required to review the return and is to submit the results of that review to Council.

In accordance with Regulation 14 and 15 of the Local Government (Audit) Regulations 1996 the Compliance Audit Return 2017 must be:

1. Presented to the Audit and Risk Committee for review and then presented to Council;
2. Adopted by Council;
3. Recorded in the minutes of the meeting at which it was adopted; and
4. A certified copy of the return, along with a copy of the minutes recording its adoption, to be submitted to the Department of Local Government by 31 March 2018.

The City's 2017 Compliance Audit Return was completed in February following a review and assessment of :

- Council meeting agendas and minutes;
- Performance plans, media advertisements, procedures and policies, registers, delegation records, local laws; and
- Interviews with responsible officers.

Key Relevant Previous Council Decisions:

Not applicable.

Consultation

The Audit and Risk Committee is required to review the return and is to submit the results of that review to Council.

Budget/Financial Implications

The 2017 Compliance Audit Return has been conducted using internal resources and there are no other financial impacts.



Department of
**Local Government, Sport
and Cultural Industries**

Nedlands - Compliance Audit Return 2017

Certified Copy of Return

Please submit a signed copy to the Director General of the Department of Local Government, Sport and Cultural Industries together with a copy of section of relevant minutes.

Commercial Enterprises by Local Governments					
No	Reference	Question	Response	Comments	Respondent
1	s3.59(2)(a)(b)(c) F&G Reg 7,9	Has the local government prepared a business plan for each major trading undertaking in 2017.	N/A	No commercial Enterprises	Lorraine Driscoll
2	s3.59(2)(a)(b)(c) F&G Reg 7,10	Has the local government prepared a business plan for each major land transaction that was not exempt in 2017.	N/A	No commercial Enterprises	Lorraine Driscoll
3	s3.59(2)(a)(b)(c) F&G Reg 7,10	Has the local government prepared a business plan before entering into each land transaction that was preparatory to entry into a major land transaction in 2017.	N/A	No commercial Enterprises	Lorraine Driscoll
4	s3.59(4)	Has the local government given Statewide public notice of each proposal to commence a major trading undertaking or enter into a major land transaction for 2017.	N/A	No commercial Enterprises	Lorraine Driscoll
5	s3.59(5)	Did the Council, during 2017, resolve to proceed with each major land transaction or trading undertaking by absolute majority.	N/A	No commercial Enterprises	Lorraine Driscoll



Delegation of Power / Duty					
No	Reference	Question	Response	Comments	Respondent
1	s5.16, 5.17, 5.18	Were all delegations to committees resolved by absolute majority.	Yes		Nicole Ceric
2	s5.16, 5.17, 5.18	Were all delegations to committees in writing.	Yes		Nicole Ceric
3	s5.16, 5.17, 5.18	Were all delegations to committees within the limits specified in section 5.17.	Yes		Nicole Ceric
4	s5.16, 5.17, 5.18	Were all delegations to committees recorded in a register of delegations.	Yes		Nicole Ceric
5	s5.18	Has Council reviewed delegations to its committees in the 2016/2017 financial year.	Yes		Nicole Ceric
6	s5.42(1),5.43 Admin Reg 18G	Did the powers and duties of the Council delegated to the CEO exclude those as listed in section 5.43 of the Act.	Yes		Nicole Ceric
7	s5.42(1)(2) Admin Reg 18G	Were all delegations to the CEO resolved by an absolute majority.	Yes		Nicole Ceric
8	s5.42(1)(2) Admin Reg 18G	Were all delegations to the CEO in writing.	Yes		Nicole Ceric
9	s5.44(2)	Were all delegations by the CEO to any employee in writing.	Yes		Nicole Ceric
10	s5.45(1)(b)	Were all decisions by the Council to amend or revoke a delegation made by absolute majority.	N/A	No changes	Nicole Ceric
11	s5.46(1)	Has the CEO kept a register of all delegations made under the Act to him and to other employees.	Yes		Nicole Ceric
12	s5.46(2)	Were all delegations made under Division 4 of Part 5 of the Act reviewed by the delegator at least once during the 2016/2017 financial year.	Yes		Nicole Ceric
13	s5.46(3) Admin Reg 19	Did all persons exercising a delegated power or duty under the Act keep, on all occasions, a written record as required.	Yes		Nicole Ceric

Disclosure of Interest					
No	Reference	Question	Response	Comments	Respondent
1	s5.67	If a member disclosed an interest, did he/she ensure that they did not remain present to participate in any discussion or decision-making procedure relating to the matter in which the interest was disclosed (not including participation approvals granted under s5.68).	Yes		Nicole Ceric
2	s5.68(2)	Were all decisions made under section 5.68(1), and the extent of participation allowed, recorded in the minutes of Council and Committee meetings.	Yes		Nicole Ceric



Department of
**Local Government, Sport
and Cultural Industries**

No	Reference	Question	Response	Comments	Respondent
3	s5.73	Were disclosures under section 5.65 or 5.70 recorded in the minutes of the meeting at which the disclosure was made.	Yes		Nicole Ceric
4	s5.75(1) Admin Reg 22 Form 2	Was a primary return lodged by all newly elected members within three months of their start day.	Yes		Nicole Ceric
5	s5.75(1) Admin Reg 22 Form 2	Was a primary return lodged by all newly designated employees within three months of their start day.	Yes		Nicole Ceric
6	s5.76(1) Admin Reg 23 Form 3	Was an annual return lodged by all continuing elected members by 31 August 2017.	Yes		Nicole Ceric
7	s5.76(1) Admin Reg 23 Form 3	Was an annual return lodged by all designated employees by 31 August 2017.	Yes		Nicole Ceric
8	s5.77	On receipt of a primary or annual return, did the CEO, (or the Mayor/ President in the case of the CEO's return) on all occasions, give written acknowledgment of having received the return.	Yes		Nicole Ceric
9	s5.88(1)(2) Admin Reg 28	Did the CEO keep a register of financial interests which contained the returns lodged under section 5.75 and 5.76	Yes		Nicole Ceric
10	s5.88(1)(2) Admin Reg 28	Did the CEO keep a register of financial interests which contained a record of disclosures made under sections 5.65, 5.70 and 5.71, in the form prescribed in Administration Regulation 28.	Yes		Nicole Ceric
11	s5.88 (3)	Has the CEO removed all returns from the register when a person ceased to be a person required to lodge a return under section 5.75 or 5.76.	Yes		Nicole Ceric
12	s5.88(4)	Have all returns lodged under section 5.75 or 5.76 and removed from the register, been kept for a period of at least five years, after the person who lodged the return ceased to be a council member or designated employee.	Yes		Nicole Ceric
13	s5.103 Admin Reg 34C & Rules of Conduct Reg 11	Where an elected member or an employee disclosed an interest in a matter discussed at a Council or committee meeting where there was a reasonable belief that the impartiality of the person having the interest would be adversely affected, was it recorded in the minutes.	N/A		Nicole Ceric
14	s5.70(2)	Where an employee had an interest in any matter in respect of which the employee provided advice or a report directly to the Council or a Committee, did that person disclose the nature of that interest when giving the advice or report.	N/A	No disclosures for the year	Nicole Ceric



Department of
**Local Government, Sport
and Cultural Industries**

No	Reference	Question	Response	Comments	Respondent
15	s5.70(3)	Where an employee disclosed an interest under s5.70(2), did that person also disclose the extent of that interest when required to do so by the Council or a Committee.	N/A	No disclosures for the year	Nicole Ceric
16	s5.103(3) Admin Reg 34B	Has the CEO kept a register of all notifiable gifts received by Council members and employees.	Yes		Nicole Ceric

Disposal of Property

No	Reference	Question	Response	Comments	Respondent
1	s3.58(3)	Was local public notice given prior to disposal for any property not disposed of by public auction or tender (except where excluded by Section 3.58(5)).	Yes	As per 53.58(3)	Peter Mickleson
2	s3.58(4)	Where the local government disposed of property under section 3.58(3), did it provide details, as prescribed by section 3.58(4), in the required local public notice for each disposal of property.	Yes	See Council Resolution or Advert	Peter Mickleson

Elections

No	Reference	Question	Response	Comments	Respondent
1	Elect Reg 30G (1)	Did the CEO establish and maintain an electoral gift register and ensure that all 'disclosure of gifts' forms completed by candidates and received by the CEO were placed on the electoral gift register at the time of receipt by the CEO and in a manner that clearly identifies and distinguishes the candidates.	Yes		Stacey Gibson

Finance

No	Reference	Question	Response	Comments	Respondent
1	s7.1A	Has the local government established an audit committee and appointed members by absolute majority in accordance with section 7.1A of the Act.	Yes		Lorraine Driscoll
2	s7.1B	Where a local government determined to delegate to its audit committee any powers or duties under Part 7 of the Act, did it do so by absolute majority.	N/A		Vanaja Jayaraman
3	s7.3	Was the person(s) appointed by the local government to be its auditor, a registered company auditor.	Yes		Lorraine Driscoll
4	s7.3, 7.6(3)	Was the person or persons appointed by the local government to be its auditor, appointed by an absolute majority decision of Council.	Yes		Lorraine Driscoll



Department of
**Local Government, Sport
and Cultural Industries**

No	Reference	Question	Response	Comments	Respondent
5	Audit Reg 10	Was the Auditor's report for the financial year ended 30 June 2017 received by the local government within 30 days of completion of the audit.	Yes		Lorraine Driscoll
6	s7.9(1)	Was the Auditor's report for the financial year ended 30 June 2017 received by the local government by 31 December 2017.	Yes		Lorraine Driscoll
7	S7.12A(3)	Where the local government determined that matters raised in the auditor's report prepared under s7.9 (1) of the Act required action to be taken by the local government, was that action undertaken.	N/A		Vanaja Jayaraman
8	S7.12A (4)	Where the local government determined that matters raised in the auditor's report (prepared under s7.9 (1) of the Act) required action to be taken by the local government, was a report prepared on any actions undertaken.	N/A		Vanaja Jayaraman
9	S7.12A (4)	Where the local government determined that matters raised in the auditor's report (prepared under s7.9 (1) of the Act) required action to be taken by the local government, was a copy of the report forwarded to the Minister by the end of the financial year or 6 months after the last report prepared under s7.9 was received by the local government whichever was the latest in time.	N/A		Vanaja Jayaraman
10	Audit Reg 7	Did the agreement between the local government and its auditor include the objectives of the audit.	Yes		Vanaja Jayaraman
11	Audit Reg 7	Did the agreement between the local government and its auditor include the scope of the audit.	Yes		Vanaja Jayaraman
12	Audit Reg 7	Did the agreement between the local government and its auditor include a plan for the audit.	Yes		Vanaja Jayaraman
13	Audit Reg 7	Did the agreement between the local government and its auditor include details of the remuneration and expenses to be paid to the auditor.	Yes		Vanaja Jayaraman
14	Audit Reg 7	Did the agreement between the local government and its auditor include the method to be used by the local government to communicate with, and supply information to, the auditor.	Yes		Vanaja Jayaraman



Department of
**Local Government, Sport
and Cultural Industries**

Integrated Planning and Reporting					
No	Reference	Question	Response	Comments	Respondent
1	s5.56 Admin Reg 19DA (6)	Has the local government adopted a Corporate Business Plan. If Yes, please provide adoption date of the most recent Plan in Comments. This question is optional, answer N/A if you choose not to respond.	N/A		Lorraine Driscoll
2	s5.56 Admin Reg 19DA (6)	Has the local government adopted a modification to the most recent Corporate Business Plan. If Yes, please provide adoption date in Comments. This question is optional, answer N/A if you choose not to respond.	N/A		Lorraine Driscoll
3	s5.56 Admin Reg 19C (7)	Has the local government adopted a Strategic Community Plan. If Yes, please provide adoption date of the most recent Plan in Comments. This question is optional, answer N/A if you choose not to respond.	N/A		Lorraine Driscoll
4	s5.56 Admin Reg 19C (7)	Has the local government adopted a modification to the most recent Strategic Community Plan. If Yes, please provide adoption date in Comments. This question is optional, answer N/A if you choose not to respond.	N/A		Lorraine Driscoll
5	S5.56	Has the local government adopted an Asset Management Plan. If Yes, in Comments please provide date of the most recent Plan, plus if adopted or endorsed by Council the date of adoption or endorsement. This question is optional, answer N/A if you choose not to respond.	N/A		Lorraine Driscoll
6	S5.56	Has the local government adopted a Long Term Financial Plan. If Yes, in Comments please provide date of the most recent Plan, plus if adopted or endorsed by Council the date of adoption or endorsement. This question is optional, answer N/A if you choose not to respond.	N/A		Lorraine Driscoll
7	S5.56	Has the local government adopted a Workforce Plan. If Yes, in Comments please provide date of the most recent Plan plus if adopted or endorsed by Council the date of adoption or endorsement. This question is optional, answer N/A if you choose not to respond.	N/A		Lorraine Driscoll



Department of
**Local Government, Sport
and Cultural Industries**

Local Government Employees						
No	Reference	Question	Response	Comments	Respondent	
1	Admin Reg 18C	Did the local government approve the process to be used for the selection and appointment of the CEO before the position of CEO was advertised.	N/A		Shelley Mettam	
2	s5.36(4) s5.37(3), Admin Reg 18A	Were all vacancies for the position of CEO and other designated senior employees advertised and did the advertising comply with s.5.36(4), 5.37(3) and Admin Reg 18A.	N/A		Shelley Mettam	
3	Admin Reg 18F	Was the remuneration and other benefits paid to a CEO on appointment the same remuneration and benefits advertised for the position of CEO under section 5.36(4).	N/A		Shelley Mettam	
4	Admin Regs 18E	Did the local government ensure checks were carried out to confirm that the information in an application for employment was true (applicable to CEO only).	N/A		Shelley Mettam	
5	s5.37(2)	Did the CEO inform council of each proposal to employ or dismiss a designated senior employee.	N/A		Shelley Mettam	

DRAFT



Official Conduct					
No	Reference	Question	Response	Comments	Respondent
1	s5.120	Where the CEO is not the complaints officer, has the local government designated a senior employee, as defined under s5.37, to be its complaints officer.	N/A	CEO is the Complaints Officer	Nicole Ceric
2	s5.121(1)	Has the complaints officer for the local government maintained a register of complaints which records all complaints that result in action under s5.110(6)(b) or (c).	Yes		Nicole Ceric
3	s5.121(2)(a)	Does the complaints register maintained by the complaints officer include provision for recording of the name of the council member about whom the complaint is made.	Yes		Nicole Ceric
4	s5.121(2)(b)	Does the complaints register maintained by the complaints officer include provision for recording the name of the person who makes the complaint.	Yes		Nicole Ceric
5	s5.121(2)(c)	Does the complaints register maintained by the complaints officer include provision for recording a description of the minor breach that the standards panel finds has occurred.	Yes		Nicole Ceric
6	s5.121(2)(d)	Does the complaints register maintained by the complaints officer include the provision to record details of the action taken under s5.110(6)(b) or (c).	Yes		Nicole Ceric

Tenders for Providing Goods and Services					
No	Reference	Question	Response	Comments	Respondent
1	s3.57 F&G Reg 11	Did the local government invite tenders on all occasions (before entering into contracts for the supply of goods or services) where the consideration under the contract was, or was expected to be, worth more than the consideration stated in Regulation 11(1) of the Local Government (Functions & General) Regulations (Subject to Functions and General Regulation 11(2)).	Yes		Nathan Brewer
2	F&G Reg 12	Did the local government comply with F&G Reg 12 when deciding to enter into multiple contracts rather than inviting tenders for a single contract.	Yes		Nathan Brewer
3	F&G Reg 14(1) & (3)	Did the local government invite tenders via Statewide public notice.	Yes		Nathan Brewer
4	F&G Reg 14 & 15	Did the local government's advertising and tender documentation comply with F&G Regs 14, 15 & 16.	Yes		Nathan Brewer



Department of
**Local Government, Sport
and Cultural Industries**

No	Reference	Question	Response	Comments	Respondent
5	F&G Reg 14(5)	If the local government sought to vary the information supplied to tenderers, was every reasonable step taken to give each person who sought copies of the tender documents or each acceptable tenderer, notice of the variation.	Yes		Nathan Brewer
6	F&G Reg 16	Did the local government's procedure for receiving and opening tenders comply with the requirements of F&G Reg 16.	Yes		Nathan Brewer
7	F&G Reg 18(1)	Did the local government reject the tenders that were not submitted at the place, and within the time specified in the invitation to tender.	Yes		Nathan Brewer
8	F&G Reg 18 (4)	In relation to the tenders that were not rejected, did the local government assess which tender to accept and which tender was most advantageous to the local government to accept, by means of written evaluation criteria.	Yes		Nathan Brewer
9	F&G Reg 17	Did the information recorded in the local government's tender register comply with the requirements of F&G Reg 17.	Yes		Nathan Brewer
10	F&G Reg 19	Was each tenderer sent written notice advising particulars of the successful tender or advising that no tender was accepted.	Yes		Nathan Brewer
11	F&G Reg 21 & 22	Did the local government's advertising and expression of interest documentation comply with the requirements of F&G Regs 21 and 22.	Yes		Nathan Brewer
12	F&G Reg 23(1)	Did the local government reject the expressions of interest that were not submitted at the place and within the time specified in the notice.	Yes		Nathan Brewer
13	F&G Reg 23(4)	After the local government considered expressions of interest, did the CEO list each person considered capable of satisfactorily supplying goods or services.	Yes		Nathan Brewer
14	F&G Reg 24	Was each person who submitted an expression of interest, given a notice in writing in accordance with Functions & General Regulation 24.	N/A	No panels of pre-qualified suppliers sought in 2017	Nathan Brewer
15	F&G Reg 24AD(2)	Did the local government invite applicants for a panel of pre-qualified suppliers via Statewide public notice.	N/A		Nathan Brewer
16	F&G Reg 24AD(4) & 24AE	Did the local government's advertising and panel documentation comply with F&G Regs 24AD(4) & 24AE.	N/A		Nathan Brewer



Department of
**Local Government, Sport
and Cultural Industries**

No	Reference	Question	Response	Comments	Respondent
17	F&G Reg 24AF	Did the local government's procedure for receiving and opening applications to join a panel of pre-qualified suppliers comply with the requirements of F&G Reg 16 as if the reference in that regulation to a tender were a reference to a panel application.	N/A		Nathan Brewer
18	F&G Reg 24AD(6)	If the local government sought to vary the information supplied to the panel, was every reasonable step taken to give each person who sought detailed information about the proposed panel or each person who submitted an application, notice of the variation.	N/A		Nathan Brewer
19	F&G Reg 24AH(1)	Did the local government reject the applications to join a panel of pre-qualified suppliers that were not submitted at the place, and within the time specified in the invitation for applications.	N/A		Nathan Brewer
20	F&G Reg 24AH(3)	In relation to the applications that were not rejected, did the local government assess which application(s) to accept and which application(s) were most advantageous to the local government to accept, by means of written evaluation criteria.	N/A		Nathan Brewer
21	F&G Reg 24AG	Did the information recorded in the local government's tender register about panels of pre-qualified suppliers, comply with the requirements of F&G Reg 24AG.	N/A		Nathan Brewer
22	F&G Reg 24AI	Did the local government send each person who submitted an application, written notice advising if the person's application was accepted and they are to be part of a panel of pre-qualified suppliers, or, that the application was not accepted.	N/A		Nathan Brewer
23	F&G Reg 24E	Where the local government gave a regional price preference in relation to a tender process, did the local government comply with the requirements of F&G Reg 24E in relation to the preparation of a regional price preference policy (only if a policy had not been previously adopted by Council).	N/A	No regional price preference	Nathan Brewer
24	F&G Reg 24F	Did the local government comply with the requirements of F&G Reg 24F in relation to an adopted regional price preference policy.	N/A		Nathan Brewer
25	F&G Reg 11A	Does the local government have a current purchasing policy in relation to contracts for other persons to supply goods or services where the consideration under the contract is, or is expected to be, \$150,000 or less.	Yes		Nathan Brewer



Department of
**Local Government, Sport
and Cultural Industries**


I certify this Compliance Audit return has been adopted by Council at its meeting on _____

Signed Mayor / President, Nedlands

Signed CEO, Nedlands

DRAFT

7.2 Internal Audits

Owner	City of Nedlands
Officer	Pollyanne Fisher – Policy & Projects Officer
Director	Lorraine Driscoll – Director Corporate & Strategy
Director Signature	
Disclosure of Interest	No officer involved in the preparation of this report had any interest which required it to be declared in accordance with the provisions of the Local Government Act (1995).
Attachments	1. BDO Audit Action Summary – In Progress 2. BDO Audit Action Summary - Completed

Executive Summary

BDO Audit (WA) Pty Ltd are the City’s appointed Internal Auditors. As part of an agreed Internal Audit plan, BDO Audit (WA) Pty Ltd have conducted a number of internal audits across various business areas within the City. This report seeks to provide Council with an update as to the actions and outcomes arising from these internal audits.

Recommendation to Audit and Risk Committee

Committee receives the City’s update for internal audits and notes the actions by Administration.

Discussion/Overview

The CEO called for tenders on 15 January 2014 inviting proposals from suitably qualified firms to provide an internal audit consultancy service, focusing on the City’s operations over a period of three years.

An internal audit provides a methodology for the City to focus on the inherent risks associated with a business area’s activities and processes, and to provide independent assurances that risks are being managed.

Pursuant to section 5.41 of the Act, the CEO is responsible for the day-to-day management of Council activities including the direction of staff and implicitly the internal audit function. The CEO has the option to engage an external auditor to complete a review of internal financial systems, or alternatively, the CEO may assign an internal audit officer to perform the task on a full-time or part-time basis.

In line with the strategic objective of managing the City's resources in a sustainable and responsible manner, the key objectives of the audit program are as follows:

- To satisfy the requirements of Regulation 6 of the Local Government (Financial Management) Regulations 1996; and
- To ensure that the City's business processes incorporate appropriate internal controls designed to safeguard the assets of the city while achieving efficient and effective utilisation of resources;

Regulation 6 of the Local Government (Financial Management) Regulations 1996 stipulate that the CEO is to:

“(c) undertake reviews of the appropriateness and effectiveness of the financial management systems and procedures of the local government regularly (and not less than once in every four years) and report to the local government the results of those reviews.”

In addition to this, the CEO sought to achieve operational improvements and efficiencies through an effective audit program to identify business processes that can be improved, and to ensure that the resources of the City are efficiently and effectively managed. Specifically, the CEO required auditing services that would examine the adequacy and effectiveness of the City's internal controls designed to safeguard the assets and make appropriate recommendations.

The areas identified to be covered within the audit program included:

- Risk Management
- Business Continuity Management
- Rates
- Investments
- Cash Handling
- Accounts Receivable
- Procurement and Contract Management
- Accounts Payable
- Human Resources
- Asset Management
- Building Services (Regulatory)
- Planning Services
- Waste Services
- Park Services
- Fleet Services
- Engineering Services
- Project Management
- Information Technology Controls

The tender was awarded to BDO Audit (WA) Pty Ltd for a three-year period commencing 1 April 2014. This contract was extended by one year in 2017 to continue providing audit services as part of an agreed program.

BDO have completed audits across a number of business areas and provided recommendations. These reports and recommendations have been reviewed by the City's Executive Management Team in the first instance, with final reports presented to the City's Audit and Risk Committee. The internal audits completed provide the City with an independent review of business functions, identifying weaknesses and improvements, all for the purpose of risk mitigation, service level improvements and increased efficiencies.

A number of agreed improvement actions have been completed to date and presented back to auditors to assist with their follow up reviews, evidencing improved business processes across a number of areas. Remaining items are in progress or pending to be completed in alignment with specific upcoming business activities. Actions currently in progress are presented in Attachment 1 whereas actions that have been fully completed are presented in Attachment 2.

Every improvement and outcome achieved by the City to address the confirmed actions that have arisen from each audit undertaken, further mitigate potential risk to the City and improves the levels of service it offers.

Key Relevant Previous Council Decisions:

Nil.

Consultation

The CEO reports to the Audit and Risk Committee in relation to the internal audit program.

Budget/Financial Implications

Sufficient operational budget is in place to cover the cost of audit services.

Compiled Outstanding Action List – Monitoring Log

Audit	Actions	Action Owner	Target Date	Status	Outcome
Project Management (item 3.4.1)	<p>Project management information A policy for the standard structure of storing project file folders and applying version control over key documentation should be communicated to all departments and become a required standard practice.</p>	Policy & Projects Officer – implement and to be carried out ongoing by project managers	<p>November 2015</p> <p>April 2018</p>	<p>On Hold</p> <p>In progress</p>	Put on hold to be implemented as part of 'SharePoint' solution under a consolidated project site. This solution became available in December 2017 and this item now being progressed.
Business Continuity Management Review (3.2.1)	<p>Formalisation of IT DRP and Business Continuity Sub Plan IT Disaster Recovery Plan IT DRP to be formalised as soon as practical, and should include the following:</p> <ul style="list-style-type: none"> • Disaster definition; • Disaster scenario; • Disaster recovery strategy; • Disaster recovery sites and services; • Disaster recovery team and responsibilities; 	Manager Corporate Strategy and Systems	<p>December 2015</p> <p>July 2016</p> <p>December 2018</p>	Completed	The BCP has been developed and tested. On the 28th of February 2017 the plan was tested for a second time and minor amendments were made to the plan.

	<ul style="list-style-type: none"> • Disaster recovery action plan; • Recovery sequence; • Test the plan; and • Maintaining the plan. 				
Business Continuity Management Review (3.2.3)	<p>IT DRP Testing</p> <p>Management to implement the following:</p> <ul style="list-style-type: none"> • Formalize the test strategy, plan and result for IT DRP testing conducted <p>Minimum testing requirements should include, nut not be limited to:</p> <ul style="list-style-type: none"> - Communication plans, - alternate site activation - Date backup and recovery - Physical and computer security; and - Recovery of critical business functions <ul style="list-style-type: none"> • Test to involve business users to conduct the business testing • Prepare test schedules for the DRP tests; • Conduct a test de brief, document issue log and lesson learned; • The City is also to provide test results on an annual basis and these are to be reported to responsible senior management and the board of directors or its responsible committee 	Manager Corporate Strategy and Systems	<p>December 2015</p> <p>July 2016</p> <p>December 2018</p>	In progress	<p>The BCP has been developed and tested. On the 28th of February 2017 the plan was tested for a second time and minor amendments were made to the plan.</p> <p>We are currently reviewing the potential of a secondary data centre for storage of the City’s backups, the chosen data centre will require the capacity and security to enable the City to go to full production in the event of a catastrophic shutdown of the primary service operating in Malaga.</p>

					Once the secondary site has been identified we can complete the IT Disaster Recovery Plan and associated procedures.
IT General Controls (3.3.1)	Formalisation of IT strategic plan With the current changes to the IT infrastructure, a documented IT strategic plan is crucial to ensure that business strategy and IT decisions are evaluated against the IT strategy to ensure alignment. The plan should be formalised, approved and signed off by management as soon as practicable.	Manager Corporate Strategy & Systems	March 2016 July 2016 December 2018	In progress	We are currently developing a Digital Strategy, the intention of this strategy is to describe a vision for the City in the way that it will conduct its business and to document the diverse and complex systems used in daily operations, and to identify the relationships between systems if at all, the age and life cycle, this in turn will help us to better prioritise, budget and manage the purchase of hardware and

					software systems in the future.
IT General Controls (4.1) <i>(Improvement Opportunity)</i>	<p>Backup and restoration testing</p> <p>Review the tapes backup process and determine whether this is still necessary with the online replication of data from production server at Malaga Data Centre to backup server at the Depot.</p> <p>If tape backup is still necessary, we recommend that management periodically restore the data from backup tapes to ensure that data could be restored successfully in the event of errors or system failure.</p> <p>To be undertaken as part of the finalisation of disaster recovery plan and documentation.</p>	Manager Corporate Strategy & Systems	<p>December 2015</p> <p>December 2018</p>	In progress	<p>The City is currently replicating 4.1 TB of core serves information, this includes, Mail, SharePoint, Authority, Associated databases, Active directory and Trim. Daily replication is currently 76GB at 3 hourly intervals and a snapshot every 7 days. Daily, Weekly and Monthly Backups are also take and test for integrity. We are currently seeking a secondary Data Centre that can be used for the soring of backups and full replication in the event of the Primary Data Center failing, this work will assist</p>

					in finalising a disaster recovery plan and associated documents
IT General Controls (4.2) <i>(Improvement Opportunity)</i>	Change Management Procedures Develop a formal change request form with the appropriate sign-off to ensure that sufficient permission is sought, rollback plan and documentation is maintained when changes are made to IT infrastructure, system and applications.	Manager Corporate Strategy & Systems	December 2015 December 2018	In progress	An electronic request form with associated work flows should be developed in SharePoint, Council's Core Information System. Further Exploration and understanding of the Documentation is required to enable practical solution.
Purchasing Card and Credit Card Control Self-Assessment (4)	Formalise credit card financial delegations and update procedure A delegation process for use of Credit cards belonging to a different card holder to be investigated and implemented.	Finance Manager	December 2016 April 2018	In progress	Policy and Project Officer to develop and implement new process within Credit Card Procedure
Purchasing Card and Credit Card Control Self-Assessment (5)	Include card cancellation process in the procedure Add card cancellation process to credit card procedure.	Finance Manager	December 2016 April 2018	In progress	Updates developed but not yet approved by Executive Team for implementation. To be followed up.
Fraud Management	Fraud management policy and procedures	Finance Manager	December 2016	In progress	Policy has been drafted and will be

Control Self-Assessment (1)	Create a formal fraud management policy and procedure based on relevant industry standards (such as AS8001-2008) to include detection, reporting, investigation and management of fraud.		June 2018		completed by June 2018
Accounts Receivable Control Self-Assessment (1)	Accounts Receivable Policy and Procedures Develop Accounts Receivable policy and update current procedures	Finance Manager	July 2018 April 2018	In progress	Policy being drafted and to be completed by April 2018
Accounts Receivable Control Self-Assessment (3)	Excessive Number of Users with Access to Accounts Receivable Modules Review current user access and allocate relevant and appropriate access for staff based on roles and responsibilities.	Finance Manager		In progress	The IT department in conjunction with the Finance team are in the process of identifying the appropriate user access on completion of this task The IT department will liaise with Civica the product vendor to have the appropriate changes made to user access
Payroll Review (2)	Improve segregation of duties for payroll Implement – audit trail (form 1 Sep 17) which identifies changes to payroll and employee particulars. To be reviewed and signed off by the Manager Finance and	Director Corporate and Strategy	December 2017	Completed	Processes are in place for improved segregation of duties.

	periodically reviewed by the Director Corporate and Strategy. Director perform weekly spot checks of payroll reports. Finance team member perform a monthly spot check of manual inputs of payroll information in payroll system.				
Payroll Review (3)	<p>Review, update and implement documented payroll policy and procedures</p> <p>Develop and document the Payroll Policy and further update the procedures to including:</p> <ul style="list-style-type: none"> -Changes to payroll data - Tax file number declarations - Termination payments - Fortnightly payroll processing - Terminating employee's payroll processing - Payroll month end reporting 	Manager Finance	<p>November 2017</p> <p>June 2018</p>	In progress	Payroll procedure updated. Policy being drafted and to be completed by June 2018
Payroll Review (4)	<p>Improve leave processing process</p> <p>Consider during phase 2 of SharePoint project to fix issues including – rejected leave requests do not update the employees leave records accurately unless a new leave request is processed</p>	Manager Human Resources	Late 2018		
Financial Applications Control (1)	<p>Improve application governance and management</p> <p>Develop policies and procedures to support the management and governance of the authority application that include</p>	Manager Corporate and Strategy	June 2018	In progress	City is in the process of reviewing 24 draft policies (8 active) and procedures for Information

	information security, data management, IT asset management, IT risk management and change management				Technology and Information Management
Financial Applications Control (2)	Improve application contract management Authority (Civica) service level agreement is out of date and does not include any reference to confidentiality and / or security requirements	Manager Corporate and Strategy	June 2018	In progress	City has already commenced discussions with Civica to develop new Service Level Agreement and City has a system health check planned
Financial Applications Control (3)	Improve application security management Authority (Civica) password policies be implemented with access managed, monitored and reviewed to ensure only authorized individuals are granted access based on business need.	Manager Corporate and Strategy	June 2018	In progress	Further investigation by the IT and Finance department and Civica to see if further improvements can be made to the Authority product
Financial Applications Control (4)	Improve disaster recovery, back-up and recovery process Develop a Disaster Recovery Plan or backup policy and procedures to ensure recovery of information assets to deliver normal business services	Manager Corporate and Strategy	June 2018		A Policy and procedure review is currently being conducted. See Business Continuity Management Review (3.2.1), (3.2.3), IT General Controls (4.1)

Financial Applications Control (4)	Improve application controls Implement data verification and input controls to Authority system, with automated transactional calculations and reconciliation where possible.	Manager Corporate and Strategy & Manger Finance	June 2018		City is engaging with Civica to review. Hall booking system currently being explored will assist with reduction in manual calculation of fees and charges.
------------------------------------	---	---	-----------	--	--

Note: A number of target dates have been extended from what was originally documented by auditors so that the activities align with various other associated business activities, and to accommodate staff changes and legislation requirements.

Compiled Outstanding Action List – Monitoring Log

Audit	Actions	Action Owner	Target Date	Status	Outcome
Risk Management (item 3.1.1)	<p>Lack of alignment of risk management strategy with the organisation's objectives and goals</p> <p>Recommendations of the audit to be incorporated into the existing draft Governance Framework for Risk Management. Framework to be implemented once approved.</p>	Manager Corporate & Strategy	October 2014	Completed	Framework implemented and reviewed monthly
Risk Management (item 3.2.1)	<p>Lack of formalisation and documentation of the risk management process</p> <p>Recommendations of the audit to be incorporated into the existing draft Governance Framework for Risk Management. Framework to be implemented once approved.</p>	Manager Corporate & Strategy	October 2014	Completed	Framework implemented and reviewed monthly
Risk Management (item 3.3.1)	<p>Insufficient risk description and communication</p> <p>Revised template for risk assessments is to be implemented and the risk register to be accessible to all via SharePoint. Greater</p>	Manager Corporate & Strategy	October 2014	Completed	

	awareness of the Framework and the location of templates and supporting documentation is to be arranged.				
Risk Management (item 3.3.2)	Missing practical advice in staff induction Staff presentation to be enhanced to include relevant information with regard to Risk Management, specifically to include practical, usable hands-on procedures that are tailored to the City's operating environment and potential needs.	Manager Corporate & Strategy	December 2014	Completed	
Risk Management (item 4.1)	Review of strategic risk register Strategic risks were included in the Strategic Community Plan and Corporate Business Plan. These are to be incorporated into the Risk Register for regular review and Governance Framework for Risk Management.	Policy & Projects Officer	December 2014	Completed	
Risk Management (item 4.2)	Job description - Corporate Strategy Director While there is already the inclusion of appropriate responsibilities in the PD for the Manager Corporate Strategy and Systems, and this officer reports to the Director Corporate and Strategy, it is agreed to update the PD for the Director to include appropriate responsibilities for risk management.	Director Corporate & Strategy	October 2014	Completed	
Procurement & Contract	Non-adherence to established procurement policies and procedures	Manager Finance	May 2015	Completed	Completed including demonstration to

<p>Management (item 3.1.1)</p>	<p>A) All staff involved in the procurement function will be reminded at least once every six months of the benefits to the City of complying with the City's Purchasing Procedure. Suppliers are also to be reminded that there could be delays in the processing of invoices not having a valid Purchase Order Number, and the City cannot be held responsible if payment terms are exceeded.</p> <p>B) In instances where the Invoice amount exceeds the PO value by not more than 30% or \$5,000 (whichever is lower), a written explanation by the authorising officer for the variance will be taken as complying with the requirements of the City. Should the variance be greater than the allowed tolerance, fresh POs would need to be raised.</p>		<p>December 2015</p>	<p>December 2015</p>	<p>Auditors that sufficient reminders are in place for this to happen every 6 months.</p>
<p>Procurement & Contract Management (item 3.2.1)</p>	<p>Lack of a complete and accurate contract list for Technical Services Full transition from TRIM to SharePoint will enable full contract listings to be efficiently maintained and generated within the SharePoint system.</p>	<p>N/A</p>	<p>N/A</p>	<p>Completed</p>	<p>Sharepoint case created for each contract, from which a list can be generated and is managed through a reporting process.</p>
<p>Procurement & Contract Management (item 3.2.2)</p>	<p>Self-approved Purchase Requisitions The independent Review of Requisitions before they are converted into Purchase Orders is sufficient control to prevent the</p>	<p>N/A</p>	<p>N/A</p>	<p>Completed</p>	<p>Control is already in place as an independent officer</p>

	raising of fraudulent POs. This is a more effective control than an exception report after the event.				reviews all requisitions made.
Procurement & Contract Management (item 3.2.3)	Purchasing Procedure needs to be reviewed and updated A review of the current procedure is to be carried out.	Policy & Projects Officer	June 2015 December 2015	Completed December 2015	Procedure updated and published to all staff.
Procurement & Contract Management (item 3.2.4)	Contract management policy and procedures should be documented Develop and document contract management policies and procedures to be communicated to all staff members.	Policy & Projects Officer in conjunction with Technical Services	September 2015 December 2015	Completed December 2015	Policy is not appropriate for contract management as this is an internal operational activity. Procedure created for staff including step by step guidance for management of contract documents and consistent data capture.
Procurement & Contract Management (item 4.1)	Multiple storage repositories for contract documentation Migrate all contractual documents whose terms have not expired from TRIM to SharePoint, to provide easy access when necessary and mitigate then risk of loss of hard copies.	Purchasing & Tenders Coordinator	July 2015	Completed July 2015	Completed. All current contract documentation copied to Sharepoint for a full listing in one accurate repository.

Project Management (item 3.2.1)	<p>Deficiency in keeping track of project management training for staff</p> <p>Training should be provided to the key staff involved in managing projects on the policies and procedures that are to be implemented. Integrated approach is to be used which aligns with annual and 6 monthly performance reviews. Manager to budget in training budgets as required.</p>	Manager Human Resources	<p>April 2015</p> <p>April 2016</p>	Completed	
Project Management (item 3.2.2)	<p>Inconsistent project risk management practices</p> <p>A) Key project management staff should be trained in the Project Risk Assessment procedure currently operated by the City.</p> <p>B) A standard Project Risk Register template with all related project risks should be documented and made available on the City's intranet.</p> <p>C) Project Managers should use the project risk register and add specific risks that relate to their projects.</p>	<p>A) Policy & Projects Officer</p> <p>B) Policy & Projects Officer</p> <p>C) Project Managers</p>	<p>June 2015</p> <p>June 2016</p>	Completed	Completed and being trialed
Project Management (item 3.3.1)	<p>Project classification</p> <p>Project scale assessment within current Project Plan and Project Implementation Document to be reviewed to reflect detailed recommendations of the audit.</p>	Policy & Projects Officer	<p>May 2015</p> <p>April 2016</p>	Completed	Completed and being trialed
Project Management (item 3.3.2)	<p>Project closure and evaluation</p> <p>A formal process to be established to complete project closure and evaluation</p>	Policy & Projects Officer	<p>April 2015</p> <p>April 2016</p>	Completed	Completed and being trialed

	with objective evaluation criteria, an authoritative review, and properly authorised approval and sign off.				
Project Management (item 3.3.3)	Project roles and responsibilities Project management and participants' roles and responsibilities are usually documented and communicated in the Project Plan.	Policy & Projects Officer	April 2015 April 2016	Completed	Completed and being trialed
Project Management (item 3.3.4)	Project change and issue management A) Project changes to be formally discussed and approved by key project stakeholders, and authorised by an individual with the delegated authority to sign off on the level of change sought. Add to change management and issue in project plan. B) A changes and issues register to be maintained on a "by project" basis as part of project documentation, including or alongside minutes of meetings. Add to change management and issue in project plan.	Policy & Projects Officer	June 2015 June 2016	Completed	Completed and being trialed
Project Management (item 3.4.2)	Project management templates In consultation with the managers of key business areas and project stakeholders, and having regard to the varying complexities and sizes of projects and the needs of sound project management practice, management should develop project management templates, forms, and	Policy & Projects Officer	June 2015 June 2016	Completed	Completed and being trialed

	checklists for each stage of the project management life-cycle.				
Cash and Bank Review (item 3.1.1)	Nab Connect User Accounts Deactivate the authorising rights when the staff members are not in the acting role.	Manager Finance	As Required	Completed	
Cash and Bank Review (item 3.2.1)	Cash Security – Administration Officer and Nedlands Library Out Station User Accounts A) The door to the cashier’s office is to be closed when no one is in the office. B) The side door to the Council Chambers is to be closed at all times, with entry restricted to those with Card Keys (swipe cards). C) Nedlands Library – the practice is to keep a small float (\$50) in a drawer at the front desk. Management is confident that the probability of theft from the drawer during the opening out is low, as is the impact of such a theft.	Director Corporate & Strategy		Completed	Administration building upgrades to address further too as an improvement opportunity. Proposed changes have Executive approval and are proceeding
Cash and Bank Review (item 3.3.3)	Authorised Signatories – Bank Records Management to request formal bank confirmations acknowledging receipt of the bank forms send in by the City. Management also to conduct a reconciliation between the signatories in the current Bank Authorisation form and the “Operation of Council Bank Accounts” Policy is accepted.	Director Corporate & Strategy	15 July 2014	Completed	

	The Financial expenditure thresholds are to be documented in the Council Policy Manual.				
Cash and Bank Review (item 3.3.4)	Breach of Term Deposit Thresholds Management to review the current deposit thresholds and Discuss whether they are still applicable and appropriate – to be implemented when the investment Policy is next reviewed in September 2014.	Director Corporate & Strategy	September 2014	Completed	
Cash and Bank Review (item 3.3.5)	Petty Cash Practices Staff to be reminded of the need to comply with the practices detailed in the Petty Cash Procedures documented. Alternatively the requirement should be removed from the Procedures document if this is an obsolete practice. Petty cash floats amounts to be introduced.	Manager Finance	July 2014	Completed	BDO identified in January 2015 review that there was an outstanding action to review the procedure. This was not required as part of the original recommendation and there are no specific issues identified that require it to be reviewed so this action is complete.
Expenses and Corporate Credit Card Review (item 3.1.1)	Inadequate or Deficient Policies, Procedures and Guidelines <ul style="list-style-type: none"> • Management to update the CCC Policy. • Card cancellation procedure will be fully documented • End of month statement review and invoice reconciliation process will be 	Director Corporate & Strategy	31 March 2015	Completed	

	<p>documented in sufficient detail and subsequent follow up and clearance of any queries.</p> <ul style="list-style-type: none"> Formalise the policy and procedures using the City of Nedlands official letter head and indicate the current and next review dates in the document. 				
Expenses and Corporate Credit Card Review (item 3.3.1)	<p>Inadequate P-Card Review Procedures</p> <p>A) Outline in the P-Card document that this list of Cardholders should be reviewed at least on a bi-annual or yearly basis</p> <p>B) Review to be performed with a view to ensure that current P-Card holders still have the need to have their P-Card, and that the approval process remains appropriate.</p> <p>C) Review will be documented and signed off as evidence of having been performed.</p> <p>D) P-Card policy to clearly define the acceptable timeframe for review.</p> <p>E) Review of P-Card Claims.</p>	Manager Finance	5 January 2015	Completed	
Expenses and Corporate Credit Card Review (item 3.3.2)	<p>Insufficient preventative restrictions over card usage</p> <p>Management should check with NAB if it is possible implement the same system controls for the CCC as for the P-card; ie to have the system restrict cardholders from withdrawing cash using a CCC.</p>	N/A	N/A	No action required	CCCs are restricted to the CEO and 3 Directors. There may be emergency situations when it is necessary for cash withdrawal by one of

					more of these executives.
IT General Controls (3.2.1)	<p>Lack of user access audit log The user log to be reviewed on a periodic basis by Security Administrator.</p>	Information Systems Coordinator	December 2015 and then ongoing	Completed	
IT General Controls (3.2.2)	<p>User Access Security Administration Procedures</p> <p>A) Improve the current user access request form to include more detail about the functions should be granted to user based on his/her job roles and responsibilities.</p> <p>In addition, the user ID deactivation form should include the list of system applications to be activated.</p> <p>B) Establish a formal user access review procedure with the view to remove or disable inactive users and to determine whether the access granted will commensurate with their current job role for the various applications in use at the City (Windows/Authority/Network folder/NAB online banking). This review should be conducted at least on a half yearly basis.</p>	Information Systems Coordinator	December 2015	Completed	Updated 6 monthly reports being provided to Management

	<p>The process should include:</p> <ul style="list-style-type: none"> • A list of users to be sent to business managers for them to validate individual user's access rights against their current job roles and responsibilities. • Once the review is performed, the IT Team should receive the inputs from business areas and perform the necessary actions or amendments. • E-mails and actions in relation to reviews should be retained as evidence of the required actions having been undertaken and for audit purposes. • Frequency of the review e.g. at least on a half yearly basis. • A user access security matrix should be developed and maintained as part of this process. 				
<p>IT General Controls (3.3.2)</p>	<p>Inadequate password parameter settings The Password Policy will be reviewed. Management should consider revising the password parameters setting to be consistent and in line with standard industry best practice as follows:</p> <p>Window Active Directory level</p> <p>A) Password Policy</p> <ul style="list-style-type: none"> • Minimum password length: 8 characters; 	<p>Manager Corporate Strategy & Systems</p>	<p>December 2015 April 2016</p>	<p>Completed</p>	<p>Implemented.</p>

	<ul style="list-style-type: none"> • Minimum password age: 7 days; • Password must meet complexity requirements - Enabled • Enforce password history – 10 passwords remembered; • Account lockout threshold – 5 invalid logon attempts; • Account lockout duration: 30 minutes <p>B) Audit Policy</p> <ul style="list-style-type: none"> • Audit account logon events: Success, failure; • Audit logon events: Success, failure; • Audit account management: Success, failure. 				
IT General Controls (3.3.3)	<p>Formalisation of ICT Protocols and Procedures</p> <p>Management should complete, review and update the ICT Protocols and Procedures document and communicate to all staff as soon as practicable.</p>	Manager Corporate Strategy & Systems	February 2016	Completed	
Fleet Review (3.2.1)	<p>Fleet vehicles policies and procedures to be updated</p> <p>The City's procedure currently identifies that three groups (unrestricted private use, restricted private use and commute use) will all have a fuel card. The City will</p>	Policy & Project Officer	December 2016	Completed	

	<p>propose to remove fuel card from commute vehicle users. It is agreed that the procedure should be updated to reference the City's fuel pump at the depot.</p>				
Fleet Review (3.2.2)	<p>Human resources (HR) review of Drivers licenses needs improvement Human Resources should perform checks on all staff that drive City vehicles once a year to check validity of license and update register. Agree that drivers licence register be completed and updated.</p>	Manager Human Resources	August 2016	Completed	And forms part of updated vehicle procedure
Fleet Review (3.2.3)	<p>Enhancement of the existing fleet vehicles register A single register to be maintained and stored in Sharepoint.</p>	Manager Engineering Services	September 2016	Completed	Polly to save the register in sharepoint and create a link from Workshop Coordinator's desktop to replace current desktop file
Fleet Review (4.1) <i>(Improvement Opportunity)</i>	<p>Potential cost saving if decommission fuel/fleet cards Costs savings would be made from removing commuter use fuel cards and issuing regular reminders to staff about using depot fuel pump where possible.</p>			Completed	
Fleet Review (4.2) <i>(Improvement Opportunity)</i>	<p>Enhancement of the SharePoint folders Sharepoint to be enhanced to include an extra column for completed when an infringement has been paid</p>			Completed	No action required. Workshop Coordinator has a 'task' created for each infringement

					that can be 'ticked' off to capture when paperwork has been processed – note the City does not pay the fine but returns paperwork to advise whom the fine is to be redirected to.
Fleet Review (4.2) <i>(Improvement Opportunity)</i>	Greater transparency of Purchase Orders Management to explore manual or system capabilities to allow Manager Engineering Services to view and track purchase orders raised by Workshop Coordinator.			Completed	Already in place
Purchasing Card and Credit Card Control Self-Assessment (2)	Review preferred payment methods to increase card security Current procedures identify email, post or facsimile as preferable methods for payment, however these carry high risk. Review process and documents and communicate out to card holders.		December 2016	Completed	
Human Resource Leave Management Control Self-Assessment (2)	Segregation of duties for leave processing process Review approval process for processing leave in Authority.		November 2016	Completed	On line leave forms will address this.
Human Resource Leave Management	Leave liability reporting process		Not applicable	No action required	Exec Management Team review in quarterly meetings

Control Self-Assessment (3)	Signing and documenting of liability reports to evidence managers have reviewed them.				and this is captured in the minutes.
Fraud Management Control Self-Assessment (2)	Formalise a fraud control plan Create a formal control plan based on a fraud risk assessment.		Not applicable		This will be implemented as we continue to develop our policies and systems and will be an on-going process with no end date.
Fraud Management Control Self-Assessment (3)	Enhance fraud control training and awareness Develop a targeted fraud training and awareness program for staff.		Not applicable		To be targeted at Directors and Managers to be fed down to staff. On-going process with no end date.
Investment management Control Self-Assessment (2)	Investment management training and awareness Consider providing staff investment management training as required to ensure adequate knowledge and skills for their specific role.		Not applicable	No action required	We do not agree that additional training in investment management is required. The investment approach at the City is fairly conservative, as determined by the policy and the officers responsible for decisions around investment are all CPA qualified, have

					experience in managing an investment portfolio such as this and regularly keep abreast of economic factors and movements in bank rates.
Investment management Control Self-Assessment (3)	<p>Assign Relevant Delegation of Authority for Investment purposes Recommend that the Delegation of Authority be updated to include investment management transactions and that these delegations should be included in the relevant policies and procedures.</p>		Not applicable	No action required	The Director Corporate & Strategy has delegated authority to approve investments. The Manager and Director are always involved in the roll over process, additionally deposit and disbursal require two signatories.
Business Continuity Management Review (3.2.2)	<p>Crisis Management and Business Continuity Response Plan a) BCP Plan Objectives, Scope & Plan Activation The sub plan for each area should initiate a process to identify critical risk to the business function. As estimate of the issue and perceived down time to the operation should then be feed to the CEO and</p>	Manager Corporate Strategy and Systems		Completed	The Manager Corporate & Strategy confirmed this Plan is completed and requires no further changes.

	<p>Executive in preparation for the possible implementation of the BCM.</p> <p>b) Clear roles and responsibilities Management to consider enhancing the current plan to include a section of description of role and responsibilities.</p> <p>c) Command Centre Command Centre to be pre designated as part of the BC strategy and the requirements to operate the command centre should be determined and documented in the plan – All communication infrastructures are cloud based, each council site is fully capable of delivering a crisis centre.</p> <p>d) Business Continuity Strategy and Response The plan is to descriptive instruction on the response option for loss scenarios.</p> <p>e) Site's office emergency plan Update the Crisis Management and business Continuity plan to provide clear reference to the site's emergency plan and remove emergency contact information from the CM and BCP to avoid maintenance of duplicate information in both plans. Also to advise emergency plan holder to update the emergency plan to include the reporting to CM and BCP team</p>				
--	---	--	--	--	--

	for deciding on activation of the CM and BCP.				
Business Continuity Management Review (3.2.4)	<p>BCP & DRP training</p> <p>Management intent to conduct work area reviews, develop documents then familiarizes the DCP process by going through the BCP exercise and tested with the staff. This will be reviewed every 2 years</p>	Manager Corporate Strategy and Systems		Completed	Activity carried out in April 2017 at the Adam Armstrong Pavilion with new Senior Staff.
Business Continuity Management Review (4.1)	<p>BCP Plan Maintenance</p> <p>Management to record all the change history and version number in the document control section rather than on the front page of the BCM Plan. Management to also define the plan maintenance procedures in the BCM policy for continuing management and monitoring.</p>	Manager Corporate Strategy and Systems		Completed	The Manager Corporate & Strategy confirmed this Plan is completed and requires no further changes.
Business Continuity Management Review (4.2)	<p>Improvement on the Crisis Management & Business Continuity Response Plan</p> <p>Management to consider enhancing the current plan to incorporate the following points:</p> <ul style="list-style-type: none"> • A decision tree approach to help guide the management team under situation of intense pressure; • Overall Crisis Management, Business Continuity Management and Emergency team organization structure; 	Manager Corporate Strategy and Systems		Completed	The Manager Corporate & Strategy confirmed this Plan is completed and requires no further changes.

	<ul style="list-style-type: none"> • Incident escalation procedures involve appropriate civil authorities and other external Agencies; • Procedures for handling the media and communications with internal and other external parties; • Notification details that the responsible officer required to provide to Emergency Management Team Directors when notified the event. <p>A glossary for technical term relating to the business continuity.</p>				
Capital Works (3.2.1)	<p>Lack of a Formalised Capital Works Framework</p> <p>A formalised framework will be developed in time for the 2016/17 Budget process. This will be linked to the Asset Management Strategy, Forward Works Plan as well as the Strategic Community Plan and Corporate Business Plan</p>	Director Technical Services and Director Corporate and Strategy		Completed	5 Year Capital Works Program has been developed in integration with Long Term Financial Planning, Asset Management Strategy and forecast, Strategic Community Plan and Corporate Business Plan
Capital Works (3.3.1)	<p>Insufficient comparative reviews of the Strategy Plan</p> <p>Management will review reporting against the Strategic Community Plan.</p>	Director Corporate & Strategy		Completed	Strategic Community Plan has been fully reported against, see 'Measuring Success in 2017' document and quarterly

					Corporate Business Plan reports, reviewed and redeveloped for more effective reviews going forwards. This is drafted along with an updated Corporate Business Plan and being reported to Council as a package with the Long Term Financial Plan.
IT General Controls (3.1.1)	<p>Inappropriate User Access Right Assignment A full review to be conducted to ensure access rights are aligned to job roles and responsibilities.</p>	Manager Corporate Strategy & Systems	No applicable	No action	<p>Reporting against user access aligned with job roles and responsibility is underway.</p> <p>The Audit report identified Authority accounts that remained open for terminated employees HOWEVER an accompanying Active Directory</p>

					<p>account is also required for these to work.</p> <p>The Active Directory Account management is effectively managed and up to date and are reported and reviewed quarterly.</p>
<p>IT General Controls (4.3) <i>(Improvement Opportunity)</i></p>	<p>Network Penetration Testing Conduct network penetration testing once the IT infrastructure changes are fully completed in order to ensure their current security measures are adequate to respond to intruder/cyber-attacks.</p>	<p>Manager Corporate Strategy & Systems</p>		<p>Completed</p>	
<p>Fleet Review (3.1.1)</p>	<p>Reliance on key personnel to perform key Workshop activities Manager Engineering will work with the Workshop Coordinator to share operational information.</p>	<p>Manager Engineering Services</p>	<p>December 2016</p>	<p>Completed</p>	<p>Manager Engineering has worked with the Workshop Coordinator to share operational information, and a new Apprentice Mechanic is now in place</p>
<p>Fleet Review (3.1.2)</p>	<p>Reliance on manual records for Fleet Services Any existing records that are hardcopy and not electronic files in TRIM or Sharepoint to</p>	<p>Manager Engineering Services</p>	<p>December 2016</p>	<p>Completed</p>	<p>Fleet solution in Sharepoint fully implemented with</p>

	be scanned into Sharepoint and this is to include any future records.				electronic data capture
Purchasing Card and Credit Card Control Self-Assessment (1)	Enhance Awareness of Purchasing Card Obligations and Responsibilities To reinforce the obligations, roles and responsibilities under the procedure, the purchase card process owner circulates the approved process (or link to) to all positions referenced in the purchasing card process on an annual basis.		September 2016	Completed	Completed and implemented annually going forwards
Human Resource Leave Management Control Self-Assessment (1)	Leave management policy and procedures Leave management policy and/or procedure to align with current business operational requirements.	Manager Human Resources			
Purchasing Card and Credit Card Control Self-Assessment (3)	Improve governance of credit card transactions For credit cards only: Currently, there is no independent review of the transactions to authorise the transaction's validity and/or appropriateness. Review process and documents and communicate out to card holders.	Finance Manager		Completed	CEO now reviews and signs off on all credit card transactions with Director Corporate and Strategy reviewing and signing off on CEOs
Purchasing Card and Credit Card Control Self-Assessment (6)	Opportunity to improve process efficiency "A credit card purchase record form must be completed for each transaction, giving details of the account numbers for costing purposes, the invoice and receipt attached	Finance Manager		Completed	Individual purchase record forms are now reconciled against the monthly statements


	<p>thereto, and submitted to the Finance Officer Accounts Payable”.</p> <p>BDO recommend creating and implementing a credit card purchase record form that captures ALL monthly transactions and required details that are incurred by the credit card holder for submission to the Finance Office Accounts Payable.</p>				
Accounts Receivable Control Self-Assessment (2)	<p>Segregation of Duties for Invoice Processing Process</p> <p>Implement reporting capabilities outlining invoice and credit transactions that are reviewed by management monthly / formal review and authorisation process for new invoice creation and credit note processing.</p>	Finance Manager		Completed	Invoice and credit notes have to be approved by Manager Finance before they are issued with a monthly review also being undertaken
Accounts Receivable Control Self-Assessment (4)	<p>Informal Accounts Receivable Delegation of Authority</p> <p>Formal delegation of authority for relevant Accounts Receivable processes.</p>	Finance Manager		Completed	Immediate approving officer signs off on invoice requests
Accounts Receivable Control Self-Assessment (5)	<p>Accounts Receivable Master File Governance</p> <p>Changes made to the master file should be segregated from the finance officer, reviewed and approved by another employee to ensure accuracy and validity of changes.</p>	Finance Manager	Not applicable	No action	This file contains contact details only. Risk is nominal.

Investment management Control Self-Assessment (1)	Investment management policy and procedures Review the current investment management policy and procedures and update it to align with the current business and operational requirements for Investment management.	Finance Manager		Completed	
Payroll Review (1)	Improve payroll system access control Remove the following positions as they are no longer required to be able to access the payroll module: - Manager Health and Compliance - Coordinator Management Accounting - Human Resource Business Partner	Director Corporate and Strategy		Completed	
Cash and Bank Review (item 3.3.1)	No Formalised Procedure for Opening and Closing Bank Accounts – Investment Accounts The policy will be reviewed and presented to the Audit and Risk Committee in the first instance for approval.	Manager Finance		Completed	Operation of Bank Accounts Policy and Procedure developed
Cash and Bank Review (item 3.3.2)	Cash Receipting – Nedlands Library Investigate the \$6.20 anomaly identified in order to determine how it arose. Measures to be put in place to prevent this issue arising again in the future. Float counts (which are evidenced) should continue to be performed at the Library; these should be performed on a sporadic basis. Management to work towards improving the receipting system implemented at	Manager Finance & Manager Community Services	1 July 2014	Completed	Finance Manager implemented new receipting checking processes

	Nedlands Library and investigate the receipting practices at the other Out Stations.				
--	--	--	--	--	--

Note: A number of target dates have been extended from what was originally documented by auditors so that the activities align with various other associated business activities, and to accommodate staff changes and legislation requirements.

7.3 BDO Audit – Financial Application Control Review

Owner	City of Nedlands
Officer	Andrew Melville - Manager Health & Compliance
Director	Lorraine Driscoll – Director Corporate & Strategy
Director Signature	
Disclosure of Interest	No officer involved in the preparation of this report had any interest which required it to be declared in accordance with the provisions of the Local Government Act (1995).
Attachments	1. BDO Audit (WA) Pty Ltd – Financial Application Control Review

Executive Summary

BDO Audit (WA) Pty Ltd are the City’s appointed Internal Auditors. As part of an agreed Internal Audit plan, BDO Audit (WA) Pty Ltd have conducted a number of internal audits across various business areas within the City. This report seeks to provide the Committee with an update on the findings of the Financial Application Control Review.

Recommendation to the Audit and Risk Committee

The Audit and Risk Committee receives the Financial Application Control Review and notes the finding and recommendation of the Audit and the actions proposed by Administration.

Background

BDO Audit (WA) Pty Ltd are the City’s appointed Internal Auditors and in accordance with the 2017/18 Internal Audit Annual Plan have facilitated a Review of the City’s financial application control processes.

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. The assessment is conducted with input from city personnel and is facilitated by the BDO Audit Team.

The attached report contains details of the issues raised and management’s comments.

The Financial Application Control Review is presented to the Audit and Risk Committee for their information.



CITY OF NEDLANDS
Financial Application Control Review

December 2017

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY	4
1.1 OBJECTIVE	4
1.2 SCOPE	4
1.3 APPROACH	4
1.4 CONCLUSION	4
1.5 SUMMARY OF KEY FINDINGS	5
1.6 ACKNOWLEDGEMENT	5
1.7 ACCEPTANCE OF REPORT	5
2. DETAILED FINDINGS & RECOMMENDATIONS	6
3. KEY ENGAGEMENT DETAILS & TIMINGS	13
4. RISK RATINGS	14
5. INHERENT LIMITATIONS	15
6. RESTRICTION OF USE	15



1. EXECUTIVE SUMMARY

1.1 Objective

In accordance with the 2017/18 Internal Audit Plan, the key objectives of this audit were to assess the design effectiveness and efficiency of controls and processes within the Authority Financial Application to assess compliance with Application policies, procedures, best practices, and regulatory requirements.

1.2 Scope

The scope of this audit were to review the City of Nedlands Authority Financial Application for the period 1 January to 31 October 2017, and included:

- Existing Financial Application control policies, procedures and practices within the city (design effectiveness)
- Compliance with policies, procedures and processes through limited sample testing (operating effectiveness).

1.3 Approach

Our approach included:

- Met with the City to agree the Terms of Reference
- Obtained and reviewed copies of all relevant, authorised policies and procedures
- Conducting interviews and walkthroughs with the Manager of Finance, Accounts Receivable Officer, Accounts Payable Officer, IT Coordinator and System and Network Administrator and documented key processes and controls
- Evaluated the design effectiveness and adequacy of key controls identified
- Performed sample testing where appropriate
- Conducted site visit to City of Nedlands Data Centre in Malaga
- Prepared weekly status report to provide audit status updates
- Prepared and issued our draft for management comments
- Reviewing management comments and issuing final report.

1.4 Conclusion

We identified improvements that can be made by implementing governance processes in various areas of the Financial Application Control, specifically in relation to Application Governance, Contract Management, Security, Disaster recovery and Application controls.

We identified 3 high risk and 2 medium risk findings. Please refer to the section 1.4 for a Summary of Findings and section 2 for Detailed Findings and Recommendations in this report for more details.



We have completed our internal audit of the Financial Application and have summarised assurance provided from our work in relation to the existing control environment, and our specific recommendations in the tables below.

LEVEL OF ASSURANCE - DESIGN EFFECTIVENESS (SEE SECTION 4 FOR DETAILED DEFINITIONS)	LEVEL OF ASSURANCE - OPERATIONAL EFFECTIVENESS (SEE SECTION 4 FOR DETAILED DEFINITIONS)
---	---

Limited

Limited

1.5 Summary of key findings

Our review identified 3 ‘High’ rated findings and 2 ‘Medium’ rated findings. These are summarised in the table below. The detailed findings and recommendation are further explained in Section 2 of this report.

SUMMARY OF RECOMMENDATIONS (SEE SECTIONS 2 FOR DETAILED FINDINGS AND RECOMMENDATIONS)	RISK SIGNIFICANCE (SEE SECTION 4 FOR DEFINITIONS)
1. Improve Application Governance and Management	High ▲
2. Improve Application Contract Management	High ▲
3. Improve Application Security Management	High ▲
4. Improve Disaster Recovery, Back-up and Recovery Processes	Medium ■
5. Improve Application Controls	Medium ■


1.6 Acknowledgement


We thank the staff at the City of Nedlands for their support and assistance to us in executing this review.


1.7 Acceptance of Report


On behalf of:	City of Nedlands	BDO
Signature:		
Name:	Greg Trevaskis	Andrew Hillbeck
Title:	Chief Executive Officer	Partner
Date:	8/2/18	12/8/18


2. DETAILED FINDINGS & RECOMMENDATIONS


1. Improve Application Governance and Management			Risk Rating: High 
Finding	Risk/Impact	Recommendation	Management Comment
<p>There are no relevant and up to date, documented policies and procedures to support the management and Governance of the Authority application that include Information Security, data management, IT asset management, IT risk management and change management within the City.</p>	<ul style="list-style-type: none"> IT assets being ineffectively managed and potential breaches of legal and regulatory requirements Inefficient and ineffective management over IT infrastructure, facilities, hardware, software, and services Security breaches, inappropriate access and unauthorised use of resources IT risks being ineffectively identified, managed, mitigated and reported Change requests are inaccurately analysed, causing adverse effects to the business or technology assets 	<p>We recommend that:</p> <p>Management design and implement an IT governance framework that is aligned to existing City governance structures and relevant IT and management frameworks, standards and best practices, such as Risk, Policy, Security and Change Management. This will ensure standardised processes, greater efficiencies, reduced duplication of effort, and increased formal processes and controls</p>	<p>Management Action:</p> <p>The City is in the process of reviewing 24 draft copies of policies (8 active) and procedures for both Information Technology and Information Management for approval. The drafts will be presented to the Executive team for their review and approval and then will be published as active policies/procedures to comply with the audit report, mitigate any associated risk, security and change management that has been identified by the audit.</p> <p>For the reasons described above the City's management consider this to be deserving of a MEDIUM Risk Rating.</p> <p>Responsible Official:</p> <p>Manager of Corporate Strategy and Systems</p> <p>Implementation Date:</p> <p>June 2018</p>


2. Improve Application Contract Management			Risk Rating: High 
Finding	Risk/Impact	Recommendation	Management Comment
<p>While the City has a written “Software Support Agreement” with Authority, we identified that this agreement is out of date and has not been reviewed and updated since September 1998. Furthermore, the existing agreement does not include any reference to confidentiality and or security requirements.</p> <p>There are currently no policies, procedures or guidelines relating to the monitoring or review processes in place to evaluate and review the service performance of external providers.</p>	<ul style="list-style-type: none"> • Activities being outsourced to a third-party who is unable to perform the activities in accordance with service, legal, and regulatory requirements introducing additional risks to the City • Financial losses, reputational damage and an inability to enforce performance expectations • Financial losses and reputational damage caused by a breach to data confidentiality, integrity or availability. 	<p>We recommend that:</p> <p>Policies and Service Level Agreement’s (SLA) / Contracts should be developed, approved and regularly reviewed to adjust for changes in the City’s business environment and signed by appropriate representatives from all relevant parties responsible for service delivery and monitoring.</p> <p>SLA’s should include:</p> <ul style="list-style-type: none"> • Clearly defined roles and responsibilities, and defined terms for addressing performance issues • Confidentiality and Security agreements • Clearly defined Key Performance Indicators (KPIs), which are monitored and reported against contractual requirements and strategic objectives. • Contract termination procedures and contingency plans to address potential failed vendor performance. 	<p>Management Action:</p> <p>Director Corporate and Strategy has had 2 meetings with Civica prior to the Christmas break and has highlighted a number of business improvements that should form part of a new Service Level Agreement Service Level Agreement for the City. The City is also planning to perform a system health check</p> <p>Director Corporate and Strategy is meeting with Civica again on the 1st of February 2018 at their Melbourne office to progress the process.</p> <p>Further CIVICA’s reference to confidentiality and or security requirements will be provided to the City for Nedlands record. Also, CIVICA’s current general Authority Service Level Agreement will be provided for Nedlands record too.</p> <p>For the reasons described above the City’s management consider this to be deserving of a MEDIUM Risk Rating.</p> <p>Responsible Official:</p>

2. Improve Application Contract Management			Risk Rating: High 
Finding	Risk/Impact	Recommendation	Management Comment
			Manager of Corporate Strategy and Systems Implementation Date: June 2018

3. Improve Application Security Management			Risk Rating: High 
Finding	Risk/Impact	Recommendation	Management Comment
<p>The City has no formal policies or procedures in place to enforce the acceptable use of IT resources or to ensure that only authorised users are granted access based on business needs and job-related functions. We identified that existing user profiles are copied to grant new users access to the application</p> <p>Further to the above, we have identified:</p> <ul style="list-style-type: none"> • 153 users have “Open Database Connections” (ODBC) to the existing authority database. We could not confirm the specific access privileges and or if these connections are encrypted and adequately secured • 7 Users have “Administrative” user access to the application <p>We could not confirm if the user password file is securely protected and encrypted (A request were send Authority to verify - At the time of this audit, we did not receive a response). However, IT should be aware of the safeguards and controls in place to ensure password file security and controls</p>	<ul style="list-style-type: none"> • Unauthorised disclosure, changes and transaction processing • Invalid, incomplete and fraudulent data transfer and processing • Unauthorised access leading to segregation of duties issues and the ability to perform unauthorised or inappropriate activities and transactions • Unprotected ODBC connections increase risk of unauthorised access to data, changes or deletion of database records • Financial losses and reputational damage caused by a breach to data confidentiality, integrity or availability 	<p>We recommend that:</p> <ul style="list-style-type: none"> • Access management and acceptable use policies are implemented • Application access is managed, monitored and reviewed to ensure only authorised individuals are granted access based on business need • ODBC authentication are investigated and reviewed to ensure implementation is required and or configured according to best practice and relevant security requirements to prevent unauthorised and or privilege access to database records • Review administrative user accounts and restrict to an appropriate number of administrators based on business need • Verify and confirm that application password file is appropriately protected and encrypted 	<p>Management Action:</p> <p>Nedlands has requested CIVICA for general Authority policies to confirm the user password file is securely protected and encrypted.</p> <p>Also, Information Technology can confirm that the windows file structure is secure and have put in place system file access permissions to safe guard.</p> <p>Responsible Official:</p> <p>Manager of Corporate Strategy and Systems</p> <p>Implementation Date:</p> <p>June 2018</p>

4. Improve Disaster Recovery, Back-up and Recovery Processes			Risk Ratings: Medium 	
Finding	Risk/Impact	Recommendation	Management Comment	
<p>The City currently have a documented Business Continuity Plan (BCP), which include Incident management procedures. However, the City does not have a clearly defined up to date Disaster Recovery Plan (DRP) or backup policy and procedures in place to ensure recovery of information assets to deliver normal business services</p>	<ul style="list-style-type: none"> • Loss of data and inability to support business operations • Ineffective ability to deliver normal business services, causing financial and reputation damage • Breaches of legal and regulatory requirements • Security breaches, inappropriate access and unauthorised use of resources 	<p>We recommend that:</p> <ul style="list-style-type: none"> • DRP are documented, reviewed, updated, approved, periodically tested, and communicated to stakeholders • Backup and restore procedures are documented and reviewed on a periodic basis • Roles and responsibilities for managing back-up operations are clearly defined and delegated • Backup and restore work orders are scheduled, completed, reviewed and backup integrity is verified 	<p>Management Action:</p> <p>City's Disaster Recovery Plan (DRP) is currently being developed by the Manager of Corporate and Strategy. Further current Information Controls and Technology draft policies include Disaster Recovery, contingency planning, backups, replication, redundancy, data recovery, Emergency response will be approved and published as active.</p> <p>Responsible Official:</p> <p>Manager of Corporate Strategy and Systems</p> <p>Implementation Date:</p> <p>June 2018</p>	

5. Improve Application Controls			Risk Rating: Medium 	
Finding	Risk/Impact	Recommendation	Management Comment	
<p>The Authority system lack functionality to support efficient and effective business transactional processing</p> <p>We have identified that</p> <ul style="list-style-type: none"> No input validation and or data integrity system controls are in place to ensure complete and accurate data input and error correction or reporting User have to manually calculate and input Accounts receivable pricing information Manual checks need to be performed by staff outside the system as the system workflow does not support the current business process 	<ul style="list-style-type: none"> Invalid and incomplete data input and processing Compromised data integrity due to human error Ineffective and inefficient workflows due to manual processing and controls maintained outside of the system 	<p>We recommend that:</p> <ul style="list-style-type: none"> Data verification and input controls be implemented in the system to ensure accuracy and validity of system transaction data input System to be configured to perform automated transactional calculations and reconciliations where appropriate System controls be implemented to minimise manual controls outside of the system 	<p>Management Action:</p> <p>City is in the process of engaging with CIVICA to review the controls that are available within the system. Also, City is restricted by the requirements to implement the “work order” module which would allow Nedlands to implement further online processing in certain modules to reduce the manual input. Proposed “work order” module implementation is scheduled next Financial year. A proposed booking system implementation is scheduled in this Financial Year for further reduction in manual calculation and input of invoices for fees and charges.</p> <p>City’s Finance department will implement manual data verification and input by having oversight by an independent Finance Officer to reduce the invalid and incomplete data input and processing and compromised data integrity.</p>	

5. Improve Application Controls				Risk Rating: Medium 
Finding		Risk/Impact	Recommendation	Management Comment
				Responsible Official: Manager of Corporate Strategy and Systems and Manager of Finance Implementation Date: June 2018



3. KEY ENGAGEMENT DETAILS & TIMINGS

Review Period Covered 1 Jan 2017 to 31 October 2017

BDO Engagement Partner Andrew Hillbeck

Report to be issued to Client Sponsor Greg Trevaskis





Key Events	Expected Date	Actual Date	Comments on Variations
Fieldwork commencement	5 December 2017	5 December 2017	
Fieldwork completion	15 December 2017	15 December 2017	
Closing meeting	21 December 2017	TBC	
Draft report sent	5 January 2018		
Management Comments Received	12 January 2018		
Final report issued	19 January 2018		

Engagement participants




Name	Title
City of Nedlands	
Vanaja Jayaraman	Acting Manager of Finance
Daniel Wong	Accounts Receivable Officer
Qurban Ali	Accounts Payable Officer
Nalin Dias	IT Coordinator
Jonathan Filippone	Systems and Network Administrator
BDO	
Andrew Hillbeck	Partner
Riaan Bronkhorst	Manager
Jessica Chiang	Senior Consultant



4. RISK RATINGS

LEVEL OF ASSURANCE	DESIGN of internal control framework	
	Findings from review	Design Opinion
Substantial 	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.
Moderate 	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.
Limited 	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.
None 	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	No system of internal control.

Risk Significance

High 	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.



5. INHERENT LIMITATIONS


Because of the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected. Further, the internal control structure within which the control procedures that are subject to internal audit operate is not reviewed in its entirety and, therefore, no opinion or view is expressed as to the effectiveness of the greater internal control structure. An internal audit is not designed to detect all weaknesses in control procedures as it is not performed continuously throughout the period and the tests performed on the control procedures are done on a sample basis. Any projection of the evaluation of control procedures to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

We believe that the statements made in this internal audit report are accurate, but no warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, client management and personnel. We have indicated within this internal audit report the sources of the information provided. We have not sought to verify those sources independently unless otherwise noted within the internal audit report. We are under no obligation in any circumstance to update this internal audit report, in either oral or written form, for events occurring after the internal audit report has been issued in final form unless specifically agreed with management.

6. RESTRICTION OF USE

This report is intended solely for the use of management, the City of Nedlands Council, the external auditors, regulatory agencies or the City's legal counsel and cannot be used by, circulated, quoted, disclosed, or distributed to third parties without BDO's prior written consent.

7.4 Regulation 17

Owner	City of Nedlands
Officer	Mike Fletcher – Manager Corporate Strategy & Systems
Director	Lorraine Driscoll – Director Corporate & Strategy
Director Signature	
Disclosure of Interest	No officer involved in the preparation of this report had any interest which required it to be declared in accordance with the provisions of the Local Government Act (1995).
Attachments	No attachments to this report

Executive Summary

This report is being presented to the Audit & Risk Committee to provide an update of the requirement under Regulation 17 of the Local Government (Audit) Regulation 1996 for the CEO to review the effectiveness of systems and procedures.

The City’s Information Technology department has been carrying out updates and upgrades of its many systems following an extensive review recently conducted by Edith Cowan University Cyber Institute (previously reported to this Committee on 10 August 2017). The City is working with suppliers to upgrade or patch systems where issues of vulnerability have been identified, a number of which have already been completed.

We are now reviewing the potential of a secondary data centre for storage of the City’s backups, the chosen data centre will require the capacity and security to enable the City to go to full production in the event of a catastrophic shutdown of the primary service operating in Malaga. Once the secondary site has been identified we can complete our IT Disaster Recovery Plan.

Previous audits have identified the need to review and update and or create new Policies with associated procedures that cover both Information Technology and Information Management requirements moving forward.

The City has recently submitted its Recordkeeping plan RKP 2018 to the State Records Office for review, RKP 2018 reflects the ongoing changes that have been made to Information Management at the City in the past few years, a review and update to the State Records Office will be provided in the latter part of 2018 as part of the ongoing work being conducted at the City.

We are developing a Digital Strategy, the intention of this strategy is to describe a vision for the City in how it will conduct its business in the future, and to document the complex systems used in daily operations, and to identify the relationships and age and life cycle of these systems. The Digital Strategy will provide us with a Roadmap to assist in prioritizing, budgeting and manage the purchase of hardware and software systems in the future.

Recommendation to the Audit and Risk Committee

Council

- 1. That the City receives this update of the progress of Risk management, Internal Controls and Legislative compliance as required under Regulation 17 of the Local Government Act**

Discussion/Overview

CEO to review certain systems and procedures (Regulation 17)

Under regulation 17 of the Local Government (Audit) Regulation 1996 the CEO is to:

- (1) The CEO is to review the appropriateness and effectiveness of a local government's systems and procedures in relation to –
 - (a) Risk management; and
 - (b) Internal controls; and
 - (c) Legislative compliance.
- (2) The review may relate to any or all of the matters referred to in sub regulation (1)(a), (b) and (c), but each of those matters is to be the subject of review at least once every 2 calendar years.
- (3) The CEO is to report to the audit committee the results of that review.

(a) Risk Management - Cyber Controls

In 2017 the City engaged Edith Cowan University Security Research Institute to help identify weaknesses in the City's network and communications architecture. A previous audit review had identified a requirement to conduct a penetration test on the IT systems as part of the ongoing audit process.

Through Professor Craig Valli a strategy was developed. Dr. Ahmed Ibrahim was assigned to the City for a six-month period to assist the IT team in identifying vulnerabilities, tools that were required and an assessment of identified items. All of the identified findings in the report have been addressed, the City's IT team are continually monitoring systems and updating as necessary.

(a) Risk management - IT Disaster Recovery Plan

During the past four years extensive work has been carried out upgrading the City's hardware, operating systems, network design and structure, cyber security, telecommunications and hosting of core infrastructure. Each of Council's sites are connected directly to a Secure Data Centre at Malaga, the City's equipment is modern although 4 years old now and the operating systems are patched and up to date, backups are conducted nightly, weekly

and monthly and restored as required. Backups are also restored monthly under a test environment to validate continuity.

Backups are kept on site at Malaga and for convenience, copies are also kept at the Council Depot, these backups can be restored to older servers that are retained in the event of a disaster occurring at the Data Centre.

In the event of the Primary data centre becoming unavailable for a period the secondary data centre will require a fixed datalink and the capacity to go to full production using the associated backup. We are in the process of identifying a secondary data centre, once established we will complete, test and validate the IT Disaster Recovery Plan, this work should be completed by the later part of 2018. We are actively seeking prices to move our off-site backups from the Depot to a secondary data centre

(b) Internal controls - Policies and Procedures

The City has many policies and procedures relating to Information Technology and Information Management and has made significant alterations to its business processes and practices during the past few years. External audits, ECU Cyber audit and the Record Keeping Plan RKP 2018 have identified the need for further development and documentation, we are currently conducting a review of all related policies and procedures and amending as required to reflect current best practice.

(b) Internal controls - Digital Strategy

We are developing a Digital Strategy, the intention of this strategy is to describe a vision for the City in the way that it will conduct its business in the future.

The outcome of this Digital Strategy will be a Roadmap identifying and prioritising business improvements and initiatives to enable Council to better develop robust systems and processes to deliver upon its Strategic Plan.

We are currently focused on business improvements to our core financial system "Authority" although the product is capable of managing financial transactions there is significant room for improvement for example integration to other products such as SharePoint; a core system used within council for information management and automated workflows. Current reporting capability within the system is basic and requires specific application expertise to develop. A number of business improvement initiatives have been implemented recently including automated workflows of 'Building' and 'Planning' lodgements, additionally a new feature 'stop the clock' allows us to automate and manage the application process more efficiently. We are currently working on a suite of business improvements in our finance processes, which will result in significant efficiencies in how we go about our business.

The Director Corporate & Strategy; Lorraine Driscoll has been meeting with key representatives of Civica (the company that provides and supports our finance systems) to establish a partnership style relationship – which is critical in the development of our Digital Strategy and Roadmap.

As part of the review of our core systems we will review and benchmark other Local Government products such as TechnologyOne and Datacom who provide modern, contemporary solutions.

c) Legislative Compliance - Record Keeping Plan

The City has just completed a comprehensive review and documentation of its Information Management system, processes, Policies and procedures as part of the development of a new Recordkeeping Plan RKP 2018.

As defined in the *Interpretation Act 1984 (WA)*, that must be complied with by all State organisations subject to the *State Records Act 2000*.

At the end of December 2017, the City has submitted its Record Keeping Plan RKP 2018 to the State Records Office for review, the plan reflects the significant changes that have taken place during the past few of years i.e. centralising all of the City's records using Microsoft SharePoint., The next step is for the City to continue to review the policies, procedures and appendices to the plan and reflect any changes that are made to the system and documentation and to submit a revised document late 2018.

Key Relevant Previous Council Decisions:

I am not aware of any previous decision/s made by Council that are relevant to this issue.

Consultation

No Community consultation has been required.

Budget/Financial Implications

A budget will be required in the 2018/19 budget for the implementation of a secondary Datacenter, this information is being gathered at present in preparation of a new budget. Other items that may be identified in the Digital Strategy will be clearly identified and articulated with associated costs and time lines for budgetary purposes.

8 Confidential Items

Nil.

9 Date of next meeting

The date of the next meeting of this Committee is to be advised.

Declaration of Closure

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