



# Five Parks Bournemouth i.e. Kings, Queens, Meyrick and Redhill Parks and Seafield Gardens

---

Year ended 31 March 2021

January 2022



# Contents



## Your key Grant Thornton team members are:

Gareth Norris

Director

T: 01908 359 568

E: [gareth.m.norris@uk.gt.com](mailto:gareth.m.norris@uk.gt.com)

Sam Harding

Senior Manager

T: 0117 305 7874

E: [sam.g.harding@uk.gt.com](mailto:sam.g.harding@uk.gt.com)

## Section

1. Headlines
2. Financial statements
3. Independence and ethics

## Page

- 3
- 4
- 7

## Appendices

- A. Follow up of prior year recommendations
- B. Action Plan
- C. Audit adjustments
- D. Fees
- E. IT Deficiencies

- 8
- 9
- 10
- 12
- 13

The contents of this report relate only to those matters which came to our attention during the conduct of our normal audit procedures which are designed for the purpose of expressing our opinion on the financial statements. Our audit is not designed to test all internal controls or identify all areas of control weakness. However, where, as part of our testing, we identify control weaknesses, we will report these to you. In consequence, our work cannot be relied upon to disclose all defalcations or other irregularities, or to include all possible improvements in internal control that a more extensive special examination might identify. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Grant Thornton UK LLP is a limited liability partnership registered in England and Wales: No.OC307742. Registered office: 30 Finsbury Square, London, EC2A 1AG. A list of members is available from our registered office. Grant Thornton UK LLP is authorised and regulated by the Financial Conduct Authority. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

# Headlines

This table summarises the key issues arising from the statutory audit of The Lower Central Gardens ('the Charity') and the preparation of the Charity's financial statements for the year ended 31 March 2021 for those charged with governance.

<b>Financial Statements</b>	<p>Under International Standards of Audit (ISAs (UK)), we are required to report whether, in our opinion:</p> <ul style="list-style-type: none"> <li>the Charity's financial statements give a true and fair view of the financial position of the Charity and its expenditure and income for the year.</li> </ul> <p>We are also required to report whether the information given in the Report of the Trustee is materially inconsistent with the financial statements or our knowledge obtained in the audit or otherwise appears to be materially misstated.</p>	<p>Our audit work was completed remotely during November 2021 to January 2022 due to the lock down restrictions resulting from the Covid 19 pandemic. Our findings are summarised on pages 4 to 6. We have identified 3 adjustments to date to the financial statements; these have not resulted in an adjustment to the Charity's net movement on funds. Audit adjustments are detailed in Appendix C. Our follow up of recommendations from the prior year's audit is detailed in Appendix A and current year recommendations in Appendix B. The audit of the parent entity Bournemouth, Christchurch and Poole Council identified a number of control deficiencies in the Council's IT system which is used by the Charity. These are reported at Appendix E.</p> <p>Our work is substantially complete and there are no matters of which we are aware that would require modification of our audit opinion or material changes to the financial statements, subject to the following outstanding matters;</p> <ul style="list-style-type: none"> <li>- outstanding queries relating to the valuation of fixed assets;</li> <li>- receipt of management representation letter;</li> <li>- engagement leader final review;</li> <li>- receipt of comfort letter confirming support from the Council; and</li> <li>- review of the final set of financial statements.</li> </ul> <p>We have concluded that the other information to be published with the financial statements, which includes the Report of the Trustee, is consistent with our knowledge of the organisation and the financial statements we have audited.</p> <p>Our anticipated audit report opinion will be unmodified.</p>
-----------------------------	--	---

## Acknowledgements

We would like to take this opportunity to record our appreciation for the assistance provided by the finance team and other staff during our audit, particularly reflecting on the impact of Covid-19 on working arrangements.

# Summary

## Overview of the scope of our audit

This Audit Findings Report presents the observations arising from the audit that are significant to the responsibility of those charged with governance to oversee the financial reporting process, as required by International Standard on Auditing (UK) 260. Its contents have been discussed with management.

As auditor we are responsible for performing the audit, in accordance with International Standards on Auditing (UK) and the Code, which is directed towards forming and expressing an opinion on the financial statements that have been prepared by management with the oversight of those charged with governance. The audit of the financial statements does not relieve management or those charged with governance of their responsibilities for the preparation of the financial statements.

## Audit approach

Our audit approach was based on a thorough understanding of the Charity's business and is risk based, and in particular included:

- An evaluation of the Charity's internal controls environment, including its IT systems and controls;

- Substantive testing of significant transactions and material account balances

We have not had to alter or change our audit plan, as communicated to you.

## Conclusion

We have substantially completed our audit of your financial statements and subject to outstanding queries being resolved, we anticipate that our audit opinion will be unmodified. These outstanding items are set out on page 3.

## Our approach to materiality

The concept of materiality is fundamental to the preparation of the financial statements and the audit process and applies not only to the monetary misstatements but also to disclosure requirements and adherence to acceptable accounting practice and applicable law.

	Amount (£)	Qualitative factors considered
Materiality for the financial statements	228,380	<ul style="list-style-type: none"> <li>• 2% of gross assets</li> </ul>
Performance materiality	171,290	<ul style="list-style-type: none"> <li>• 75% of headline materiality</li> </ul>
Trivial matters	11,400	<ul style="list-style-type: none"> <li>• 5% of headline materiality</li> </ul>
Specific materiality for income	24,260	<ul style="list-style-type: none"> <li>• 3% of income</li> </ul>
Specific materiality for expenditure	32,200	<ul style="list-style-type: none"> <li>• 3% of expenditure</li> </ul>

# Significant risks

Risks identified in our Audit Plan	Commentary
<p><b>1 Occurrence of voluntary income</b></p> <p>Under ISA (UK) 240 there is a rebuttable presumed risk that revenue may be misstated due to the improper recognition of revenue.</p> <p>We have rebutted this presumed risk for donations and support received from the Council, as the amount received will be confirmed by the Parent Council.</p> <p>We have not deemed it appropriate to rebut this presumed risk for all other material streams of the Charity, comprising income derived from charitable activities, given the greater judgement involved in recognising the related transactions in the financial statements.</p> <p>We have therefore identified the occurrence of these income sources as a significant risk, which was one of the most significant assessed risks of material misstatement.</p>	<p><b>Auditor commentary</b></p> <p>We:</p> <ul style="list-style-type: none"> <li>documented and gained an understanding of controls around monitoring and receipt of cash and the recording in the general ledger</li> <li>obtained the breakdown of income for the period and agreed to supporting records</li> <li>tested a sample of in-year income to supporting records</li> </ul> <p>Our testing has not identified issues in respect of income.</p>
<p><b>2 Management over-ride of controls</b></p> <p>Under ISA (UK) 240 there is a non-rebuttable presumed risk that the risk of management over-ride of controls is present in all entities.</p> <p>We therefore identified management override of control, in particular journals, management estimates and transactions outside the normal course of business as a significant risk, which was one of the most significant assessed risks of material misstatement.</p>	<p><b>Auditor commentary</b></p> <p>We:</p> <ul style="list-style-type: none"> <li>evaluated the design effectiveness of management controls over journals</li> <li>analysed the journals listing and determined the criteria for selecting high risk unusual journals</li> <li>tested unusual journals made during the year and the accounts production stage for appropriateness and corroboration to supporting documents</li> <li>gained an understanding of the accounting estimates and critical judgements applied by management and considered their reasonableness</li> </ul> <p>Our audit of the Council's IT system which is used by the Charity identified a number of deficiencies attached at Appendix E. Our testing of journals included procedures to address the impact of these findings. Our testing has not identified any further issues in respect of management override of controls.</p>

# Other communication requirements

We set out below details of other matters which we, as auditors, are required by auditing standards to communicate to those charged with governance.

	Issue	Commentary
1	<b>Matters in relation to fraud</b>	We have not been made aware of any incidents of fraud in the period and no issues have been identified during the course of our audit procedures.
2	<b>Matters in relation to related parties</b>	We are not aware of any related parties or related party transactions which have not been disclosed.
3	<b>Matters in relation to laws and regulations</b>	You have not made us aware of any significant incidences of non-compliance with relevant laws and regulations and we have not identified any incidences from our audit work.
4	<b>Written representations</b>	A letter of representation has been requested from the Charity.
5	<b>Accounting practices</b>	<p>We have evaluated the appropriateness of the Charity's accounting policies, accounting estimates and financial statement disclosures. Our review found no material omissions in the financial statements.</p> <p>The Accounting policies have been amended to reference the impact of the Covid-19 pandemic on the Charity's activities.</p>
6	<b>Audit evidence and explanations/significant difficulties</b>	All information and explanations requested from management was provided.

# Independence and ethics

We confirm that there are no significant facts or matters that impact on our independence as auditors that we are required or wish to draw to your attention. We have complied with the Financial Reporting Council's Ethical Standard and confirm that we, as a firm, and each covered person, are independent and are able to express an objective opinion on the financial statements

We confirm that we have implemented policies and procedures to meet the requirements of the Financial Reporting Council's Ethical Standard and we as a firm, and each covered person, confirm that we are independent and are able to express an objective opinion on the financial statements.

Details of fees charged are detailed in Appendix D.

## **Audit and Non-audit services**

For the purposes of our audit we have made enquiries of all Grant Thornton UK LLP teams providing services to the Charity. No non-audit services were identified.


## Follow up of prior year recommendations

We identified the following issues in the audit of the Charity's 2018/19 financial statements, which resulted in four recommendations being reported in our 2018/19 Audit Findings report. Two of the previously communicated issues remain unaddressed.




	Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
1	X	<p>A separate ledger should be set up for the Trust to make sure there is a clear distinction in the recording of the relevant transactions</p> <p>Alternatively a service level agreement, or similar, could be established between the Council and the Trust to recognise the income and expenditure transactions between the two bodies.</p> <p>Consideration should be given to the recording of events managed by the Council using land owned by the Trust and whether they should be recognised in the Council's accounts with consideration paid to the Trust for use of the site.</p>	<p>No action taken on the recommendation. However, a separate cost centre already exists for the Lower Gardens Trust, which is excluded from the Council Financial Accounts. Currently year end transfers are made out of the Council's range of cost centres to this specific code</p> <p><b>Management response</b></p> <p>The Director of Law and Governance / Monitoring Officer is undertaking a thorough review in early 2022 of all of the Council charities, where necessary seeking legal advice, which will cover within its remit the issues of governance. Until this review is concluded actions to resolve the points made will be suspended. The pandemic has caused delays in actioning the findings from the internal audit report as the Council's response to the pandemic took top priority.</p>
2	X	<p>Internal Audit carried out a review of governance arrangements at the Charity, issuing their report in September 2019. Their report identified a number of issues concerning governance arrangements at the Charity.</p> <p>The target dates for completion of the recommendations made by Internal Audit were December 2019 and January 2020</p> <p>Management should ensure that consideration is given and action taken to address the issues identified from the review. At the time of the 2018/19 report, a number of recommendations remained outstanding and are therefore overdue.</p>	<p>This review remains ongoing at the Council.</p> <p><b>Management response</b></p> <p>The Director of Law and Governance / Monitoring Officer is undertaking a thorough review in early 2022 of all of the Council charities, where necessary seeking legal advice, which will cover within its remit the issues of governance. Until this review is concluded actions to resolve the points made will be suspended. The pandemic has caused delays in actioning the findings from the internal audit report as the Council's response to the pandemic took top priority.</p>

# Action plan

We have identified 1 recommendation for the Charity as a result of issues identified during the course of our audit. We have agreed our recommendations with management. The matters reported here are limited to those deficiencies that we have identified during the course of our audit and that we have concluded are of sufficient importance to merit being reported to you in accordance with auditing standards.

	Assessment	Issue and risk	Recommendations
1		<p><b>Fixed assets useful life</b></p> <p>Our testing identified that a number of the Charity's building assets had low useful remaining lives, that may not appropriately reflect the expected life of the asset.</p> <p>We acknowledge, however that any impact on depreciation charged would be trivial.</p>	<p>The Charity should review the remaining useful lives of its assets to ensure they accurately reflect the period of continued use.</p> <p><b>Management response</b></p> <p>The remaining useful lives of its assets will be reviewed to ensure they accurately reflect the period of continued use.</p>

## Controls

-  High – Significant effect on control system
-  Medium – Effect on control system
-  Low – Best practice

## Appendix C

# Audit Adjustments

We are required to report all non trivial misstatements to those charged with governance, whether or not the accounts have been adjusted by management.

## Impact of adjusted misstatements

All adjusted misstatements are set out in detail below along with the impact on the key statements and the reported net movement in funds for the year ending 31 March 2021.

Detail	Statement of Financial Activities £	Balance Sheet £	Impact on total net movement in funds £
<b>Net movement in funds</b>			<b>(£ 264,488)</b>
<b>1 Staff Recharges</b>	527	No impact	527
Our testing identified that an error had been made in the salary recharge from the Council to the Charity. This was £525. Although trivial management has made the adjustment.			
This is matched by increase in the donation from the Council.	(527)		(527)
<b>2 Tangible fixed assets</b>			
Testing identified that the full value of Meyrick Park Golf Club was included in the Charity's accounts, although only 74% of the asset resides in the Charity's land and only 74% of the income relating to this asset has been recognised. This error relates to the current and prior year financial statements. The opening value of this asset has been reduced by £650,000 and depreciation by £13,000.	13,000		13,000
A further error was identified as the valuer had used an incorrect floor area for the Kings Park athletics stadium. This error related to 2020/21 only. This has resulted in an increase in the value of this asset of £919,428.		339,915	(339,915)
Increase in tangible Fixed Assets		(339,915)	339,915
Increase in restricted income fund			
<b>Net movement in funds</b>			<b>(£ 251,488)</b>

# Audit Adjustments

We are required to report all non trivial misstatements to those charged with governance, whether or not the accounts have been adjusted by management.

**Impact of unadjusted misstatements**  
There are no unadjusted misstatements.

**Misclassification and disclosure changes**  
The table below provides details of misclassification and disclosure changes identified during the audit which have been made in the final set of financial statements.

Disclosure omission	Auditor recommendations	Adjusted?
A small number of minor typographical and disclosure changes were made to the financial statements.	<ul style="list-style-type: none"><li>These were amended by management.</li></ul>	✓


# Fees

We confirm below our final fees charged for the audit.




## Audit Fees

	Proposed fee	Final fee
Charity Audit	10,000	10,000
Total audit fees (excluding VAT)	£10,000	£10,000


# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
1. 	<p><b>Segregation of duty (SoD) threats due to Oracle Fusion administrators being assigned elevated finance roles.</b></p> <p>The IT Security Manager role enables the user to create, edit and delete users, edit responsibilities, manage application configurations and security settings.</p> <p>Our audit identified 10 users from the Financial Management Systems (FMS) team, 1 user from the Procurement team (ADMIN_HARWOODKAT), 1 user from the IT team and 5 active generic IDs as having been assigned the 'IT Security Manager role', and a combination of, but not limited to, the following critical access finance roles in Oracle:</p> <ul style="list-style-type: none"> <li>Accounts Payable Manager.</li> <li>Accounts Receivable Manager.</li> <li>Cash Manager.</li> <li>Procurement Manager.</li> </ul> <p>It was also identified that four users from the FMS team (BCP_GREENJ, BCP_ADAMSLA, BBC_MASONJO and BBC_COTTRELLS) have been assigned the IT Security Manager role on both their end user and administrator accounts.</p> <p><b>Risk</b> Assigning excessive privileged access roles increases the risk that system-enforced internal control mechanisms could be bypassed resulting in users being able to:</p> <ul style="list-style-type: none"> <li>Make unauthorised changes to system configuration parameters.</li> <li>Create unauthorised accounts.</li> <li>Make unauthorised updates to user account privileges.</li> </ul>	<p>It is recommended that management:</p> <ul style="list-style-type: none"> <li>Perform a review of all users and their access rights in Oracle Fusion and confirm if these align with their designated roles and responsibilities.</li> <li>Revoke the access to the IT Security Manager role for the procurement user immediately.</li> <li>Ensure that users with elevated privileges only have one account with administrator privileges assigned to them. The access to the IT Security Manager role on the day-to-day accounts for the users identified should be revoked immediately.</li> <li>Evaluate the need to assign finance roles to the system administrators and if no longer required they should be revoked.</li> <li>Always assign access to any application on the principle of least privilege.</li> </ul> <p><b>Management response</b></p> <p>These roles are assigned within the FMS Team to enable carry out business admin functions and development/testing. Interfacing external systems with Fusion is an end user function of the FMS Team.</p> <p>Controls are in place to ensure that these roles are used appropriately. For example, end user functions are documented and records of the processing by the FMS Team are kept.</p> <p>The purpose of why each role is assigned to each user will be documented and kept under review as will the effectiveness of the controls in place.</p> <p>We will review all users access rights and act upon the finding in this reports including reducing the privileges of users where necessary. As an example, we have already revoked access by ADMIN_HARWOODKAT to the IT Security.</p> <p>The FMS Team does require the finance (AP and AR) roles as they carry out end user functions, but this will also be reassessed.</p>




## Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
2. 	<p><b>SoD threats due to Oracle system administrator accounts with developer / implementation roles.</b></p> <p>Our audit identified 15 active accounts belonging to system administrators with the IT Security Manager role had been assigned combinations of the following roles:</p> <ul style="list-style-type: none"> <li>• Application Developer</li> <li>• Application Implementation Manager;</li> <li>• Application Implementation Consultant; and</li> <li>• Application Implementation Administrator.</li> </ul> <p>'Application Implementation Consultant' is one of the roles assigned when Oracle Fusion is first implemented, allowing the application to be configured as required.</p> <p>Each of the Application Implementation roles allows the user assigned with this role to make changes to the Oracle Fusion system configuration with differing levels of access.</p> <p><b>Risk</b></p> <p>The combination of access to implement changes and security administration in production is a SoD conflict that could lead to inappropriate or unauthorised changes to data and functionality within Oracle Fusion. This risk is further elevated owing to a lack of proactive monitoring of privileged user accounts.</p>	<p>It is recommended that management restrict access to implementation roles on a need-to-use basis. Permissions should be assigned for a pre-agreed window to implement a change and then revoked again. Activity during the implementation window should be monitored closely.</p> <p>It is also recommended that management enforce segregation of duties between personnel responsible for developing and implementing changes.</p> <p><b>Management response</b></p> <p>The FMS Team is responsible for both the admin and the limited development of the Oracle System. As identified, development capability is extremely limited and is focused on configuration.</p> <p>The current modules in use (i.e. not full Payroll / HR) requires constant configuration/development access to maintain workflows for Procurement/Account Payables.</p> <p>On the topic of Control for example, any changes to approval rules are not initiated by the FMS Team. They required authorization which is documented from the Service Director or Service Accountant.</p> <p>FMS team require access to Workflow engine to enable the need to change rules based on changing business need</p>




## Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
3. 	<p><b>SoD threats due to business users performing system administrator duties in Civica.</b></p> <p>Administrative access to Civica has been granted to two users (Service Development Manager and Revenue Benefits Manager), both of whom have financial responsibilities in the Revenues and Benefits teams.</p> <p>The combination of financial responsibilities with the ability to create, amend and delete users and administer batch scheduling is considered a segregation of duties conflict.</p> <p><b>Risk</b></p> <p>Assigning excessive privileged access roles increases the risk that system-enforced internal control mechanisms could be bypassed resulting in users being able to:</p> <ul style="list-style-type: none"> <li>• Make unauthorised changes to system configuration parameters.</li> <li>• Create unauthorised accounts.</li> <li>• Make unauthorised updates to user account privileges.</li> </ul>	<p>It is recommended that Management:</p> <ul style="list-style-type: none"> <li>• Review the need for the two individuals identified to have privileged access to Civica.</li> <li>• Grant access to Civica on the principle of least privilege, ensuring access is commensurate with job roles and responsibilities.</li> </ul> <p>If it is unavoidable to grant privileged roles to business users due to organisational size constraints, management should ensure that use of these roles are proactively monitored by reviewing system reports of detailed transactions; selecting transactions from these reports and comparing these to supporting documents; reviewing reconciliations of balances or performing them independently.</p> <p><b>Management response</b></p> <p>Civica OpenRevenues - As part of the annual review of access it was deemed that for Business Continuity that additional users need to have access and the user assigned should have a good understanding of the system, this was limited to Senior Managers. Julie is currently seconded to cover Benefit Manager role in additional Service Development, where the admin permissions would be required to develop the system. A FULL Group security profile rebuild 2021 is in progress, it will be explored on whether other admin profiles should remain for the other users.</p>




## Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
<p>4. </p>	<p><b>Excessive access to interface files by IT and Finance users.</b></p> <p>An excessive number of users have the ability to access the shared folder which contains the information held pertaining to the ASM interface between Oracle Fusion and the feeder systems across the Council.</p> <p>Access to the 'inbox' folder where source feeder files are deposited is not secured appropriately. A significant number of user groups have access to this folder with full control to read and write files. This also includes any administrators on the Bournemouth domain.</p> <p>Included in the list of users who have access to the 'inbox' file are two direct links to the Christchurch and Poole domains. As a result of this, there is no governance over the users who are accessing this folder as they do not appear in the Bournemouth domain on which the Fusion interface is hosted.</p> <p>It was further noted that any users with administrator access in Active Directory have access to manipulate the SQL scripts used to convert the data in the interface process.</p> <p><b>Risk</b></p> <p>There is a risk that users with excessive access privileges in the shared folder could manipulate the interface files that are then processed and loaded in to Oracle.</p> <p>Furthermore, there is a risk that unauthorised changes are made to the SQL scripts that support the interfaces as a result of the access for all Active Directory administrators.</p> <p>This may then adversely impact on the integrity or completeness and accuracy of data within the system.</p>	<p>It is recommended that management restrict the access to the shared folders used in the ASM interface process to named, authorised users only.</p> <p>Access should be restricted based on the types of files a user is responsible for depositing in the folder, such as restricting access to the Civica files to members of the Bournemouth Revenues team.</p> <p>It is also recommended that management automate the process of extracting data from feeder systems where possible. This will reduce the number of users needing access to shared folders where data is being held for processing.</p> <p><b>Management response</b></p> <p>We will annually review the users that have access to the interface folders and ensure the access is still required. We continue to automate the interfacing with the ERP as much as possible.</p> <p>Civica OpenRevenues - Folder security within network share has been restricted against R&amp;B Staff depending on roles, however I will let ICT comment on access permissions they have assigned in addition</p>

## Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
5. 	<p><b>Suspended users with critical access privileges assigned.</b></p> <p>Our audit identified 123 suspended accounts (accounts which can be brought back in to use by users with the IT Security Manager role assigned) that had been assigned roles with critical access assigned, which included but were not limited to the following:</p> <ul style="list-style-type: none"> <li>• Application Developer</li> <li>• Application Implementation Roles</li> <li>• IT Security Manager</li> <li>• AP Manager;</li> <li>• Cash Manager;</li> <li>• AR Manager;</li> <li>• Procurement Manager; and</li> <li>• Supplier Manager;</li> </ul> <p>The Council only suspends no longer needed user accounts and does not fully deactivate them. Suspension of accounts can be reversed by users who have been assigned the IT Security Manager role.</p> <p><b>Risk</b></p> <p>There is a risk that highly privileged suspended accounts could be enabled and used to fraudulently or erroneously manipulate financial data without detection. This risk is further elevated by the lack of audit logging within Oracle Fusion, thus making it difficult to assign accountability to the user responsible.</p>	<p>It is recommended that management:</p> <ul style="list-style-type: none"> <li>• Remove all roles for suspended accounts.</li> <li>• Enable audit logging and proactively monitor user activity for users with elevated permissions.</li> <li>• Deactivate rather than suspend accounts. Deactivating accounts for terminated users removes the Oracle license associated with that account.</li> </ul> <p>It should also be noted that accounts for terminated users which are suspended still count as active licenses for Oracle Fusion.</p> <p><b>Management response</b></p> <p>The policy about accounts of leaver is now to double lock the accounts – inactivated and locked – i.e. can not be reactivated by anyone outside of the FMS Team. We will remove all roles from suspended accounts. We do not use the HR modules that would allow for termination of workers</p>




## Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
6. 	<p><b>Inappropriate critical security and configuration functions embedded in standard roles.</b></p> <p>Our audit identified six active users that have access to a privilege 'impersonate roles' through the 'Application Implementation Manager', 'Application Developer' and 'Sales Administrator' roles that allow them to log on to the application and conduct activities in another users name without leaving an audit trail relating to their own User Identifier (ID). Five of these users have also been assigned the IT Security Manager role.</p> <p>It was also noted that detailed audit logging has not been enabled in Oracle Fusion, and is therefore not proactively reviewed.</p> <p><b>Risk</b></p> <p>There is a risk that highly privileged accounts could be enabled and used to fraudulently or erroneously manipulate financial data without detection. This risk is further elevated by the lack of audit logging within Oracle Fusion, thus making it difficult to assign accountability to the user responsible.</p>	<p>It is recommended that management:</p> <ul style="list-style-type: none"> <li>Remove all 'Impersonate User' privileges from the application, or at a minimum be de-linked from the roles identified.</li> <li>Enable audit logging and proactively monitor user activity for users with elevated permissions.</li> </ul> <p><b>Management response</b></p> <p>The impersonate user privileges requires both the impersonator and the impersonate to both setup this function – we have done limited testing to see if this was something that would be useful to roll out for covering user duty for periods of leave. We did not find that it would be useful.</p>

## Assessment



-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

# IT general controls assessment findings




Assessment	Issue and risk	Recommendations
7.	<div><div><div></div></div><div><p><b>End-users with critical access privileges assigned.</b></p><p>‘Critical access privileges’ are elevated IT functions which can be used to execute and approve financial transactions and manage configurations for the modules to which they are assigned.</p><p>Our audit identified 454 end users that have been assigned one or more roles that have critical access privileges attached to them, some of these roles include:</p><ul style="list-style-type: none"><li>• AP Supervisor.</li><li>• AP Manager.</li><li>• AR Manager.</li><li>• Procurement Manager.</li><li>• Supplier Manager.</li></ul><p>Three out of these 128 users were also identified as having AP Manager, AR Manager and Cash Manager roles assigned simultaneously.</p><p>The high risk objects attached to these accounts include, but not limited to, combinations of the following:</p><ul style="list-style-type: none"><li>- Manage All Application Profile Values</li><li>- Setup and Maintain Applications</li><li>- Assign Business Unit Business Function</li></ul><p>The functions currently assigned are the default functions assigned when Oracle Fusion is implemented. A full list of roles and the functions attached to them can be provided to management on request.</p></div></div>	<p>It is recommended that management:</p> <ul style="list-style-type: none"><li>• Undertake a full review of all users who have been assigned critical access privileges and revoke critical privileges for those users where they no longer align with the user’s roles and responsibilities.</li><li>• Ensure roles that allow system configurations to be altered are restricted on a need-to-use basis and are not assigned to users in the normal course of business.</li><li>• Review the default privileges that are attached to end user roles and consider whether they remain appropriate for the Council.</li></ul> <p><b>Management response</b></p> <p>There are system controls like double authorization of payment / BACS files in addition to system enforced controls that mitigate against these risks however the points will be assessed and actioned on where possible.</p>

*Continued on next page*


# IT general controls assessment findings

	Assessment	Issue and risk	Recommendations
7.		<p><i>Continued from previous page</i></p> <p><b>Risk</b></p> <p>Bypass of system-enforced internal control mechanisms through inappropriate use of critical access rights increases the risk of financial misstatement through fraud or error, as a result of users making unauthorised changes to transactions and system configuration parameters.</p>	
8.		<p><b>Lack of event logs in Oracle Fusion and Civica and lack of proactive review of event logs in Capita.</b></p> <p>It was identified that Oracle Fusion and Civica are not currently configured to generate security event logs, other than for supplier monitoring in Oracle Fusion.</p> <p>It was also identified that whilst Capita generates event logs capturing amongst other things, user activities, these are not proactively reviewed.</p> <p><b>Risk</b></p> <p>Not enabling or reviewing event logs increases the risk of not detecting and resolving inappropriate or unauthorised user activity in a timely manner. This could lead to incomplete and / or inaccurate processing of financial information.</p>	<p>It is recommended that management:</p> <ul style="list-style-type: none"> <li>Implement a process whereby event logs are periodically reviewed for Capita. These reviews should be performed by one or more knowledgeable individuals who are independent of the day-to-day use or administration of these applications.</li> <li>Retain evidence of event logs being reviewed to help ensure they are undertaken in a consistently robust and effective manner.</li> <li>Enable event logs in Oracle Fusion and Civica for specific high-risk users and activities, such as system administration and development activities.</li> </ul> <p><b>Management response</b></p> <p>In Oracle Fusion we have automated reports that log all newly approved orders, new supplier setups, supplier amendments. There are system logs for suppliers.</p> <p>Civica OpenRevenues - There are daily reports to identify account updates across CT/HB and SD. This is used to monitor staff performance and to enable sample checking of updated records by Team Leader. A process to review system access to the Database will be implemented on a monthly basis to review connections made and will be reviewed by System Admin.</p>




## Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach


# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
9. 	<p><b>Leavers' access to Oracle Fusion not disabled in a timely manner.</b></p> <p>For two sampled users it was identified that their access to Oracle Fusion was not disabled for two months following their termination date.</p> <p><b>Risk</b></p> <p>Where system access for leavers is not disabled in a timely manner, there is a risk that former employees will continue to have access and can process erroneous or unauthorised access transactions.</p> <p>There is also a risk that these accounts may be misused by valid system users to circumvent internal controls.</p>	<p>Management should ensure that leavers' access to Oracle Fusion is revoked no more than 24 hours after their termination date.</p> <p>For the process to be effective, the FMS team must be provided with timely notifications from HR and/ or line managers. HR and line managers should be reminded of their responsibilities to make the FMS team aware of leavers in advance of their termination date.</p> <p><b>Management response</b></p> <p>We do receive regular from HR about leavers in advance of their leaving dates however we look to promote a process where the FS team are informed as leavers as soon as possible.</p>


## Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach




# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
<p>10. </p>	<p><b>Governance over the use of shared generic administrator accounts in Capita OneRevenues and Civica</b></p> <p><b>Capita OneRevenues.</b></p> <p>Our audit identified that there are no controls in place to actively monitor the usage of the generic 'aisdba' and 'academy' accounts which are used to administer the Ingres database supporting the Capita OneRevenues system. The accounts are also a privileged user in the front end of the application.</p> <p>Whilst KeePass is used for storing the details of this account by the IT team, members of the SVPP Operations team who have access to the account do not use this tool. Instead they manage the password locally through the use of password protected spreadsheets.</p> <p>The password for the accounts are currently changed every 90 days in line with the parameters enforced within the application.</p> <p><b>Civica</b></p> <p>Our audit identified 17 generic accounts had been set up as administrators with access to the Civica database and these accounts are not monitored. Whilst we were informed that these accounts are maintained in a password-protected spreadsheet, there was no evidence to support this.</p> <p>There is also no proactive monitoring over of the activity undertaken by any of these accounts to allow timely identification of any inappropriate usage.</p> <p><b>Risk</b></p> <p>The use of generic or shared accounts with high-level privileges increases the risk of unauthorised or inappropriate changes to the application or database. Where unauthorised activities are performed, they will not be traceable to an individual.</p>	<p>Where possible, privileged generic accounts should be removed, and individuals should have their own uniquely identifiable user accounts created to ensure accountability for actions performed.</p> <p>Alternately, management should implement suitable controls to limit access and monitor the usage of these accounts (i.e., through increased use of password vault tools / logging and periodic monitoring of the activities performed). Where monitoring is undertaken this should be formally documented and recorded.</p> <p>Passwords for generic administrative accounts should be changed after every use.</p> <p><b>Management response</b></p> <p>As part of the FULL Security Profile review 2021, Generic accounts will be reviewed and where deemed, still appropriate will be converted to individual accounts. Access logs will also be monitored monthly as part of point 8.</p>


# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
11. 	<p><b>Lack of formal change management procedures for Oracle Fusion.</b></p> <p>Our audit identified that the Council does not manage the change process in Oracle through a ticketing system, instead relying on an Excel tracker that is updated by members of the FMS team.</p> <p>For a sampled configuration change, it was identified that:</p> <ul style="list-style-type: none"> <li>• There was no formal written request from the business users for the change.</li> <li>• There was no formal authorisation to commence development work.</li> <li>• Testing was not formally documented in line with a formal test plan.</li> <li>• Authorisations for promotion in to production were not formally documented.</li> </ul> <p>While we understand that the underlying system changes are managed by Oracle Cloud services, application level changes can impact on the system and users.</p> <p><b>Risk</b></p> <p>The absence of formal change management procedures and formal documentation for changes that have been implemented increases the risk of unauthorised and untested changes being implemented into the production environment, impacting on the integrity and security of data and systems, or resulting in unscheduled system down-time.</p>	<p>It is recommended that management develop and implement a formal change management procedure for changes to Oracle, ensuring that all elements of the change process are formally approved and documented by both business and IT management. Change management procedures typically consist of the following:</p> <ul style="list-style-type: none"> <li>• Documented approvals by business and IT management, including justification and business need for change.</li> <li>• Formally documented testing undertaken by business and IT team users, along with formal sign off by business and IT management.</li> <li>• Documented approvals (such as email trails) of authorisation to promote changes into production.</li> <li>• Documented post implementation reviews confirming if changes have been implemented in line with expectations.</li> </ul> <p>Management should also ensure that the change management procedures are comprehensive and include procedures for different types of change, including Oracle quarterly releases, configuration changes, data changes or emergency changes.</p> <p>and appropriate according to the change type. At a minimum, changes should be:</p> <ul style="list-style-type: none"> <li>• Assigned a 'category/type' including application and emergency changes to ensure that the appropriate approach is taken</li> <li>• Recorded in a service desk ticket or SharePoint form with details of the individual raising it and what further approval is required etc.</li> <li>• Assigned rollback processes in case of change failure.</li> </ul> <p><b>Management response</b></p> <p>We have implemented a non-self assigning of roles and all other change management process are documented in MS Teams – the example picked up was before this change was implemented following the previous year audit.</p> <p>No instances of self-assignment of access rights have occurred since our 2020 report was issued.</p>

## Assessment


-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

# IT general controls assessment findings




12. Assessment	Issue and risk	Recommendations
<p>12. </p>	<p><b>Application password settings not in compliance with the Information Security Policy.</b></p> <p>It was identified that the password configurations in Oracle Fusion are in not in line with the Council's Information Security Policy as follows:</p> <ul style="list-style-type: none"> <li>• Passwords are set to a minimum of 8 characters in Oracle; however, the Information Security Policy requires a minimum of 9 characters.</li> <li>• Oracle only remembers the previous password used; however, the policy requires the previous three passwords to be remembered.</li> </ul> <p>The following password configurations for administrators and generic users in Capita are not in line with the Information Security policy:</p> <ul style="list-style-type: none"> <li>• Passwords are set to a minimum of 7 characters in Capita; however, the Information Security Policy requires a minimum of 9 characters.</li> </ul> <p>The following password configurations for Civica are not in line with the Information Security policy:</p> <ul style="list-style-type: none"> <li>• Number of invalid attempts before account lockout is not defined; however, the Information Security Policy requires this to be set to a maximum of 6 invalid attempts.</li> </ul> <p>Furthermore, it was noted that the Council's Information Security Policy and password guidance on SharePoint are not consistent with each other as the Information Security Policy does not define the number of invalid attempts prior to accounts being locked out.</p>	<p>It is recommended that password parameters for applications used across the Council are aligned to those stipulated in the Information Security Policy.</p> <p>Where this is not possible due to application limitations, management should consult with the application vendor to identify what alternative methods can be used to make the process of logging into the application more robust, such as the use of single sign on.</p> <p>Management should also revise the Information Security Policy to ensure that it reflects the Council's agreed standard password settings (including account lockout) and that this is communicated to all staff.</p> <p>The following password parameters are commonly used by organisations across a wide range of sectors:</p> <ul style="list-style-type: none"> <li>• Minimum password length should be set to 8 characters or above.</li> <li>• Password expiry should be set between 30-60 days.</li> <li>• Password complexity should be enabled.</li> <li>• User accounts should be automatically locked out after a maximum of 5 unsuccessful attempts.</li> <li>• Reset account lockout counter should be set to 15 minutes.</li> <li>• Previous 24 passwords remembered.</li> </ul> <p>The policy should also be revised to account for applications where the standard password criteria cannot be met due to vendor-imposed limitations.</p> <p><b>Management response</b></p> <p>We seek to make the password policy aligned as closely as the system allows.</p> <p>Civica OpenRevenues – Invalid login is hard coded to 3 attempts before user is disabled. We will increase password length to 9 with immediate effect, there is already a requirement to enter a password that contains at least 1 Numeric and Alpha chars and expire every 40 days, with a weekly sweep for inactive users too.</p>

*Continued on next page*

# IT general controls assessment findings

Assessment	Issue and risk	Recommendations
12. 	<p><i>Continued from previous page</i></p> <p><b>Risk</b></p> <p>By not ensuring that application password settings comply with the IT Security Policy increases the risk of users choosing weak passwords which could be easily breached.</p> <p>In the event of a password becoming breached there is an increased risk of fraudulent or erroneous transactions being posted with a lack of accountability.</p>	

## Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

