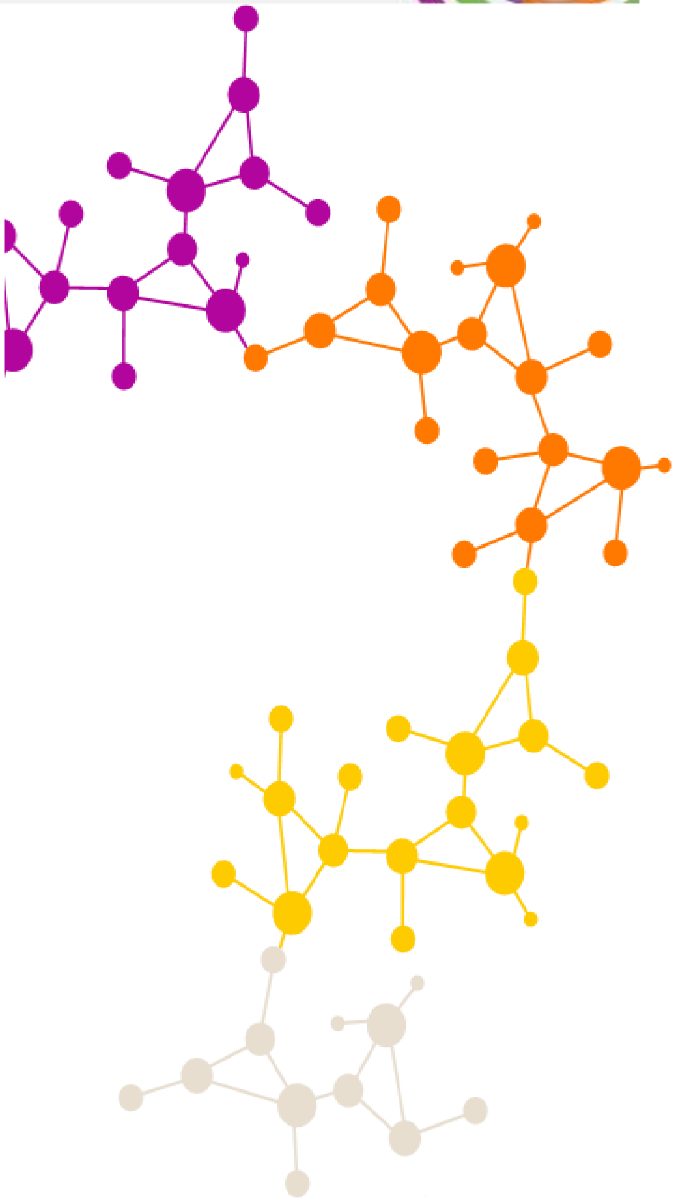
Grant Thornton

An instinct for growth™



Plymouth City Council

Information Technology General Controls (ITGC) Audit Report

Year Ended March 2019

CONFIDENTIAL

This document has been prepared only for Plymouth City Council as part of the 2018-19 financial statements audit and for internal use only. Its existence may not be disclosed, nor its contents published in any way without the prior written approval from Grant Thornton. Grant Thornton does not accept any responsibility to any other party to whom it may be shown or into whose hands it may come.

Grant Thornton
An instinct for growth™

Contents

1. EXECUTIVE SUMMARY

1.1 Introduction

To support its opinion on the financial statements of Plymouth City Council (the Council), Grant Thornton has completed a review of the design effectiveness of the IT General Controls (ITGC) within the IT environment, as they affect the financial statements for year ended 31 March 2019.

This report sets out the summary of observations, scope of the work, the detailed observations, and recommendations for control improvements.

The matters raised in this report came to our attention as a result of the limited-scope ITGC design effectiveness review and that we believe needed to be brought to your attention. Therefore, our comments cannot be expected to include all possible control improvements in Plymouth City Council's ICT environment, where a more wide-ranging engagement might usefully identify additional improvements to improve both efficiency and security.

We would like to take this opportunity to thank all the staff at the Council for their assistance in completing this IT Audit.

1.2 Summary of Observations

- **IT General Controls:** The following control weaknesses were noted in the Security and Access of Plymouth City Council's systems.

    - Lack of formal reviews of Information Security (IS) Policies and enforcement of IS training by business managers
    - Account lockout does not comply with IS Policy
    - Lack of proactive reviews of logical access within Civica, Academy, and iTrent

2. SCOPE & SUMMARY OF WORK COMPLETED

The primary objective was to complete an ITGC review of Plymouth City Council's systems to support the Financial Statements audit. These include:

- Civica (Core Financial System)
- Academy (Revenues & Benefits)
- iTrent (Payroll)
- Active Directory (network)

We completed the following tasks, as part of this IT Audit:

- IT General Controls (Design Effectiveness)
- Documentation of the test results and provided evidence of the observations to IT services for remediation actions.

3. CLASSIFICATION OF RECOMMENDATIONS

The observations contained herein and the detailed recommendations supporting the individual points are broadly classified into two classifications. The assessment for each observation reflects the effect the findings have upon internal control and the Financial Statements.

Assessment	Key to assessment of internal control deficiencies
🔴	Significant Deficiency - risk of significant misstatement
🟡	Deficiency - risk of inconsequential misstatement

4. DETAILED OBSERVATIONS AND RECOMMENDATIONS

No	Observations	Risk(s)	Recommendation & Management Response	Assessment
1.	**Lack of regular formal reviews of Information Security (IS) policies and procedures** We noted that existing IS policies had not been formally reviewed or updated for some time. We were provided with Five policies and an examination revealed: • Access Control Policy (U03), last reviewed June 2011. • Information Protection (U02), last reviewed June 2011, no reference to GDPR & reference to old HMG data classification. • Devon Information Security Partnership, last reviewed Feb. 2007 • Information Security Policy, last reviewed 2007, authorisation by former Chief Executive • Resource Protection Policy (U05) last reviewed June 2009 The Council also provides IS training materials on-line to encourage staff to maintain an effective security awareness.	a) The most current & up to date security administration processes and control requirements may not be formalized, understood by, or communicated to those within the organization responsible for observing and/or implementing them b) Effectiveness of security administration processes and controls may be diminished due to environmental and/or operational changes c) The lack of up to date information security requirements may make sanctioning employees for inappropriate use of information resources more difficult.	We recommend that management: a) Ensure that an annual review of all IS related policies and procedures is undertaken. A record of this activity should be recorded in the version history on each document along with the next review date. b) Senior / strategic management should authorise the distribution of any updated policy and procedure to ensure that information security retains a high profile within the company. **c)** Management should also introduce a process whereby all employees are required to formally acknowledge (at least annually) that they have read, understand, and will abide by requirements outlined in the organization's IS related policies and procedures. Documentation of these acknowledgements should be retained for future reference. d) Departments should be challenged to ensure that their staff remain up to date with the on-line security training materials provided by the Council.	●

No	Observations	Risk(s)	Recommendation & Management Response	Assessment
	We were provided with details of the following three on-line IS related training courses with evidence to support the monitoring. We selected two business areas, 'Finance' and 'Children & Young People and the Environment' for scrutiny and the percentage of staff reviewing this material is given. The results suggest that the review of this training material is not being consistently enforced: 1. **<u>Information Security @ the Council</u>** **Finance**: of 148 staff, 62 had reviewed this material (42%) **Children & Young People & Environment:** of 19 staff, 11 had reviewed this material (58%) 2. **<u>Data Protection Essentials</u>** **Finance:** 19 had reviewed (13%), **Children & Young People & Environment** 18 had reviewed (95%) 3. **<u>Data Safe</u>** **Finance**: 108 had reviewed (73%), **Children & Young People & Environment:** 5 had reviewed (26%)		**<u>PCC Management Response:</u>** • The IS Polices are being embedded within the corporate operating manual, and this will ensure the policies are reviewed annually • A current review of the Policies will start on the 5th July 2019	

No	Observations	Risk(s)	Recommendation & Management Response	Assessment
2.	**Current System Lock-Out Policy** The current infrastructure and password configuration does not comply with the Council's Access Control Policy (U03) which requires that users are locked out for 30 minutes if they fail to provide the correct user account access credentials after three attempts. An examination of the Council's system parameters revealed that this has been set to 30 which is far too high.	Compromise of user accounts through password guessing or cracking.	We recommend that the current account threshold lock-out parameter should be reviewed as the present setting is too high. This setting should ether be altered to comply with the Council's Access Control Policy (i.e. three) or changed following a risk assessment to determine what it should be. If the number of attempts is altered from that stated in the Access Control Policy, then this policy should be updated to reflect the new threshold. **Management Responses:** **Delt Response:** We can easily amend the failed account login attempts from 30 to a lower level on instruction from our customer with immediate effect. **PCC Response:** The Council will ask Delt to review the current settings compared to the Policy	●

No	Observations	Risk(s)	Recommendation & Management Response	Assessment
3.	**Detailed Proactive Reviews of Logical Access within Civica, Academy, iTrent and the network** User accounts and associated permissions within Civica, Academy, and iTrent were not being thoroughly reviewed for appropriateness on a routine basis. We were also not provided with evidence that demonstrated formal, periodic reviews of the network We noted that some elements of user access within these systems were being routinely reviewed for appropriateness, but these reviews were not taking place at a sufficient level of detail. The Council's own Access Control Policy requires that these reviews should take place once every six months.	a) User access to information resources and system functionality may not be restricted on the basis of legitimate business need. b) No-longer-needed permissions that have been granted to end-users may lead to Segregation of Duties (SoD) conflicts. c) Over time, as staff move around the organisation or take on new responsibilities, their IFS access privileges may become disproportionate to their actual job role and duties. Again, this could undermine effective SoD. d) Enabled, no-longer-needed user accounts may be misused by valid system users to circumvent internal controls.	It is our experience that access privileges tend to accumulate over time. As such, there is a need for business management to perform periodic, formal reviews of the user accounts and permissions within financial systems to help maintain an effective SoD. We recommend that business management: a) Undertake reviews of critical financial systems that comply with the Council's own Access Control Policy which stipulates that these are performed every six months. If the Council decides that this is too frequent, then a risk assessment should be undertaken to determine the most efficient approach. The Access Control Policy should be updated accordingly. b) Reviews of Civica, Academy and iTrent and the network user access permissions would support the efforts of the Council to ensure that access is restricted to authorised users only. Evidence of these should be retained for future scrutiny.	●

No	Observations	Risk(s)	Recommendation & Management Response	Assessment
			c) The reviews should also evaluate both the necessity of existing user ID's as well as the appropriateness of user-to-group assignments (with consideration given to adequate SoD). **Management Responses:** **Delt Response:** The recommendation is for business management to carry out actions. Delt do not administer line-of-business security that is internal to the application. We can provide consultancy to assist with those reviews, if 3rd party application vendors are unwilling to provide recommendations. **PCC Responses:** **One Digital Revs and Bens (Academy) and Civica W2** Access review will take place every 6 months. A list of current users will be extracted from each database and users will be contacted by email and expected to complete a new DOI identifying their personal details, service area and team.	

No	Observations	Risk(s)	Recommendation & Management Response	Assessment
			The current DOI form will be reviewed and if necessary, a new online DOI form will be designed and produced, and the appropriate link will be sent to users. The form will include a 'review' option and users will be able to select and provide responses for one or more of the modules within the software applications. The form will generate an emailed PDF that will be sent to the Digital Systems inbox. This is a change from the current route to the 'CustomerServiceImprovement' inbox. Details of the responses will be recorded on a spreadsheet. Liaison with management needs to take place to establish the impact of reducing and/or standardising access levels. **<u>Civica Financial Systems</u>** Access review will be conducted as a rolling 6-month programme across the cohort. This is because a periodic review of users across the databases would be unwieldy due to the numbers involved.	

No	Observations	Risk(s)	Recommendation & Management Response	Assessment
			The Civica Task Centre Alerter system will be used to create emails that are sent to users every 6 months. The email will detail the current permissions and will request that the user responds with their current requirements and within a specified time frame, or risk their access being suspended and ultimately revoked. The user response will be routed to the 'finansys' inbox. Details of the responses will be recorded on a spreadsheet.	