Key to assessment of internal control deficiencies

	Material Weakness - risk of material misstatement
	Significant Deficiency - risk of significant misstatement
	Deficiency - risk of inconsequential misstatement

No.	Assessment	Issue and Risk	Recommendation

No.	Assessment	Issue and Risk	Recommendation
1	●	**Clarity of responsibility for Information Security Policies and Procedures** Documented policies and procedures are in place for the payroll provider, Liberata. Pendle BC have adopted a Trustmarque Access Control policy for their own use. However, it was not clear which other policies apply to Council users or whether they are subject to any of the Liberata policies. The Security policy for Liberata has been reviewed annually, but the Trustmarque policy provided has not been reviewed since 2011. This condition poses the following risk(s) to the organisation: a) Security administration processes and control requirements may not be formalised, understood by, or communicated to those within the organisation 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) Information security processes, requirements and controls may be inconsistently defined, understood and implemented throughout the organisation. d) The lack of formal (documented) information security requirements may make sanctioning employees for inappropriate use of information resources more difficult.	The Pendle BC security administration policies and procedures addressing security administration and related control requirements should be clearly defined, formally approved and communicated to relevant personnel responsible for implementing them and/or abiding by them. Documents should be periodically, formally reviewed (at least annually) to ensure their continued accuracy and appropriateness. **Management Response**: i) The Liberata policies which have been adopted by the Council are included in the latest Information security Management Policy framework document. These policies are; - Access Control policy - Third Party Access(This is now contained in section 3.12 Remote Access Security in the Access Control policy) - Data and Asset management policy - Mobile Computing security policy - Data retention and disposal (This is now in section 3.8 in the Data & Asset Management policy) - Compliance policy ii) The policies which require updating currently not covered by the above and uploading on the Council Intranet are; - IT Assets physical and Environmental Security policy - Malicious code protection policy - Wireless policy Jan 2017 Update – All polices have been reviewed and signed off pending upload to the intranet.

No.	Assessment	Issue and Risk	Recommendation
2	●	**Periodic Employee Acknowledgement of Infosec Policy Requirements** At time of review, existing employees are required via the eLearning package 'Bob's Business' to read and understand the security policies as they are amended. However, they are not required to periodically formally acknowledge that they will abide by them. This condition poses the following risk(s) to the organisation: It is important that senior management promotes a culture where end-users of information resources are aware of their roles, responsibilities and accountability with respect to security of information assets. The lack of periodic formal acknowledgements of information security requirements may make sanctioning employees for inappropriate use of information resources more difficult. The lack of these acknowledgements may lead to a lack of employee awareness of expectations over the use of IT resources. For example, a user who caught sharing personal passwords with other employees may be able to claim ignorance of any wrongdoing.	Management should introduce a process whereby employees are required to periodically (at least annually) formally acknowledge that they will abide by requirements outlined in the organisation's information security policies. Documentation of these acknowledgements should be retained for future reference. **Management Response**: All new employees are informed of Information Security policies as part of their formal induction to the Council. Information to maintain and promote awareness of the policies is also circulated to all staff periodically. The use of 'Bob's Business' as an on-line training resource also supports this activity. Every time staff log on to the network they are presented with the following message which they have to "OK" to proceed: **Important Notice!** *This system and all information contained herein is the property of the Council, and access is granted for authorised users only. Use of this system constitutes your acceptance that use is subject to Council policy and any violation that breaches these provisions may result in disciplinary proceedings.* *All users of this system are expected to have read the appropriate company policies before making use of this system which may be subject to monitoring.* *Log off immediately if you do not agree to these terms.* OK The arrangements outlined above are considered proportionate but during 2016/17 we will consider this again. Jan 2017 Update – No change proposed at this time

No.	Assessment	Issue and Risk	Recommendation
3	●	**Security Administration Rights Granted to Those Performing Financial Reporting Processes or Controls** At time of review, at least one individual responsible for performing financial reporting processes or controls had the ability to administer security and batch processing within Civica Financials and administer security within Chris 21. The combination of financial reporting duties and security administration is considered a segregation of duties conflict. This condition poses the following risk(s) to the organisation: a) Bypass of system-enforced internal control mechanisms through inappropriate use of administrative functionality by (1) making unauthorized changes to system configuration parameters, (2) creation of unauthorized accounts, (3) making unauthorized updates to their own account's privileges, or (4) deletion of audit logs or disabling logging mechanisms. b) Required maintenance and support requests may not be resolved (or may not be resolved timely) due to competing administrative and operational responsibilities. c) Security administration processes (such as user administration processes) may not function consistently or reliably over time to control access to information assets. d) Internal access to information assets and administrative functionality may not be restricted on the basis of legitimate business need.	The responsibility of administering security within Civica Financials and Chris 21 should be transferred to IT system administrators who do not perform financial reporting, processes or controls. Security administration rights within Civica Financials and Chris 21 granted to personnel performing financial reporting processes and controls should be revoked. Alternatively, management should implement a formal / documented monitoring process designed to detect misuse of administrative functionality by personnel responsible for performing financial reporting processes or controls. **Management Response**: Accepted but would like to consider the proposed resolutions outlined above more fully and have the opportunity to discuss the implications of each with the IT Auditor. Jan 2017 Update - remains under review

No.	Assessment	Issue and Risk	Recommendation
4	●	**New User requests for Civica Financials** Line managers verbally notify the Civica System Administrator of any new members of staff. No new user request form is in place. No evidence of the line manager's authorisation for the creation of a user account is retained. This condition poses the following risk(s) to the organisation: a) Internal access to information assets may not be restricted on the basis of legitimate business need b) Individuals' access rights and changes thereto may not be determined and approved by competent management authority c) New employee set-up, modification and termination of access rights may not be performed accurately, comprehensively, or on a timely basis d) Accumulation of access rights as a result of a job transfer may introduce segregation of duties conflicts	The Council should develop and implement a new user form for the Civica Financials system. Line managers should complete this form detailing the access rights required by a new member of staff and leave evidence of their authorisation to create the corresponding user account. Evidence of this form and the line manager's authorisation should be retained. **Management Response**: Agreed. A formal process with supporting documentation will be instigated requiring service management to authorise requests. Jan 2017 Update Implemented - Resolved
5	●	**Lack of Adequate Minimum Password Length Enforcement within Northgate iWorld** At time of review, Northgate iWorld did not enforce adequate minimum password length restrictions. This condition poses the following risk(s) to the organisation: Compromise of user accounts through password guessing or cracking.	We recommend that the Council should enable minimum password length restrictions within Northgate iWorld to a value in-line with good practices and/or the organisation's information security policy requirements (good practice is at least 8 characters). **Management Response**: Password minimum length will be changed as per the recommendation. This will be rolled out when the next software release is installed on the live database (due before 30/9/16). Jan 2017 Update Implemented - Resolved

No.	Assessment	Issue and Risk	Recommendation
6	●	**Network Passwords stored with inadequate encryption security** Network passwords are stored by using reversible encryption. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords which is insecure and not recommended. This condition poses the following risk(s) to the organization: Compromise of user accounts which could result in unauthorised access to data, disruption to IT operations and reputational damage.	We recommend that the "store passwords using reversible encryption" setting is disabled within the AD password group policy. Adequate testing should be performed before implementing this change to validate that it does not have any detrimental impact on other IT applications. **Management Response**: The recommendation is agreed and the "store passwords using reversible encryption" has now been disabled as at the 22nd July 2016 (evidence provided) Jan 2017 Update Resolved

No.	Assessment	Issue and Risk	Recommendation
7	●	**Chris 21 and Northgate iWorld password complexity enforcement** Password complexity (i.e. the requirement that passwords must contain characters from three out of four categories i.e. letters (uppercase), letters lowercase, numbers and special characters) was not enforced within Chris 21 and Northgate iWorld at time of review. This condition poses the following risk(s) to the organization: Compromise of user accounts through password guessing or cracking.	Where this is possible within the application, password complexity should be consistently enforced within Chris 21 and Northgate iWorld. **Management Response**: (a) Northgate iWorld When using passwords that are encrypted (as we do for Northgate iWorld) we cannot use case-sensitivity. With regard to using punctuation, Northgate's advice is that its use may cause system issues. I have attached Northgate's latest security guide and pages 15 and 16 refer in that regard. Passwords already must be alpha-numeric. Please refer to separate WORD document provided with this response which outlines Northgate's position on this. Jan 2017 Update Not feasible to implement – Audit aware (b) Chris 21 Agreed. There is capability within the system for a password criterion to be set up that meets the complexity requirements. Frontier to advise on how this is done locally. Jan 2017 Update - resolution being progressed with Frontier currently.

No.	Assessment	Issue and Risk	Recommendation
8	●	**Removing Leavers' Access Rights within Civica Financials** Security administrators within Civica Financials rely solely upon a monthly HR produced listing of leaver activity to notify them of which accounts should be disabled as a result of HR activity. Because of the time elapsing between termination dates and the dates these reports are provided to security administrators, this practice leaves a potential window for leavers' user accounts to remain enabled. This condition poses the following risk(s) to the organisation: a) Access to information resources and system functionality may not be restricted on the basis of legitimate business need b) Enabled, no-longer-needed user accounts may be misused by valid system users to circumvent internal controls c) Terminated employees may continue to access information assets through enabled, no-longer-needed user accounts d) Revocation of access rights may not be performed accurately, comprehensively, or on a timely basis	All logical access within Civica Financials belonging to terminated personnel (i.e. "leavers") should be revoked in a timely manner (preferably at time of termination). Whilst historical reports (e.g., monthly) of leaver activity enable security administrators to identify and revoke logical access associated with leavers, relying solely on such reports does not enable leavers' logical access rights to be removed in a timely manner. Civica Financials administrators should be provided with (a) timely, proactive notifications from HR of leaver activity for anticipated terminations and (b) timely, per-occurrence notifications for unanticipated terminations. Security administrators of financially critical applications should then use these notifications to either (a) end-date user accounts associated with anticipated leavers or (b) immediately disable user accounts associated with unanticipated leavers. **Management Response**: The primary control is the removal of a leavers access to the Active Directory – Managers are required to complete a series of steps when a staff member is leaving including revocation of their network access. As a secondary control Finance will request that HR update finance immediately with termination dates for staff leavers. Jan 2017 Update - Resolved

No.	Assessment	Issue and Risk	Recommendation
9	●	**Proactive Reviews of Logical Access within Chris 21, Northgate iWorld and Active Directory** User accounts and associated permissions within Chris 21, Northgate iWorld, and Active Directory were not being formally, proactively reviewed for appropriateness. This condition poses the following risk(s) to the organization: a) Gaps in user administration processes and controls may not be identified and dealt with in a timely manner b) Access to information resources and system functionality may not be restricted on the basis of legitimate business need c) Enabled, no-longer-needed user accounts may be misused by valid system users to circumvent internal controls d) No-longer-needed permissions may granted to end-users may lead to segregation of duties conflicts e) Access privileges may become disproportionate with respect to end users' job duties	It is our experience that access privileges tend to accumulate over time. As such, there is a need for management to perform periodic, formal reviews of the user accounts and permissions within Chris 21, Northgate iWorld, and Active Directory. These reviews should take place at a pre-defined, risk-based frequency (annually at a minimum) and should create an audit trail such that a third-party could determine when the reviews were performed, who was involved, and what access changed as a result. These reviews should evaluate both the necessity of existing user ID's as well as the appropriateness of user-to-group assignments (with due consideration being given to adequate segregation of duties). **Management Response**: (a) Northgate We already review open accounts on a quarterly basis and accounts with no recent activity are closed. We will, however, look at an annual review of all users' job roles in conjunction with section managers and team leaders. Jan 2017 Update - to be scheduled prior to end Mar 2017. (b) Chris 21 Agreed. This is normal practice at year end, however, due to staff changes occurring at year end this year, there has been a delay in this review taking place. Jan 2017 Update - resolved. (c) Active Directory Jan 2017 Update - Currently, as part of the transition of the service from Trustmarque to Liberata there is a review being undertaken on Pendle AD accounts which should be complete by the year end.

No.	Assessment	Issue and Risk	Recommendation
10	●	**Reviews of Information Security Logs Created by Civica Financials, Chris 21, Northgate iWorld, and Active Directory** Logs of information security activity within Civica Financials, Chris 21, Northgate iWorld, and Active Directory were not being formally, proactively, and routinely reviewed. This condition poses the following risk(s) to the organisation: Without formal, proactive, and routine reviews of security event logs, inappropriate and anomalous security activity (e.g., repeated invalid login attempts, activity violating information security policies) may not identified and/or addressed in a timely manner.	Given the criticality of data accessible through Civica Financials, Chris 21, Northgate iWorld, and Active Directory, logs of information security events (i.e., login activity, unauthorised access attempts, access provisioning activity) created by these systems should be proactively, formally reviewed for the purpose of detecting inappropriate or anomalous activity. These reviews should ideally be performed by one or more knowledgeable individuals who are independent of the day-to-day use or administration of these systems. **Management Response**: (a) Northgate We would like further clarification/advice on this point please. If we are ruling out knowledgeable individuals who are not independent of the day-to-day use or administration of these systems then who is best placed to do this, as this potentially rules out anyone who would have the necessary knowledge to do the reviews. I have discussed this with Pendle BC's Audit & Performance Manager who feels it would also be inappropriate for Internal Audit to do. Incidentally, Iworld Accounts are automatically locked after 3 unsuccessful login attempts. (b) Financials Knowledge of the logs is limited and we will discuss this further with Civica, the application provider. We also need to consider the reference to 'knowledgeable individual' independent of the system as it is unclear how, for example, someone outside of finance would know what would represent the appropriate use of the application modules for each user. (c) Frontier Agreed. Frontier have confirmed that such audit reports exist and will advise on how to set them up. Jan 2017 Update - resolution being discussed with Frontier & Civica currently.