Appendix 1

Key to assessment of internal control deficiencies

	Assessment	Issue and risk	Recommendation
1	●	**Default SAP roles are assigned to SAP users** The organisation has provided IT staff with SAP functions that allow financial data to be managed within the live environment. There are 3 users from third party support AXON who have access to SAP standard role SAP_FI_GL_BALANCE_CARRYFORWARD The list of 3 users is as below C-KWIRAWAN C-MAMUZNI C-PRUMANOUW This is a repeat observation from 2014/15 IT audit The process of creating ad-doc user permissions that are not identifiable with a job position in the organisation increases the risk that the permissions will be inappropriate and segregation of duties conflicts will be introduced. SAP default user profiles should generally be restricted from use as they may grant excessive privileges	Management should ensure that user permissions are consistent with job positions within the organisation. Periodic reviews of the SAP profiles should be undertaken to ensure that the profiles and roles match the job position over time. Where it is necessary for IT support staff to have financial management access, this should be strictly controlled through the use of a firefighter account. **Management response:** These 3 users are not active, both C-KWIRAWAN and C_MAMUZNI have an end date of 30.06.2014, C-PRUMANOUW has an end date of 31.12.2014. SAP_FI_GL_BALANCE_CARRYFORWARD has been removed from these accounts and all other SAP standard roles have been removed from end users. The SAP Security Policy has been updated to include the process to be followed for assigning and removing the firefighting role and accounts.
2	●	**Segregation of Duties Conflicts** The organisation lacks adequate controls to prevent segregation of duties conflicts from occurring within the SAP role structure. We note that several medium to high-risk conflicts were present	It is recommended that management take steps to examine the extent of all user access segregation conflicts and reduce the number of conflicts where possible given the size of the organization. Management should examine whether existing compensating controls are appropriately configured to

	Assessment	Issue and risk	Recommendation
		in user accounts. Our analysis focused on two business cycles, purchase to pay and record to report. For brevity, only the key highlights are noted here – a more detailed is provided in a separate document. In consideration of the accounts payable 'P2P' process we noted the following: • A total of 9 users have core authorisations to vendor master data and can enter a vendor invoice. • A total of 3 users have core authorisations to vendor master data and can enter a purchase order. • A total of 3 users have core authorisations to create a purchase order and post goods receipt linked to this purchase order. • A total of 3 users have core authorisations to vendor master data and can enter goods receipts. • A total of 2 users have core authorisations to enter a goods receipt and enter a vendor invoice. In respect of the record to pay process (general ledger reporting) and manual postings in the SAP FI module, we noted the following: • A total of 834 users have core authorisations to record manual adjustment for accounts payables and clear them at the general ledger level. • A total of 35 users have core authorisations to make manual accounts payable postings and release them for payment. • A total of 19 users have core authorisations to open or close financial periods and make manual postings.	control the risks posed by the access conflicts. Management should consider a process to prevent further conflicts from being introduced into the SAP role structure and user base. **Management response:** The users concerned are in Finance Operations or the SAP Support Team. Users in Finance Operations will have the conflicts removed and a firefighter role created for their purposes. The relevant P2P transactions will be removed from the support roles. To be actioned by end June 2016. A comprehensive strategy is in the process of being developed to address SoD conflicts, which recommends the use of a specialist tool to assist the process. This will be presented to the SAP Finance Governance team in June 2016. In the meantime some changes are being made which will remove transactions from roles that are responsible for a large number of these conflicts. 1. Remove Create GL from Imprest roles. Approx. 300 users. 2. Remove clearing transactions from ACCMAN/ACCADMIN 3. Remove inappropriate AP roles from users as necessary – to be completed by 30.06.2016

	Assessment	Issue and risk	Recommendation
		• A total of 15 users have core authorisations access to open or close a financial period and make a mass reversal of documents for a previous period. The above user listing contains all SAP dialog accounts (type A) available in the SAP system. The CSI AA 2014 tool (used for SoD analysis) functions in a manner that it reports SoD conflicts across SAP company codes. There are defined rule sets in the CSI AA 2014 tool that evaluate your SAP system authorisations to a rule set combination of SAP standard authorisation (SAP t-code and SAP authorisation objects) in conflict. This is a repeat observation from 2014/15 IT audit The organisation lacks adequate controls to prevent segregation of duties conflicts from occurring within the SAP role structure. We note that a large several medium to high risk conflicts were present in user accounts. Our analysis focused on two business cycles, purchase to pay and record to report. For brevity, only the key highlights are noted here – a more detailed analysis can be provided on request.	
3		**Excessive access to execute SAP programs** In the SAP Production server, it was noted that 80 dialogue SAP user accounts from user group BCC and 3 dialogue SAP user accounts from user group CASUAL had access to SA38. This is a repeat observation from 2014/15 IT audit The use of the transaction code SA38 in the production environment should be highly restricted since it provides access	The use of SA38 should be restricted to system administrators and personnel who have been given permission to access all custom programs. Access to SA38 provides full access to any program that does not contain an authority check and can therefore circumvent the standard SAP authorisation model. **Management response:**

	Assessment	Issue and risk	Recommendation
		to run custom programs that have not been secured with authorisation objects or authorisation groups, thereby allowing the user to access functionality nor associated with their normal SAP role.	SST will investigate which end user roles in user group BCC contain transaction SA38 and why. Transactions will be created for the programs concerned and SA38 removed from users in user group BCC. To be actioned by 31.08.2016.
4		**Excessive access to edit SAP programs directly in the SAP production system** We noted 1 SAP user account "C-HCLERPSRM" from AXON, 2 SAP user accounts (ARCLARKE, MWILKINSON) from BCC and 8 SAP user accounts from Systems Solutions team (SST) have access to SAP transaction code SE38 with core authorisations to change SAP programming code. The use of SAP transaction code SE38 with core authorisations to make code changes directly in the SAP production system could lead to SAP system instability, unauthorised changes to BCC programs and the risk of financial misstatements.	The use of SE38 should be restricted via the use of fire fighter accounts that are kept logged in the system and the usage is controlled via management approval and is constantly logged for review and follow up actions. **Management response:** Z:SUP_DEBUGGER_ACCESS_ALL has been removed from ARCLARKE. MWILKINSON is a member of the support team and her account group has been changed accordingly to SST. Further investigation will be carried out to assess whether access to this transaction can be limited further. See previous response regarding the procedure for accessing the firefighter account.
5		**Excessive access to change system wide parameters in RSPARAM** The RZ10 transaction is not appropriately restricted to a minimum number of users. It was noted that 3 SAP user accounts (CARJENKINS, RSHOVELL, SHARLOCK) from user group BCC and 4 SAP user accounts (C-KMANGIPUDI, DEMACKENZIE, MHEYWOOD, SFLOYD) from User group SST had access to the RZ10 transaction.	Access to this transaction code should be restricted to the BASIS team and the EMERGENCY or fire-fighter user ID. No end users or other IT staff should have access to this transaction. **Management response:** Inappropriate access to RZ10 is no longer available to end

	Assessment	Issue and risk	Recommendation
		This is a repeat observation from 2014/15 IT audit Inappropriate use of the RZ10 transaction can expose the SAP system to security breaches and other operational problems. The transaction allows many system security and operational parameters to be switched off or changed for example and is a transaction that should be used only where there is approval from management under a change control process.	users. A new Auditor role has been created. SST RZ10 access for support staff will be restricted to 'display only'. It has been removed from other users.
6	●	**Super user access to SAP system is not restricted** At the time of review we observed that SAP_ALL profile was assigned to 3 user accounts BCC-BATCH FALYAS MJACKSON The SAP_ALL authorisation profile contains virtually full system rights and should not be used with any dialogue type accounts within the production environment. The profile provides access to all IT functions as well as business transactions which if misuse can cause operational instability and financial misstatements.	The SAP_ALL profile should be reserved for use within an emergency or fire-fighter type ID that can be locked when not in use since most day to day administrative activities do not require such wide ranging access as provided by SAP_ALL. **Management response:** The SAP_ALL profile has been removed from MJACKSON and FALYAS. BCC-BATCH is used for creating and running batch jobs. The account type has been changed to "system" from "dialogue".
7	●	**Excessive access to SAP batch jobs administration** The ability to change the batch schedules and potentially implement new programs is not restricted with authorised users only. Our review noted 91 SAP user accounts from user group BCC and 3 SAP user accounts (C-LEAHSMITH, C-NFOSH, SALLSMITH) from user group CASUAL have administrator access to SM37 (via authorisation object S_BTCH_ADMIN).	Management should ensure that batch administration utilities are restricted to appropriate users. Normally users require batch authorisations to be able to run transactions in the background and this can be given using the S_BTCH_JOB authorisation object. **Management response:** A review of users with authorisation to run batch jobs will be

	Assessment	Issue and risk	Recommendation
		Batch programs have the capability of making multiple postings which without proper authorisation and appropriate scheduling may lead to unreliable reporting. Because all valid batch jobs including especial purpose jobs, access to the administration options provided by S_BTCH_ADMIN can lead to inappropriate batch jobs being run and allow unauthorised users to run jobs as another user.	carried out. This review will also ensure that access to batch jobs is restricted and users are only able to submit batch jobs to run with their own user-id. To be completed by 31.07.2016.
8		**Excessive access to modify live SAP table data** The SM30 or SM31 transaction is not appropriately restricted and the number of users appears to be excessive for the sensitivity of the transaction code. It was observed that 4 SAP user accounts (CARJENKINS, MWILKINSON, RSHOVELL, SHARLOCK) and 14 SAP user accounts from user group SST, BASIS, AXON had access to SM30 or SM31 transaction. We also note, the setting rec/client was set to OFF. The current setting prevents any current logging of SAP tables changes and therefore the possibility of a compensating control. This is a repeat observation from 2014/15 IT audit Access to these transactions under certain conditions can allow customised or standard data tables to be edited directly potentially resulting in unauthorised entries or database integrity problems.	Management should ensure that customisable tables are adequately protected by preventing users from using the SM30 or SM31 transaction code. Where this is not possible due to business requirements customisable tables should be protected via authorisation groups and users should be restricted in their access to those authorisation groups. At a very minimum, no user with access to SM30 and SM31 should have a wild card entry (*) in the DICBERCLS field of the S_TABU_DIS authorisation object. In all cases where users (both IT and end user) have access to SM30 and SM31, management should consider logging the use of these transactions and should review them periodically. **Management response:** We have reviewed which users have access to transactions which modify SAP table data and restricted their access to specific tables in the system. Logging table changes: by default the rec / client is set to

	Assessment	Issue and risk	Recommendation
			'off'. We are concerned that enabling this feature will have a detrimental effect on system performance and therefore do not plan to implement it.
9		**Absence of SAP User Access Reviews** During our review, we noted that SAP user access reviews are not performed. In addition, no review is performed on potentially conflicting assignment of SAP access roles or transactions. Ensuring that system access remains pertinent to a person's job responsibilities is considered to be a basic ITGC control and is achieved by regular review. The absence of user access reviews on a periodic basis may lead to users accumulating excessive access in SAP. Inappropriate or excessive access rights to SAP may result in inappropriate user access potentially leading to financial misstatements.	A user access review should be carried out at least annually, though it is recommended that the process is split up bi-annually. The user access review should consist of two primary objectives: - assess whether the user still requires SAP access - assess whether the user should retain the authorisations currently held It is also recommended that the review considers sensitive transactions. Sensitive transactions are business functions that have a significant impact on the system or data. The review process can also provide an opportunity to review any compensating controls that have been agreed to mitigate risks with users that have sensitive transactions or segregation of duties conflicts. We acknowledge that the SAP application does not provide effective tools to easily report on what users have access to. We therefore recommend management to consider the acquisition of third-party tools that enable this task to be performed. **Management response:** We have undertaken a high-level review of Security and Authorisations and developed an action plan to address the key risks, including facilitating a process to enable Managers to comply with the requirement to review SAP access for their

	Assessment	Issue and risk	Recommendation
			staff on an annual basis. Deadline for implementation 31 December 2016.
10	●	**Password logical access controls** The organisation is not currently enforcing very strong passwords by the configuring the application to force user to create passwords which contains at least 1 special character. The SAP System is vulnerable to password guessing and thus may lead to unauthorised access to SAP financial information.	Management should improve the complexity of passwords by enforcing the need for at least one special character in the password string. Special characters are a key feature in ensuring that passwords are not easily guessed or easily discovered through the use of dictionary attacks against the password's hashed value. **Management response:** Most users access SAP through the Enterprise portal which authenticates passwords against Active Directory (AD). BCC operates a default password policy which requires the password to contain characters from at least three of the following categories: Uppercase letters Lowercase letters Base 10 digits (0 through 9) Non-alphanumeric characters (special characters) (for example , !, $, #, %) Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. Password validation for users logging on with the SAPGui is designed to replicate the above policy, but does not enforce the use of special characters. We do not propose to change this policy by forcing the use of at least 1 special character.
11	●	**Segregation of duty conflict – SAP development and user security administration access**	Programmers should normally be restricted from having any operational access in the production environment which is best achieved by removing their user record. Temporary

	Assessment	Issue and risk	Recommendation
		The organisation does not adequately separate responsibilities for programming from security or other operational functions. It was noted that one user MJACKSON had access to development utilities as well as user management functions such as SU01. We also note that under certain circumstances, the user management functions could be used to assign the SAP_ALL profile. The failure to maintain separation between programming responsibilities and system security can potentially allow system security parameters to be compromised and unauthorised data changes to be go undetected.	production access may be appropriate for certain change projects, however it is recommended that such access is removed after a defined period of time or closure of the project. **Management response:** SAP_ALL has been removed from MJACKSON. See earlier comments about Firefighter access.
12	●	**Passwords to SAP default accounts are not changed** The organisation has not adequately secured the SAP default accounts. The review noted that default passwords were still assigned to SAPCPIC default account in SAP client 001. The SAP default accounts use powerful profiles that give full access to the productive or installation reference system. Default passwords are used with default accounts to allow the installation of SAP. All default accounts present an opportunity for inappropriate use, however, RFC type accounts represent the greatest risk. RFC accounts can be used to set up commands between installation and production clients.	Default passwords should be changed immediately to avoid the risk of system compromise. A priority should be to change default passwords on default account like SAPCPIC which are used to run RFCs between the SAP clients. **Management response:** Audit logs show that this account has not been used at all in over 12 months for any type of login (Dialog/RFC/CPIC) nor used to start a transaction nor report. The password has been changed.