APPENDIX 3 – Executive Summaries finalised since last update to Accounts, Audit & Risk Committee May 2022

Finalised Audits 21/22:

Key Financial Systems 21/22

Overall conclusion on the system of internal control being maintained	A

SYSTEMS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Sales to Cash	A	1	5
Procure to Pay	A	0	3
Record to Report	G	0	1
Budget to Control	G	0	0
		1	9

.

Opinion: Amber	
Total: 10	Priority 1 = 1 Priority 2 = 9
Current Status:	
Implemented	9
Due not yet actioned	0
Partially complete	1
Not yet Due	0

Following a successful project implementation, the Unit 4 finance system went live at the start of the 2021/22 financial year. This audit has focussed on review of key processes across the main key financial systems, considering how well these are working in practice post implementation.

Some weaknesses were noted in the Sales to Cash process including delays in clearing of the debtor suspense account, inconsistencies and delays in debt monitoring and recovery, delays in processing of write offs and inconsistencies in retention of documentation to support write offs. Delays were also noted in the processing of refunds. Management actions have been agreed to strengthen these processes which include the development of clear guidance for finance staff to promote consistency in approach and clarify expectations in relation to process, retention of documentation and timescales.

Duplicate customer and supplier accounts were identified. Unnecessary duplicate customer accounts can complicate debt monitoring and recovery and unnecessary duplicate supplier accounts can make tracking of supplier spend more complex and prone

to error. Whilst it is acknowledged that some of these duplicates are unavoidable (for example where a supplier is part of a franchise and has the same name, but different contact and payment details), this requires review to ensure that any unnecessary duplicate accounts are removed.

In relation to procure to pay, some instances were identified where purchase orders were being raised retrospectively. Management action has been agreed in relation to running routine reporting on this within finance, so that this can be followed up with the relevant service area. Some discrepancies were noted in the accuracy of recording of payment due dates on Unit 4. Whilst this did not have an impact on the timeliness of making payment, performance reporting on the timeliness of payments is based on the invoice due date recorded on the system. Therefore, inaccuracies in recording could impact on the accuracy of performance reporting in this area.

Issues with procurement processes at service level including delays in goods receipting and prompt action to pass on invoice documentation for payment were noted as part of a separate audit of Waste Collection Services. Management actions were agreed to address the weaknesses as part of the reporting on that audit. Audit testing completed as part of this audit has not identified these issues across other service areas tested.

No significant issues were identified in relation to Budget to Control processes. It is noted that budget monitoring processes continue to develop with Budget Managers now completing forecasting themselves on Unit 4, with less reliance on Finance Business Partners.

Performance reporting arrangements are also being developed which will allow Directors and Assistant Directors to add commentary to monthly financial reporting within the Unity performance reporting system.

Finalised audits 22/23:

Cyber Security 22/23

Overall conclusion on the system of internal control being maintained	A

SYSTEMS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Education and Awareness	A	0	2
Malware Scanning	A	0	3
Privileged Access	A	0	4
Vulnerable Services	G	0	1
Vulnerability Scanning	R	1	0

Security Patching	G	0	0
Backups	A	0	2
Incident Response	R	1	0
		2	12

Opinion: Amber	
Total: 14	Priority 1 = 2 Priority 2 = 12
Current Status:	
Implemented	13
Due not yet actioned	1
Partially complete	0
Not yet Due	0

Cyber security remains a key area of business risk and there are no signs of this changing given the seemingly endless reports on data breaches, ransomware, phishing and other types of cyber-attack. All organisations that have digital systems are vulnerable to cyber-attacks and must operate strong security controls to minimise the risk of any attack being successful. It is important to note that fully implementing all of the actions in this report will not provide a complete guarantee that the organisation will be cyber-secure. The nature of the risk is such that there is never 100% security against a cyber-attack.

Education and Awareness:

Senior management and Members at the council are given updates on cyber security and have also been made aware of specific threats, such as phishing. Cyber is included on the IT risk register and also the corporate risk register, although we noted that the risk is not scored consistently between the two and hence senior management may not have an accurate assessment of the overall risk to the council. The risk registers were also found not to include all the relevant controls that are relied upon to manage the risk to ensure any changes in the control framework are reflected in the risk assessment.

Users are sent periodic general reminders on cyber security and made aware of specific threats when they arise. Cyber security is also covered in the mandatory training for all users.

Malware Scanning:

A number of different tools are used to scan for malicious software, including ransomware. IT Services subscribe to the National Cyber Security Centre's (NCSC) security and monitoring services for the public sector.

Privileged Access:

The accounts with privileged access should be reviewed and the owners of such accounts made aware of their responsibilities.

Vulnerable Services:

A review of some common network services, which are often exploited in ransomware attacks, confirmed that risk exposure is minimised.

Vulnerability Scanning:

A new vulnerability scanning tool is being implemented to replace a previous tool.

Security Patching:

No risk areas have been identified.

Backups:

Backups are taken to the cloud and protected against ransomware attacks.

Incident Response:

There is a draft Cyber Incident Response Plan, which details how IT Services will respond to a major cyber-attack. The plan needs to be further developed and formally tested to ensure it is effective.

IT Infrastructure 2022/23

Overall conclusion on the system of internal control being maintained	A

SYSTEMS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
IT Roles and Responsibilities	G	0	0
Documentation	A	0	2
Infrastructure Monitoring	A	0	1
Access Controls	A	1	1
		1	4

.

Opinion: Amber	
Total: 5	Priority 1 = 1 Priority 2 = 4
Current Status:	
Implemented	2
Due not yet actioned	2
Partially complete	0
Not yet Due	1

The council's IT infrastructure, which runs all critical IT applications and services, has recently been migrated from a joint data centre with South Northamptonshire Council into the Microsoft Azure cloud.

IT Roles and Responsibilities:

The Technical Services team within IT Services are responsible for managing and monitoring all IT infrastructure in the Azure Cloud. There are four designated members of the team who look after the council's infrastructure and their responsibilities are documented within job descriptions. The size of the team and access to wider resources within IT Services means there is no key person dependency. There is a weekly meeting between the IT Technical Services Manager, Principal Technical Consultants and the four infrastructure leads to review and discuss any issues.

Documentation:

The documentation in place to support the Azure environment is limited and incomplete in many areas. This audit was undertaken prior to the full completion of the SNC (South Northamptonshire Council) separation project, for which the priority was to successfully complete all technical work to agreed deadlines. Documentation was scheduled to be completed later to ensure that it was accurate and up to date at the close of the project. Now that the migration work is complete, all documentation will be produced and finalised to ensure the Azure environment is fully understood and can be effectively supported and maintained.

Infrastructure Monitoring:

The procedures for monitoring applications and services within Azure need to be improved to reduce the risk of poor system performance and, in a worst case scenario, a system failure. Azure has a solution for monitoring applications and services but it has been setup by a third-party and is new to the IT infrastructure team and consequently their skills are limited as they are learning on the job. Formal training for members of the team may be helpful so that the solution can be further developed to alert on how applications and services are performing and to proactively identify any issues affecting them or the resources they depend on.

Access Controls:

User groups are setup to manage access within Azure and our testing confirmed that membership of these groups is limited to designated users within IT Services and that their access is subject to multi-factor authentication (MFA) in accordance with good practice. Third-party suppliers also have access to Azure for supporting systems and applications and their access is limited to the environments they support. We found that supplier access is not subject to MFA and their accounts are not disabled when they are not being used. This presents a risk that supplier accounts are compromised in a cyber-attack to get unauthorised access to Azure or that suppliers make changes to systems and applications without prior notice or approval, which could impact on system integrity and availa