Critical Application Controls

Allerdale Borough Council

MIAA ASSURANCE

Contents

1. Executive Summary

Information technology is all pervasive in modern organisations and the reliance on data, systems and the underpinning infrastructure are increasingly business critical. It is essential to ensure there are robust controls in place to maintain confidentiality, integrity and availability of the Council's services.

The Council, recognising the criticality of effective application control frameworks commissioned a review as part of its Internal Audit Plan, which has been delivered under contract, by MIAA that was started towards the end of the 18/19 plan period.

The review has confirmed that the Council's IT Department is exercising good practice in a number of areas however, a number of areas of risk have been identified which require consideration for remedial action these are summarised in the table below:

Area	Findings
Governance and risk management **(Abavus system)**	**Good practice noted included (for all three systems):** • A corporate risk management system was in place and active; • The council have demonstrated a broad range of controls across its services at network level; • Public Services Network (PSN) standards compliance. **Area for consideration included (for all three systems):** • Risk assessments of the specific applications had not been undertaken and the corporate risk system did not include system risks; • Although they were happy with control framework in place, when interviewed system owners were not aware of the details of control frameworks implemented (i.e. how long logs kept, maximum possible data loss, etc).
Legal compliance (for systems holding PID)	**Good practice noted included (applicable to all three systems):**

(Academy system)	• The council provided evidence that an organisation wide data flow analysis including the lawful basis of the data was held for all three of the systems.
User Access Controls **(Elector8 system)**	**Good practice noted included (applicable to all three systems):** • The council IT team liaised with HR to ensure leavers were removed from the network; • The council are in the process of introducing a system whereby desktop profiles and applications are assigned by staff functional group. **Good practice noted from other systems:** • **Academy,** evidence of an active formal user authorisation request was reviewed, including a declaration of interests system which allows user exclusion for records based on personal relationships etc. **Area for consideration included:** • **Elector8,** documented job roles are in place for user accounts within the system, with a small user base. However of the 15 user accounts 3 were generic access administrator accounts, and we were informed that one of the generic admin accounts is utilised by two members of IT staff. • **Applicable to all,** the council did not perform regular account dormancy or user privilege reviews for any of the three systems covered by this review.
Data Stores **(Abavus system)**	**Good practice noted included (for all systems):** • **Applicable to all systems**, IT staff demonstrated good knowledge of issues around data store security on the council network; • **Academy,** Separate instance for Allerdale council. **Area for consideration included (Abavus system):** • As a hosted system the council should consider how it gains ongoing assurances around the segregation and security of its data.

Logging and Monitoring **(Academy system)**	**Good practice noted included (Academy systems):** • Logging was demonstrated as being detailed and currently held for the life of the system. **Area for consideration included (for all systems):** • It was not clear that guidance or standards had been agreed at the council in relation to logging requirements for its systems to ensure compliance to GDPR legislation, for example retention period, detail recorded, etc.
Support, patching and vulnerability management **(Elector8)**	**Good practice noted included (for all systems):** • Patching was largely up to date; • Council staff demonstrated flexibility ensuring patching was done outside of core work hours. **Area for consideration included (Elector8):** • A local decision to halt routine patching of the Elector8 election system and servers by the technical team during election periods had not been endorsed by the system owner.
Change control **(Abavus system)**	**Good practice noted included:** • **Abavus**, Changes are authorised via purchase order; • **Academy**, formal change request system implemented by Carlisle team. **Area for consideration included (Elector8):** • The council does not operate a formal change control system, changes are raised as jobs on the help desk system and authorisation recorded on the job.
Testing	**Good practice noted included (for all systems):** • **Academy,** separate segregated test system**;**

(Academy system)	• **Abavus**, Development version of system implemented for testing forms. **Area for consideration included (for all systems):** • There are no formal testing guidelines or standards implemented by the council.
Resilience, recovery and continuity **(Elector8 system)**	**Good practice noted included:** • **Elector8**, backups proven to be operating consistently; • **Applicable to all**, Council staff continuity arrangements are documented generically for the council's network and recovery priorities in place; • **Applicable to all**, spare capacity and alternative site in place for council network. **Area for consideration included (for all systems):** • There was no system specific recovery documentation for critical applications or evidence of recovery tests specific to those systems; • Interviewed system owners were not aware of maximum possible data losses or downtimes.

As a result of these findings the level of assurance provided, in accordance with the criteria set out at Appendix B, is:

Limited Assurance

2. Background and Introduction

The review of critical application control processes at Allerdale Borough Council was conducted in accordance with the requirements of the Audit Plan.

Technology is a critical enabler within the council providing both inward and public facing services. This technology drives the core business of the council and provides a critical interface to the population enabling the redesign of services in order to increase the quality of services while driving down the cost of delivery.

The applications selected for review were:

- Abavus, a digital communication and work flow management system provided by a commercial at third party;
- Academy, a benefits management system, provided and supported by Carlisle Council under agreement; and
- Elector8, an election management system.

As repositories of critical business information, it is essential that the council is able to manage access and ensure the integrity and availability of the data to both support effective delivery of council services but also to ensure that it is compliant with its legal, regulatory and best practice guidelines including but not exclusive to:-

- The Public Services Network Compliance - which creates the right environment to share information and services;
- The National Cyber Security Centre's Cyber Essentials / Cyber Essentials Plus Scheme – demonstrate commitment to cyber security and are backed by Government and Industry.
- The EU General Data Protection Regulation – which as well as driving data protection requirements also requires that organisations ensure the on-going availability of systems and data[1];.

Recognising the importance of appropriate controls in place to maintain confidentiality, integrity and availability of the Council's service, senior management commissioned this review to obtain assurance relating to the protection of these key systems, and identify opportunities for improvement, where appropriate.

3. Objective

The objective of this review was to provide a high-level assessment of the development and application of critical controls over a sample of key systems. The review sampled

[1] The regulation carries penalties for non-compliance to a maximum value of €20m or 4% of turnover, whichever is the greater.

controls over systems, providing an opinion upon the understanding and application of controls across these systems, rather than providing an in depth opinion upon the control of any given system.

The assessment was delivered against the three systems identified and agreed by the IT and Audit teams on the matrix basis detailed below:

Control area	Abavus	Academy	Elector8
A. Governance and risk management	x		
B. Legal compliance (for systems holding PID)		x	
C. User access control			x
D. Data stores	x		
E. Logging, monitoring and alerting		x	
F. Support, patching and vulnerability management			x
G. Change control	x		
H. Testing		x	
I. Resilience, recovery and continuity			x

Some difficulties were experienced in sampling during the review, this was due to some areas being provided by third parties, and local election preparations. The review has also included areas of good practice and issues noted during the audit that fell outside of the sampling matrix which have also been included for consideration.

4. Findings, Recommendations and Action Plan

Consideration should be in respect of all the recommendations below not just in relation to the systems in scope, but also in relation to all council systems to provide an holistic control framework.

4.1 System owner risk assessments	**Risk Rating: High**
	Scope Area: A

Issue Identified

The Council demonstrated a control framework applied generically around IT systems, with criticality of its services for recovery purposes, controls that have been applied generically by the IT department, legality of the data held etc. It has not, however, yet completed formal risk assessments to fully assess the key risks, vulnerabilities and dependencies of these applications with the system owners.

Specific Risk

Failure to fully understand risk exposure may result in incomplete or ineffective controls to minimise the risk of disruption and may lead to extended recovery times in the event of a service disrupting incident.

Recommendation

To build upon the existing network control framework, the Council should consider a formal risk assessment of the possible threats to the systems, and the appropriateness of its current controls, recognising some systems may sit outside of the council's direct control framework. For example, the system data may not be included in the council backup regime, user account controls may be weaker than those for the Council's networks, unsupported software may be used in the architecture of third-party solutions, etc.

In addition, the Council should consider the development of guidance or an assessment proforma to aid the completion of the assessment of the systems, for example documenting expected controls for password strength, activity logging, maximum acceptable data loss, etc.

Such a development must dovetail in with, and expand upon, the existing risk management system. An example template of such a system risk assessment was shared with council staff with the draft version of this report, however other standards could be considered such as those provided by the National Cyber Security Centre guidance (NCSC).

Management Response (Remedial Action Agreed)

IT already house a System Asset Register which details all of the applications, servers and services used within the Council. This documentation includes system maintenance information including patch cycles, backup and recovery information and so on.

The IT service will extend their Asset Register to provide a level of governance for systems owned and administered outside of IT. It will be used to house any collected information.

The framework will comprise of guidance and processes that have to be undertaken by any systems owners.

This will include:-

- Change Management
- User Management
- System Risk Register
- System security verification.
- Backup and Recovery Processes

To ensure that System owners fully understand their responsibilities we will carry out workshops where we will discuss the standards being applied by IT, systems risk and so on. The System Register will then be updated appropriately

Responsibility for Action

IT Manager Development of Framework and Workshops

Risk assessments to be maintained by system owner

Deadline for Action

December 2019

4.2 Specific system recovery documentation and testing	**Risk Rating: Medium**
	Scope Area: I

Issue Identified

Although continuity arrangements are documented generically for the Council's network and recovery priorities in place, there was no system specific recovery documentation for the 'critical' applications or evidence of recovery tests specific to those systems.

Specific Risk

In the event of a full recovery event materialising, delays may be experienced in restoring services.

Recommendation

The council should consider development of specific recovery documentation for its 'critical' applications as part of its continuity and recovery plans, recognising any areas of third-party reliance.

Once these have been implemented, a rolling schedule of testing for these application plans should be considered to allow the provision of assurances and opportunities for lessons learnt.

The NCSC exercise in a box (https://www.ncsc.gov.uk/information/exercise-in-a-box) is a good reference of example for consideration in development of a testing regime.

Management Response (Remedial Action Agreed)

The current applications register and server data based records will be extended to support additional information.

A business continuity workshop is to be arranged where BC responsibilities will be explained and work relating to TPO, RPO etc will be undertaken. Where information cannot be obtained a this meeting, individual service workshops will be undertaken

Responsibility for Action

IT Manager

System Owners – Document own System requirement needs

Deadline for Action

December 2019

4.3 Third party assurances	**Risk Rating: Medium**
	Scope Area: D

Issue Identified

The Abavus system is hosted by a third party, whilst staff who were interviewed were happy with the contractual arrangements in place, it was not clear (in reference to recommendation 4.1) that there was a clear understanding of detail data stores of the application (although the system as used contains little confidential data).

Specific Risk

In the event of a full recovery event materialising, delays may be experienced in restoring services. Potential financial penalty under GDPR.

Recommendation

As a hosted system the council should consider how it gains ongoing assurances around the segregation and security of its data. Such considerations should be part of how wider assurances are gained where systems and process are hosted or delivered by third parties, for example continued certification to recognised standards, such as Cyber Essentials or from the ISO (International Organisation for Standardisation) series.

Management Response (Remedial Action Agreed)

As part of the new framework an annual process will be implemented to obtain details of security and certification against all applications. This will be an action for the system owners

to undertake, with information being collated within the IT Service within the IT service Asset /Application register

Responsibility for Action

IT Manager (collation and verification)

System Owners – obtaining certification etc

Deadline for Action

Complete Framework Deployment 2019

4.4 Local patching arrangements	Risk Rating: Medium
	Scope Area: F

Issue Identified

A local decision, to halt routine patching of the Elector8 election system and servers, by the technical team during election periods in order to minimise the chances of unintentional disruption being introduced to the platform, had not been endorsed by the system owner.

Specific Risk

There is a risk that system disruption, could be experienced from exploitation, potentially including issues regarding confidentiality and integrity, of known non critical vulnerabilities during such a period.

Recommendation

Whilst this decision can be part a reasonable risk based approach to managing this area, such decisions should be made in conjunction with, and approval of the system owners, to ensure organisational responsibility is maintained.

Management Response (Remedial Action Agreed)

The Change Management Process will be extended to include change being carried out on all systems not only those under direct IT control. The Process will include agreement requirements from all stakeholders, IT and Service Owners

We will look at how we may adopt our processes and tools to enable full change management across the organisation.

We will amend and have agreed the internal change management documentation for all System Owners to follow and make this part of the wider System Owner responsibility.

Responsibility for Action

IT Manager

Deadline for Action

A more developed process is now in place, completion of policies and FreshService procedures – December 2019

4.5 User account reviews	Risk Rating: Medium
	Scope Area: C

Issue Identified –

Although the IT team liaised with HR to ensure leavers were removed from the network, the council did not perform regular dormancy or privileged user reviews. The Elector 8 system has 15 user accounts 3 of which were generic access administrator accounts, and we were informed that one of the generic admin accounts is utilised by two members of IT staff.

Specific Risk

Increased risk of inappropriate system access. Lack of accountability should an issue arise.

Recommendation

A schedule of user account reviews should be introduced where system owners confirm the accounts and their associated privileges remain appropriate over time.

Additional consideration should be considered for an auto dormancy check where any network account not accessed in a defined time period (for example six months) is automatically suspended.

The Council should ensure that access to systems is via individual named accounts wherever possible. In the case of the issue reported with Elector8, the use of the generic admin account should be discontinued. If this is not possible, increased monitoring and alerting controls should investigated for this account.

Management Response (Remedial Action Agreed)

In line with Facilities already undertaken within the IT Service, we will extended our operating framework out to all System Owners.

We will look to develop at the minimum an automated service reminder for account verification to be undertaken and completed to ensure privileges are current. In the immediate term a reminder can be sent to all system admins to verify their service data.

We will also review our leavers process so System owners are notified of a user leaving when IT disable them from the network so they can also be removed them from individual systems.

Responsibility for Action –

IT will work to develop a process to assist in the works, by identifying and notifying services of Leavers

System Owners are responsible for their own system management

Deadline for Action –

Reminders – Monthly 1st of every month. immediate

December 2019 for assistive System

System Owners immediate

4.6 Formalisation of practice and provision of guidance	Risk Rating: Medium
	Scope Area: C, D, E, F, G, H

Issue Identified

In a number of areas and in the absence of specific system reviews, formal standards had not been agreed The majority of change control requests are dealt with via helpdesk requests to record authorisations, etc. However there was no formalised policy in this area and the helpdesk would not necessarily capture changes to systems not maintained by the IT department.

Specific Risk

Changes performed outside of an agreed change control standard for authorisation, testing and accountability, are more prone to introduce errors or system disruption.

Recommendation

Areas of practice should be formalised in procedure or policy, such as change control and testing expectations. Guidance regarding expected control requirements for 'critical' application systems should also be provided, for example activity log retention requirements.

Management Response (Remedial Action Agreed)

IT will develop a system ownership framework

It will build upon the framework currently in place within the IT Service. We will develop a system owner 'manual' detailing responsibilities

This will include:

- Change Management
- User Management
- System Risk Register
- System security verification.
- Backup and Recovery Processes

Responsibility for Action

IT Manager

Deadline for Action

December 2019

Appendix A: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken the review of the process, subject to the following limitations.

Internal control

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgement in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

The assessment of controls relating to the process is that at April 2019. Historic evaluation of effectiveness is not always relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Appendix B: Assurance Definitions and Risk Classifications

Guide to the audit assurance opinions	
Comprehensive	There is a sound system of controls designed to meet objectives, manage risks and controls are consistently applied in all the areas reviewed.
Substantial	There is a good system of controls and risks are managed. However, there are opportunities for improvement in the design or consistency of application that will assist in the achievement of objectives identified as being at risk in the areas reviewed.
Limited	Key controls exist to help achieve objectives and manage principle risks. However, there are opportunities for improvement in the overall control environment which would enhance the design and application of controls, thereby assisting the achievement of objectives identified as being at risk in the areas reviewed.
Minimal	The absence of basic key controls or the inconsistent application of key controls is so severe that the audit area is open to abuse or error. Risks to objectives are not being managed.

Risk Rating	Assessment Rationale
Critical	Control weakness that could have a significant impact upon, not only the system, function or process objectives but also the achievement of the organisation's objectives in relation to: • the efficient and effective use of resources • the safeguarding of assets • the preparation of reliable financial and operational information • compliance with laws and regulations.
High	Control weakness that has or is likely to have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall organisation objectives.
Medium	Control weakness that: • has a low impact on the achievement of the key system, function or process objectives; • has exposed the system, function or process to a key risk, however the likelihood of this risk occurring is low.
Low	Control weakness that does not impact upon the achievement of key system, function or process objectives; however implementation of the recommendation would improve overall control.

Review prepared on behalf of MIAA by

Name	P Grimes
Title	Senior Technology Risk Assurance Manager
☎	Paul.Grimes@miaa.nhs.uk

Acknowledgement and Further Information

MIAA would like to thank all staff for their co-operation and assistance in completing this review.

This report has been prepared as commissioned by the organisation, and is for your sole use. If you have any queries regarding this review please contact Tony Cobain.

MIAA would be grateful if you could complete a short survey using the link below to provide us with valuable feedback to support us in continuing to provide the best service to you.