Selby Area Internal Drainage board

Additional information re assertion 10 on the Annual Governance

In response to 'No' for assertion 10 on the Annual Governance statement, we enclose our IT provider and website designer's comments to this assertion. We meet many of the requirements and are making significant progress towards the rest. We will be working alongside the providers to move this from a No to a Yes.

IT providers comments on the Digital compliance –

Having reviewed the requirements relating to Assertion 10 – Digital and Data Compliance, my view is that both Boards are already in a strong position and have implemented the majority of the controls expected under the AGAR guidance.

It is possible that this area is receiving greater scrutiny from auditors this year following updates to the AGAR guidance and the increased emphasis being placed on digital governance, cyber security, records management and data protection. Given that the query has arisen during the Kyle audit, my assumption is that similar questions are likely to be raised across other Boards, including Selby Area IDB, and therefore it makes sense to review these requirements collectively rather than treat them as an isolated issue specific to Kyle.

It is also worth noting that many of the changes made to the Boards' IT arrangements over the last 12–18 months were implemented specifically to improve cyber governance, security, accountability and compliance. The transition towards our Cyber Secure SLA, which includes managed Microsoft 365 services, managed devices, stronger identity and access controls, and more formalised IT management, was undertaken proactively as we anticipated that public-sector and quasi-public-sector organisations would increasingly be expected to demonstrate higher standards of cyber security, data governance, records management and organisational accountability.

This trend is not limited to public-sector organisations. Many SMEs are now subject to increasing scrutiny from Professional Indemnity, Cyber and Business Insurers, who are increasingly expecting organisations to demonstrate appropriate cyber security, data protection and governance controls as part of the underwriting and renewal process.

In many respects, the requirements now being assessed under Assertion 10 align closely with the objectives of our Cyber Secure SLA and the wider governance improvements that have already been implemented across both Boards. This includes the move away from personal (BYOD) devices, adoption of managed devices, implementation of stronger identity and access controls, ongoing Cyber Essentials best-practice alignment, and a broader focus on governance, security and accountability.

For simplicity, I have summarised the key areas below.

1. Authority-Owned Email Accounts

AGAR expects public bodies to conduct business through authority-owned email domains rather than personal email accounts.

Current Position:

- Board email is hosted within Microsoft 365.

- Authority-owned domains are in place.
- Managed user accounts are used.
- This requirement is substantially met.

2. Data Retention and Freedom of Information Requirements

As a public authority, the Board should be able to retain and retrieve records if required for audit, governance, regulatory or Freedom of Information purposes.

Current Position:

- Microsoft 365 Business Premium provides the capability to implement retention policies across email, SharePoint, OneDrive and Teams.
- By default, we do not generally implement a specific long-term retention policy unless there is a defined business, regulatory or governance requirement to do so. Retention requirements vary considerably between organisations and can have wider implications for mailbox storage, SharePoint and OneDrive data growth, records management and overall data lifecycle management.
- For example, implementing a seven-year retention policy does not simply preserve important records; it can also prevent deleted content from being permanently removed during that retention period. As a result, emails and documents that users may have deleted can continue to be retained for compliance, governance and recovery purposes, with associated implications for storage utilisation and data management.
- For most commercial organisations, retention settings are therefore configured according to their individual operational, regulatory and governance requirements. Given the Boards' status as public authorities, it would be prudent to review the current configuration and determine whether a formal records retention policy should be adopted and enforced through Microsoft 365.
- Whilst AGAR does not prescribe a specific retention period, it would be prudent for the Boards to adopt a documented records retention policy and align Microsoft 365 retention settings accordingly. A minimum seven-year retention period for general correspondence and records would be consistent with common governance practice for public authorities, whilst certain governance records such as Board minutes, annual returns and statutory documents should be retained permanently.
- From a technical perspective, adapting the Microsoft 365 environment to support these requirements is not an issue and can be achieved through policy configuration within the existing Microsoft 365 Business Premium licensing.

3. Backup and Recovery of Records

Public bodies should be able to recover information in the event of accidental deletion, corruption or data loss.

Current Position:

- Selby Area IDB already benefits from Datto SaaS Protect backup for Microsoft 365 data.

- Kyle & Upper Ouse IDB does not currently have equivalent Microsoft 365 backup protection in place.
- Whilst this may appear excessive for a small number of users from a purely operational perspective, from a governance, compliance and records recovery standpoint I would recommend that this is addressed for any mailboxes actively in service.
- This would provide consistency between the Boards and strengthen the ability to recover historic records should they be required for audit, Freedom of Information requests, accidental deletion or other governance-related matters.

4. Website Compliance

Public authorities are expected to maintain websites that comply with public-sector requirements, including accessibility and publication obligations.

Areas to Review:

- Accessibility compliance (WCAG 2.2 AA).
- Accessibility Statement.
- Publication of governance documents, annual returns, meeting minutes, policies and other statutory information.
- Freedom of Information and Transparency Code requirements.

This is primarily a governance and website review exercise rather than an IT infrastructure issue.

5. GDPR and Data Protection

The Board must demonstrate that personal information is processed appropriately and securely.

Current Position:

- Microsoft 365 provides secure storage and access controls.
- Managed accounts and security controls are in place.
- Ongoing policy and governance reviews form part of the Cyber Essentials alignment process.

6. Security Controls

AGAR expects evidence that appropriate technical controls exist to protect Board information.

Current Position:

- Microsoft 365 Business Premium.
- Multi-factor authentication.
- Managed identities and access controls.
- Device and account security controls.
- Cyber security management through the Board's IT support arrangements.

- As part of the ongoing Cyber Essentials alignment programme, the Boards have transitioned away from the use of personal (BYOD) devices for routine business activities and towards managed devices under IT administration and control.

These areas align strongly with Cyber Essentials requirements and current cyber security best practice.

7. IT Policies and Governance

AGAR now specifically references the need for an IT policy governing the use of technology, systems and devices.

Current Position:

- This forms part of the wider governance review currently being undertaken.
- The move away from personal devices and towards managed devices supports this requirement and aligns with both Cyber Essentials and general public-sector best practice.
- Any remaining policy gaps can be addressed through the Cyber Essentials alignment process.

8. Cyber Essentials Alignment

Whilst Cyber Essentials certification is not specifically mandated by AGAR, it provides an excellent framework for demonstrating many of the controls being assessed under Assertion 10.

Current Position:

- The majority of the required controls are already in place.
- Both Boards have been aligned with, and are actively progressing towards, Cyber Essentials certification as part of the wider Cyber Secure SLA programme.
- Significant progress has already been made, including the adoption of managed Microsoft 365 services, multi-factor authentication, managed user accounts, controlled access to systems, and the move away from Bring Your Own Device (BYOD) and unsupported devices towards centrally managed and controlled devices operating under formal IT administration.
- The remaining work is largely focused on governance, documentation, policy review and final alignment activities rather than significant technical changes.
- Formal certification has not yet been completed, as a number of alignment activities are linked to the ongoing office relocation project. It is sensible to complete the office move and associated infrastructure changes before undertaking the final certification assessment.
- Cyber Essentials certification has previously been quoted for both Boards; however, formal approval to proceed with certification has not yet been provided. In light of the observations raised by the Internal Auditor, I believe it would be beneficial to revisit this. I will ask Mark to refresh the proposals for both Boards, as I believe completion of the accreditation process would provide strong independent evidence that the appropriate cyber security, governance and data management controls are in place.

- Whilst certification itself is not a requirement of AGAR, achieving the standard would, in my view, more than satisfy many of the digital governance and cyber security expectations now being raised by auditors.

Summary

Overall, I believe both Boards are in a strong position with respect to Assertion 10. The majority of the technical controls are already implemented through the existing managed service arrangements and Microsoft 365 platform. The remaining actions are primarily centred around reviewing retention settings, website compliance, policy documentation, backup arrangements for Kyle & Upper Ouse IDB, and completing the Cyber Essentials alignment process.

Importantly, the Boards have not arrived at this position by accident. Over the last 12–18 months, considerable effort has been made to move away from legacy and informal IT practices and towards a more structured, managed and secure operating model. The move away from personal devices, the adoption of managed Microsoft 365 services, stronger access controls, cyber security improvements and governance-focused IT management were all implemented with the expectation that public bodies would face increasing scrutiny around digital governance, cyber security and data management.

In many respects, the work currently being undertaken as part of the Cyber Essentials alignment programme directly supports the objectives of AGAR Assertion 10 and provides a structured framework for evidencing compliance with many of the digital governance, security and data management requirements now being assessed by auditors.

Given the observations raised during the Kyle audit, I believe completing the Cyber Essentials accreditation process for both Boards would provide a clear and independently verified demonstration that appropriate cyber security, governance and data management controls are in place. In my view, this would place both Boards in a very strong position when responding to future audit enquiries relating to Assertion 10.

I hope this provides sufficient context for responding to the Internal Auditor. However, I would be happy to undertake a more detailed review of any individual area if required.

Website Provider comments

This is our in house review/audit of assertion 10 and the controls/systems in place we have.

1.50 obviously relates to the website and we have undertaken a Accessibility Study Review and we are currently implementing suggested changes from the report.

Please use the table as you please, but it hopefully provides you with something that you can send to the internal auditor.

Criterion Ref	Description	Officers' Score	Evidence Available

	(Assertion 10 added to clarify data compliance, previously covered under Assertion 3) **Note: Assertion 10 will not appear on the AGAR until 2025-26** To warrant a positive response to this assertion, the authority needs to have taken the following actions:		
1.47	Email management - Every authority must have a generic email account hosted on an authority owned domain, for example clerk@abcparishcouncil.gov.uk or clerk@abcparishcouncil.org.uk rather than abcparishclerk@gmail.com or abcparishclerk@outlook.com for example. **Guidance points 5.117 to 5.120**	3	Emails to EA (submission of audit docs, for example) clearly demonstrate [redacted] domain in use
1.48	All smaller authorities (excluding parish meetings) must meet legal requirements for all existing websites regardless of what domain is being used.	2	Not covered in the guidance, uncertain what legal requirements are being referred to here. Is it just saying 'you must obey the law'?
1.49	All websites must meet the Web Content Accessibility Guidelines 2.2 AA and the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 (where applicable). **Guidance point 5.123**	1.5	Report received Feb 2026 and is available for inspection.
1.50	All websites must include published documentation as specified in the Freedom of Information Act 2000 and the Transparency code for smaller authorities (where applicable). **Guidance points 5.125 to 5.128**		Publication Scheme under Policy (SGW) Transparency Code (E&S IDB only) - Items listed in section Paragraph 10 are either published in every meeting bulletin (SGW) , Published in Elector' Rights notice (SGW), shown in the Membership section of Shire Group Website/Members' Code of Conduct under Policies or are not applicable. However *draft* minutes are not yet published in accordance with the code.
1.51	All smaller authorities, including parish meetings,		

	must follow both the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act (DPA) 2018. **Guidance point 5.124**		
1.52	All smaller authorities, including parish meetings, must process personal data with care and in line with the principles of data protection **Guidance point 5.124**		More of a general principle than a verifiable requirement
1.53	The DPA 2018 supplements the GDPR and classifies an authority as both a Data Controller and a Data Processor.		A general note more than a specific requirement All Board registered as Data Controllers with the Information Commissioner
1.54	All smaller authorities (excluding parish meetings) must also have an IT policy. This explains how everyone - clerks, members and other staff - should conduct authority business in a secure and legal way when using IT equipment and software. This relates to the use of authority-owned and personal equipment. **Guidance points 5.121 to 5.122 (later includes link to draft IT Policy as a start point)**		Nothing yet, but draft IT Policy is here as a start point: https://docs.google.com/document/d/1LS-2nTHt-c6mu58ijhEBuTYtzP2lFbrfnYxLm6CIduc/edit?tab=t.0#heading… MJ/CB discussed 19.12.25, requirements covered by JBA's own IT policy *(this policy applies to all individuals who use the Board's IT resources, including computers, networks, software, devices, data, and email accounts - Section 2. (Scope) in the draft IT policy)*