IJB Audit & Risk Committee 03.06.26
Agenda Item: 5.2.3
Purpose: For Decision

# Western Isles Integrated Joint Board

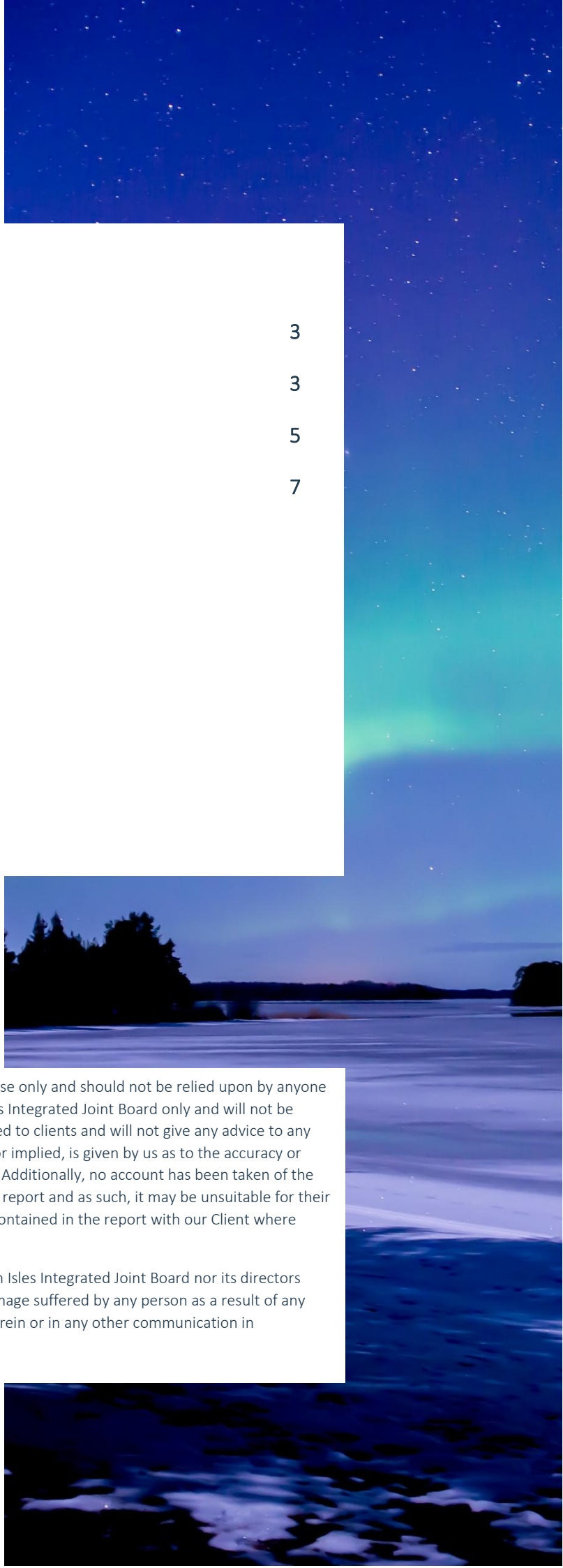
## Internal Audit Report 2025/26

## Cyber Security

May 2026

Review Sponsor: Emma Macsween, Interim Chief Officer

azets.co.uk



# Table of Contents




This report is intended for Western Isles Integrated Joint Board use only and should not be relied upon by anyone else for any purpose whatsoever. Azets is acting for Western Isles Integrated Joint Board only and will not be responsible to any other person for providing protections afforded to clients and will not give any advice to any recipient of this report. No representation or warranty, express or implied, is given by us as to the accuracy or completeness of the information and opinions contained herein. Additionally, no account has been taken of the needs of third party organisations in producing and agreeing this report and as such, it may be unsuitable for their purposes. Third parties should therefore verify the information contained in the report with our Client where necessary.

To the fullest extent permitted by law, neither Azets nor Western Isles Integrated Joint Board nor its directors shall be liable for any direct, indirect or consequential loss or damage suffered by any person as a result of any third parties relying on any information or opinions contained herein or in any other communication in connection with this report.

# Executive Summary

## Conclusion

Our review has identified that positive steps have been taken to address incident response and staff training risks.

Mandatory training has been issued to all Comhairle staff and there was an 85% completion rate at the time of our review. This training is also mandatory for all new starts.

In addition, a Cyber Incident Response Plan has been created and been subject to a review at a technical level by the IT team. It is planned to perform a wider, corporate exercise which will be beneficial to assess the effectiveness of the Plan in being able to support the response to a cyber incident.

Our review has identified areas where the IJB would benefit from assurance in relation to cyber security supply chain risk.

The Comhairle primarily uses procurement frameworks when procuring digital solutions. It has been assumed that the framework operators will have performed cyber security due diligence activity when appointing suppliers to the framework. This is not always the case.

The IJB should seek assurances that the Comhairle has validated that frameworks being used for procurement of digital solutions have performed appropriate cyber security due diligence on framework suppliers before they are used. Where this is not the case, the IJB should seek assurances that the Comhairle has applied its own cyber security due diligence processes prior to contract award.

The IJB should also seek assurances that formal and proportionate cyber security due diligence processes are established for the commissioning of care services or any other service which involves processing of data.

In addition, the IJB should seek assurances that the Comhairle has implemented formal processes for reviewing cyber security of key suppliers throughout the contract lifecycle. This should include affirmation that the supplier maintains and regularly tests their cyber incident response plans

# Background and scope

Western Isles Integrated Joint Board (the IJB) was negatively impacted by the cyber incident suffered by Comhairle nan Eilean Siar in November 2023. This has included an inability to produce annual accounts.

The Comhairle's Internal Audit report on lessons learnt from the cyber incident was reported to the Comhairle's Audit and Scrutiny Committee in November 2024. The Comhairle's Chief Internal Auditor produced follow-up reports to the 6 February and 1 May 2025 meetings of the Committee. The IJB was not engaged in the lessons learnt review.

In May 2025, we assessed what assurances the IJB could take from the lessons learnt reports and the subsequent follow-up reports. We highlighted risks that the IJB needed to address in future. The report from this review was presented to the IJB Audit & Risk Committee in November 2025.

### Scope

In accordance with the 2025/26 Internal Audit Plan, we performed a review of the IJB's progress in implementing recommendations from the report presented to the IJB Audit & Risk Committee meeting in November 2025.

The review also included a critical friend review of measures being implemented which allow the IJB to gain assurance that effective cyber security supply chain risk management is in place.

## Key Contacts and Audit Team

| Key Contacts | Audit Team |
|---|---|
| Emma Macsween, Interim Chief Officer | Paul Kelly, Head of Cyber Services |

## Acknowledgement

We would like to take this opportunity to thank all members of management and staff for the help, courtesy and co-operation extended to us during the year.

# Follow-up of 2024-25 cyber security audit

Our 2024-25 cyber security audit identified several risk areas covering the following areas:

- Financial reporting risk
- Cyber security supply chain management
- Incident response planning and lessons learned
- Staff training and awareness
- Updates on lessons learnt recommendations

Our follow-up work focused on incident response planning and lessons learned as well as staff training and awareness. The other two risk areas were identified as having been fully addressed or not applicable.

A wider, critical friend assessment on cyber security supply chain management has been provided in a separate section, below.

## Follow-up review results

We have set out, below, our assessment of progress made in addressing recommendations from our 2024-25 cyber security audit.

| Risk area: Incident response planning and lessons learned |
|---|
| *Recommendation* |
| The IJB should seek assurance from the Comhairle that they have appropriate cyber incident response plans and that these are tested at least annually. This will provide assurance that plans are capable of supporting the response to a cyber security incident. |
| *Management response* |
| Lessons learnt completed. All Business Continuity Plans include cyber incidents and the Health and Social Care Department within the Comhairle activated the necessary actions appropriately. BCPs are tested annually. Updates to cyber incidents aspects will be communicated and managed through CMT ahead of consideration by the Comhairle at the June 2025 series of meetings. |
| *Azets update (April 2026)* |
| It was stated that a tabletop exercise of the Cyber Incident Response Plan was performed by the Comhairle's IT team in late March 2026. This was purely a technical review of the Cyber Incident Response Plan. A formal plan to test the Cyber Incident Response Plan is not yet in place.<br><br>It was stated that there are discussions ongoing with Scottish Government contacts to facilitate a wider, corporate exercise of the Cyber Incident Response Plan. |
| *Action status: Partially complete* |
| The IJB should seek assurance that the Comhairle has performed a formal, corporate exercise of the Cyber Incident Response Plan. This will provide reassurance that the Plan is capable of supporting the response to a cyber incident and that key parties are aware of their roles and responsibilities. |

| Risk area: Staff training and awareness |
| --- |
| *Recommendation* |
| The IJB should seek assurances from the Comhairle on progress with developing and delivering mandatory cyber security training.<br><br>When the training is released, the IJB should request information on completion rates as well as information on results of any future phishing simulations. This will allow the IJB to confirm that the Comhairle is taking appropriate action to minimise behavioural cyber security risks. |
| *Management response* |
| Cyber training live and completion rates will be monitored and shared with CMT in June 25. Responsibility for compliance will sit with the Chief Officers for the service. |
| *Azets update (April 2026)* |
| Mandatory annual training has been issued to all staff. Completion status is reported to CMT monthly with any actions being devolved to Chief Officers to address within their respective areas of responsibility. When issued, staff have one year to complete the training. All new starts must complete mandatory training as part of induction.<br><br>At the time of our audit work, it was reported that 85% of staff had completed training. |
| *Action status: Complete* |

# Cyber Security Supply Chain Risk Management

Our 2024-25 report included the following recommendation for the IJB:

*"The IJB should request confirmation from the Comhairle that there are robust cyber security supply chain due diligence processes in place. This should primarily focus on those systems that represent highest risk to the IJB's processes.*

*This should include assurance that all system suppliers are subject to appropriate security due diligence as part of procurement processes and that the Comhairle has processes for gaining ongoing assurance that the system supplier maintains robust security.*

*Confirmation should also be sought that the supplier has current cyber incident response plans and that these are regularly tested to confirm they are effective. Assurances should also be sought to confirm that suppliers maintain appropriate and secure backups."*

Through our discussions, it was identified that there are no formal controls in place to identify, assess and manage cyber security risks associated with the use of key third parties – either through procurement of digital solutions or as part of wider commissioning of care services.

It was explained that, when procuring digital solutions, the IT team will primarily use recognised frameworks agreement. In doing so, it has been assumed that the framework operators undertake sufficient cyber security due diligence on all suppliers. As a result, assurance has not been sought to ascertain the extent of cyber security due diligence performed.

From our own experience in being appointed to public sector procurement frameworks, the level of cyber security due diligence performed on potential suppliers varies significantly. Some frameworks have extensive requirements whereas others do not perform any cyber security due diligence and expect this to be assessed during the buyer's procurement process.

Where a framework is not used to procure a digital solution, the Comhairle has a questionnaire which is based around the National Cyber Security Centre's Supply Chain Security principles. This would be completed by the supplier and assessed before a contract is awarded.

This is not applied for commissioning of care services.

We also noted that there are no processes in place to confirm that key suppliers maintain robust cyber security measures throughout the contract lifecycle.

### Recommendations

The IJB should request assurance from the Comhairle that:

- they have obtained assurance from framework providers that cyber security due diligence performed on appointed suppliers is aligned to the Comhairle's requirements;
- where gaps in cyber security due diligence are identified , the Comhairle includes specific cyber security requirements as part of the tender documentation;
- applies formal. proportionate cyber security due diligence for commissioning of care services any other service which involves processing of data; and

- formal processes are implemented for reviewing cyber security of key suppliers throughout the contract lifecycle. This should include affirmation that the supplier maintains and regularly tests their cyber incident response plans.

© Azets 2026.  All rights reserved.

Registered to carry on audit work in the UK and regulated for a range of investment business activities by the Institute of Chartered Accountants in England and Wales.