ITEM NUMBER: 9.1

CONFIDENTIAL REPORT

INTERNAL AUDIT – CYBER SECURITY REVIEW Report No: 420/20)

Pursuant to Section 90(2) of the Local Government Act 1999 the Report attached to this agenda and the accompanying documentation is delivered to the Council Members upon the basis that the Council consider the Report and the documents in confidence under Part 3 of the Act, specifically on the basis that Council will receive, discuss or consider:

e. matters affecting the security of the council, members or employees of the council, or council property, or the safety of any person.

Recommendation – Exclusion of the Public – Section 90(3)(e) Order

1 That pursuant to Section 90(2) of the *Local Government Act 1999* Council hereby orders that the public be excluded from attendance at this meeting with the exception of the Chief Executive Officer and Staff in attendance at the meeting in order to consider Report No: 9.1 Internal Audit – Cyber Security Review in confidence.

2. That in accordance with Section 90(3) of the *Local Government Act 1999* Council is satisfied that it is necessary that the public be excluded to consider the information contained in Report No: 9.1 Internal Audit – Cyber Security Review on the following grounds:

e. pursuant to Section 90(3)(e) of the Act, the information to be received, discussed or considered in relation to this Agenda Item is related to matters affecting the security of the Council.

3. The Council is satisfied, the principle that the meeting be conducted in a place open to the public, has been outweighed by the need to keep the information or discussion confidential.

Item No: **9.1**

Subject: **INTERNAL AUDIT – CYBER SECURITY REVIEW**

Date: 16 December 2020

Written By: General Manager, Strategy and Business Services

General Manager: Strategy and Business Services, Ms P Jackson

---

SUMMARY

In September 2020, Council's internal audit service provider, Galpins, conducted a review of cyber security for Council and Alwyndor. This has now been reviewed by Administration and finalised including agreed actions. The report is tabled for the Committee's consideration.

RECOMMENDATION

That the Audit Committee:

1. advises Council it has received and considered an internal audit report from Galpins on cyber security and notes the actions agreed; and

RETAIN IN CONFIDENCE - Section 91(7) Order

2. having considered Agenda Item 9.1 Internal Audit – Cyber Security Review in confidence under Section 90(2) and (3)(e) of the *Local Government Act 1999*, the Council, pursuant to section 91(7) of that Act orders that the report, attachments and minutes be retained in confidence for a period of 24 months and that the Chief Executive Officer is authorised to release the documents prior to that time if and when all parties to the contract have provided their consent.

COMMUNITY PLAN

A Place that Provides Value for Money

COUNCIL POLICY

Not Applicable.

STATUTORY PROVISIONS

Sec 122 Local Government Act.

BACKGROUND

As part of the agreed internal audit program, in September 2020 Galpins completed a review of Council and Alywndor's cyber security.

REPORT

The internal audit report has been reviewed by Administration, and actions have been agreed. The report is included as Attachment 1.

Refer Attachment 1

Administration has commenced actioning the findings from the audit. An action plan has been developed, including the status of each action. This plan will be tabled with the Audit Committee on a quarterly basis until the agreed actions are completed. The action plan is included as Attachment 2.

Refer Attachment 2

BUDGET

The costs incurred from the implementation of the agreed actions will be incorporated in existing budget.

LIFE CYCLE COSTS

This report does not have any direct full life cycle cost implications.

Galpins

Accountants, Auditors & Business Consultants

City of Holdfast Bay

Internal Audit Report – Cyber Security Review

September 2020

Mount Gambier
233 Commercial Street West
PO Box 246, Mount Gambier SA 5290
DX 29044
P: (08) 8725 3068
F: (08) 8724 9553
E: admin@galpins.com.au

Stirling
Unit 4, 3-5 Mount Barker Road
PO Box 727, Stirling SA 5152
P: (08) 8339 1255
F: (08) 8339 1266
E: stirling@galpins.com.au

Norwood
3 Kensington Road, Norwood SA 5067
PO Box 4067, Norwood South SA 5067
P: (08) 8332 3433
F: (08) 8332 3466
E: norwood@galpins.com.au

www.galpins.com.au

Table of contents

Document Control

Date	Revision Number	Revision Details	Author	Reviewer
21.09.2020	V1.0	Draft report	Jo Stewart-Rattray	Janna Burnham
1.10.2020	V.10	**Final** report	Jo Stewart-Rattray	Janna Burnham
4.12.2020	V2.0	CHB Response	Robert Zanin	Pamela Jackson

1. Executive Summary

1.1 Background

The 2020-21 Internal Audit Plan provides for a review of Council's cyber security activities. Cyber security is of increasing importance and has recently become prominent in the SA local government setting, after a large Council was subject to a ransomware attack. Cyber security attacks can have significant impacts on overall business continuity of an organisation, with implications for the security of sensitive data, communications and physical information technology infrastructure.

Local Government in South Australia does not have a mandated approach to cyber security. The South Australian Government, however, does have the mandated *SA Cyber Security Framework* (2019). This aligns with Australian Government principles and will be the basis used for auditing the CHB's approach to cyber security.

Internal audits of cyber security can enhance the ongoing internal culture of security. Council recently engaged an IT security company to conduct reviews of security arrangements at both Alwyndor Aged Care (Alwyndor) and the City of Holdfast Bay (CHB). Finalised in February 2020, these reviews predominantly included technical review, with three 'non-technical' elements covered – including risk assessment, security policies and security awareness training.

1.1 Objectives

The audit assessed the maturity of Council's (including both CHB's and Alwyndor's[1]) approach to cyber security across elements as outlined in the South Australian Cyber Security Framework (SACSF), which included:

Governance

- leadership, organisational and structure and staff responsibilities
- policies, practices, procedures and compliance (including a review of the Kaon model and suggestions for strengthening/improvement)
- risk management processes
- supplier management
- audit and assurance
- cyber security insurance coverage

Information

- information asset identification and classification
- vulnerability management
- administrative access
- incident management, response and recovery
- technology controls
- processes to ensure compliance with the Privacy Act 1988 (Cth), including mandatory data breach reporting requirements

Personnel

- education and awareness
- appropriate screening/ applicable code of conduct

[1] The term 'Council' is used within this report to describe the whole organisation – including the traditional Council operations and Alwyndor. To differentiate Alwyndor from the traditional administration, this report refers to Council's administration as 'CHB'.

Physical

- providing a safe and secure environment for people, information and assets.

Arrangements at both Alwyndor and the CHB were reviewed.

1.2 Relevant Strategic Risks

This audit aligns with Council's strategic risks including:

- Inability to respond and recover effectively from disruptive events.

1.3 Good Practices Observed

- ✓ The executive team demonstrated some awareness and willingness to further understand the issues that were observed during the audit, as well as a desire to remediate and create a more secure environment through the use of appropriate practices, tools and staff training and awareness activities.
- ✓ In addition, we understand that technology and security infrastructure and services at Alwyndor will be amalgamated with CHB and external specialist resources will be brought in to assist with the design and implementation, to ensure an appropriate architecture is developed.
- ✓ A number of audits and reviews appear to have been undertaken in recent times which assists with the assurance posture of the organisation.
- ✓ Reasonable physical security controls are in place. For example, visitors must be escorted on premises and IT equipment is stored within locked racks. This reduces the chance of opportunistic access to sensitive information and devices.

1.4 Key Findings and Recommendations

This internal audit engagement aimed to assess the controls established to address strategic risk *Inability to respond and recover effectively from disruptive events*. Based on the work undertaken, and when considering the design and/or effectiveness of controls collectively, we conclude that the control environment **Requires Significant Improvement.**[2]

We recognise that there have been numerous changes within the Information Technology (IT) Team over the past 18 months, which has contributed to the current need for strengthening the controls environment. However, with an understanding of the required technology, security capabilities and the subsequent recruitment of appropriate resources / outsourcing of some functions, Council can enhance the ability to significantly improve the effectiveness of its cyber security arrangements. We note that there were no findings in relation to the 'physical' security element of the SACSF.

[2] Please refer to Appendix 1, Overall Control Effectiveness Ratings for further information.

Findings are summarised below.

Finding	Recommendation	Audit Risk Rating[3] – CHB	Audit Risk Rating – Alwyndor	Client Risk Rating	Completion Date
GOVERNANCE					
2.1 A need to define required technology and security capabilities	**Recommendation 1:** Assess CHB and Alwyndor's existing technology and security capabilities to inform decision-making about the structure of the function (for example outsourcing, in-sourcing, co-sourcing). **Recommendation 2:** Develop an information security strategy, applicable to CHB and Alwyndor. This can address: • alignment with the organisation's overall strategic direction • governance/oversight mechanisms • approach to compliance with relevant laws and regulations • roles and responsibilities, including expectations in relation to external suppliers • monitoring and reporting, including audit and assurance requirements. Ensure this is approved by management and is made available to both employees and relevant external parties. **Recommendation 3:** Develop a process to ensure that all recommendations from reviews/audits in relation to information security capabilities are tracked and monitored. *Note: the majority of these reviews are conducted independent of the internal audit program.*	High	High		

[3] All risks are inherent and based on Council's Risk Matrix, please see Appendix 2 for details.

Finding	Recommendation	Audit Risk Rating[3] – CHB	Audit Risk Rating – Alwyndor	Client Risk Rating	Completion Date
2.2 Lack of approved IT/Security policy framework	**Recommendation 4:** Develop an IT/Security Policy Framework that is tailored to Council's needs. This can include, for example, policies in relation to: ▪ information security ▪ mobile devices and teleworking ▪ acceptable use of assets ▪ human resource screening ▪ asset management ▪ information classification ▪ supplier management ▪ media handling (e.g. use of portable media) ▪ access control. Due to the intent for Council (Alwyndor and CHB) to amalgamate core functions (including IT security), these policies could be developed to address the needs of both parties, with some requirements specific to their differing needs, as required. *Note – ISO27001/2 outlines relevant expected policies and control.*	High	Moderate		
2.3 Lack of technology/ information risk assessment	**Recommendation 5:** Conduct regular risk assessments within IT/information security functions. These should occur at least annually and when there is a significant change to the environment, for example with change of key suppliers.	High	Moderate		
2.4 Lack of escalation for security incidents within supplier relationships	**Recommendation 6:** Council to formalise its supplier relationship management. This can include: ▪ developing principles to assess supplier risk prior to engagement ▪ defining escalation points for cases when security incidents occur	High	High		

Finding	Recommendation	Audit Risk Rating[3] – CHB	Audit Risk Rating – Alwyndor	Client Risk Rating	Completion Date
	▪ developing expectations that suppliers agree to abide by relevant Council policies. In addition, CHB can work to formalise the arrangement in place with its existing technology provider (or re-approaching the market if appropriate and then formalising with the successful provider). Further guidance in relation to supplier management is included in ISO27002 *Information Technology Security Techniques Code of practice for information security controls*				
INFORMATION					
2.5 Lack of incident management response and recovery plans	**Recommendation 7:** Develop an Incident Management Framework that covers operations for the organisation, including both CHB and Alwyndor. **Recommendation 8:** Ensure that the Disaster Recovery Plans for the organisation are up to date and relevant. This includes: ▪ ensuring that a disaster recovery plan has been documented for CHB, and ▪ reviewing the Alwyndor plan and receiving input from the business to ensure that it is fit for purpose. **Recommendation 9:** CHB to investigate the use of a Mobile Device Management tool which will allow the remote wiping of devices should they become compromised, lost or stolen.	High	High		
2.6 Lack of information asset identification and classification	**Recommendation 10:** Develop an asset register to track technology assets across the organisation, including for both CHB and Alwyndor. **Recommendation 11:** Develop an Information Identification and Classification process, and use this to classify and protect Council's	High	Moderate		

Finding	Recommendation	Audit Risk Rating[3] – CHB	Audit Risk Rating – Alwyndor	Client Risk Rating	Completion Date
	data on a risk basis. For example, critical information can be subject to more rigorous protection than lower-value information.				
PERSONNEL					
2.7 A need to formalise cyber security training and security checks	**Recommendation 12:** Include IT and Information Security Components in Employee Induction Programs across the organisation. **Recommendation 13**: Conduct regular security awareness raising activities across the organisation. This process is ongoing and a reminder to staff about appropriate security practices. Examples may include 'cyber hygiene', awareness raising in relation to phishing and the appropriate security of devices.	Moderate	Low		
2.8 Lack of police checks for IT/Security staff	**Recommendation 14:** Establish a process for police checking IT/security staff at the CHB, with triggers to ensure re-review every three years.	High	N/A		

2. Detailed Findings and Recommendations

2.1 Governance: A need to define required technology and security capabilities	Audit Risk Rating - CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	High	High	

Key Findings

- There are five vacant positions within CHB's IT Team, and the 'Manager Innovation & Technology Services' role has an 'acting' status. This creates a lack of ability to consistently implement management approaches and practice in relation to security.
- Neither CHB nor Alwyndor have an existing governance model that defines segregation of duties.
- Alwyndor is heavily reliant upon a third-party service provider for most of its IT service, and there is a lack of clarity about the role of the two Alwyndor staff members on site who perform day-to-day IT activities.

Discussion

The audit scope called for a review of the maturity of Council's (including both CHB's and Alwyndor's) governance stance, in line with the SACSF. This included consideration in relation to leadership, organisational and structure and staff responsibilities.

A summary of results of analysis for the 'governance' element of the SACSF is outlined below, including information about findings and links to relevant recommendations.

SACSF element	Status – CHB	Status – Alwyndor	Discussion points
Leadership, organisa-tional and structure and staff responsibili ties	Ineffective [4]	Ineffective	There is a need to: • understand required technology and security capabilities in order to inform decision about internal staffing and/or outsourcing model • define governance model, including segregation of duties • define IT roles and responsibilities at Alwyndor. See **Recommendation 1** and **Recommendation 2.**
Policies, processes, procedures and compliance (including a review of	Ineffective	Requires Significant Improve-ment	Alwyndor has established draft policies, these require tailoring to the organisation's needs. Council has purchased template policies from 'Kaon' vendor, these include headings and lack detail relevant to Council's needs. There is a need to develop and implement policies and procedures to guide technology and security practices

[4] For consistency, controls in relation to each SACSF element were rated in line with the framework included in Appendix 1.

SACSF element	Status – CHB	Status – Alwyndor	Discussion points
Kaon model)			across CHB (including Alwyndor). See **Recommendation 4** in Section 2.2**.**
Risk manage-ment processes	Ineffective	Requires Significant Improve-ment	Council and Alwyndor have a documented risk management framework/approach, however Audit understand that technology and security risk assessments are not consistently undertaken. There is a need to implement an IT/security risk management process. See **Recommendation 5** in Section 2.3.
Supplier manage-ment	Ineffective	Ineffective	• Opportunity to strengthen supplier management processes. For example: o principles to assess supplier risk prior to engagement o with defined escalation points for if a security incidents occur o with suppliers agreeing to abide by relevant Council policies See **Recommendation 6** in Section 2.4. Further guidance in relation to this is included in ISO27002 *Information Technology Security Techniques Code of practice for information security controls.*
Audit and assurance	Ineffective	Ineffective	Council and Alwyndor have commissioned relevant audits, for example a Network Assessment Report (February 2020). Audit identified a lack of transparent and consistent implementation of audit recommendations. See **Recommendation 3.**
Cyber security insurance coverage	Ineffective	Ineffective	Council has an insurance policy in place, that offers 'cyber security and privacy protection'. Internal Audit identified a lack of assurance that a claim would be paid in case of an incident. Insurers would require evidence that reasonable steps had been taken to ensure compliance with relevant information security frameworks (for example SASCF, NIST[5] Cybersecurity Framework, COBIT,[6] ISO27001/2).

[5] National Institute of Standards and Technology

[6] Control Objectives for Information and Related Technologies framework for IT management and governance.

SACSF element	Status – CHB	Status – Alwyndor	Discussion points
			No specific recommendation is raised in relation to this finding, as a whole this report's recommendations aim to strengthen Council's information security posture.

Risk Exposure

- Continuity of IT leadership is not assured, this creates a lack of ability to consistently implement management approaches and practice in relation to security.
- A lack of understanding of required technology and information security capabilities can lead to poor decision making and inability to structure the function appropriately.

Recommendation 1	Assess CHB and Alwyndor's existing technology and security capabilities to inform decision-making about the structure of the function (for example outsourcing, in-sourcing, co-sourcing).
Agreed Actions	Finalise vacant positions: • Manager Innovation & Technology Services appointed 3 Aug 2020 • Team Leader Technology Operations appointed 2 Nov 2020 Define leadership, organisational structure across both CHB and Alwyndor Define internal staff capabilities/responsibilities across both CHB and Alwyndor and mitigate internal gaps by procuring external resources. Note CHB and Alwyndor have gone to the market (closed 20 Nov 2020) to tender for the Provision of Information Technology Specialist Services for a period of three (3) years in the following categories: • Enterprise Architecture Services • Application Portfolio Management Services • Solution Architecture Services • Advisory Services • Essential Platform Services • Change Delivery Services
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	• Provision of Information Technology Specialist Services – Tender closes 20 Nov 2020 with a contact commencement 11 Jan 2021 • Define leadership, organisational structure across both CHB and Alwyndor – 29 Jan 2021 • Define internal staff capabilities/responsibilities across both CHB and Alwyndor- 29 Jan 2021

	• Augment internal gaps by procuring external resources – 26 Mar 2021

Recommendation 2	Develop an information security strategy, applicable to CHB and Alwyndor. This can address: • alignment with the organisation's overall strategic direction • governance/oversight mechanisms • approach to compliance with relevant laws and regulations • roles and responsibilities, including expectations in relation to external suppliers • monitoring and reporting, including audit and assurance requirements. Ensure this is approved by management and is made available to both employees and relevant external parties.
Agreed actions	Develop an approved information security strategy model for both CHB and Alwyndor that: • Assess the security requirements • Performs a gap analysis • Prioritises initiatives and build a security roadmap • Plans for the transition • Executes and maintain
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	25 Jun 2021

Recommendation 3	Develop a process to ensure that all recommendations from reviews/audits in relation to information security capabilities are tracked and monitored. *Note: the majority of these reviews are conducted independent of the internal audit program.*
Agreed Actions	Developed and implement a process to • Commission an internal Cyber Security panel • Record security reviews and audit recommendations • Analyse the recommendations • Document the agreed actions including responsible person(s) and completion date/time • Review agreed actions to ensure recommendations are mitigated
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	26 Mar 2021

2.2 Governance: Lack of approved IT/Security policy framework	Audit Risk Rating - CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	High	Moderate	

Key Findings

- CHB has a lack of relevant policies related to information security, existing policies are outdated and cover appropriate electronic communication and IT resource use only.
- There is no framework of policies and procedures to act as a guide for IT and security staff in relation to their roles.
- CHB has paid for a policy framework from the vendor Kaon. These policies are of a template nature, and need to be tailored to the specific requirements of the CHB.
- Alwyndor has a range of draft policies, however these have not been approved or distributed to staff as part of the implementation process.

Discussion

The audit scope called for a review of Council's approach to governance, in line with the SACSF, policies, procedures and compliance (including a review of the Kaon model and suggestions for strengthening/improvement). Please see the summary table in Section 2.1, for further detail.

Audit's review of policies and procedures in place identified a significant lack of policies in relation to information security:

- Within Council: two policies were in place, for example an Electronic Communication Policy (2014) and IT Resources Policy (2009). The IT Resources Policy in particular includes a lack of detail about expected and appropriate use of equipment, in line with information security requirements.
- Council has purchased a range of policies from the vendor 'Kaon'. Audit found that these are of a template nature and require significant alteration. For example, the policies included subject headings and generic text underneath for Council to tailor to ensure relevance.
- Alwyndor has a range of draft policies, these have not been finalised, approved or distributed to staff as part of the implementation process.

Risk Exposure

- Inability to articulate a consistent message to all staff and third parties in relation to their responsibilities, for the security of the information that they may handle, create, process, store or transmit for and on behalf of CBH or Alwyndor.

Recommendation 4	Develop IT/Security Policy Framework that is tailored to Council's needs. This can include, for example, policies in relation to: ▪ information security ▪ mobile devices and teleworking

	▪ acceptable use of assets ▪ human resource screening ▪ asset management ▪ information classification ▪ supplier management ▪ media handling (eg use of portable media) ▪ access control. Due to the intent for Council (Alwyndor and CHB) to amalgamate core functions (including IT security), these policies could be developed to address the needs of both parties, with some requirements specific to their differing needs, as required. *Note – ISO27001/2 outlines relevant expected policies and control.*
Agreed Actions	Develop standard policies to cover the following areas for both CHB and Alwyndor: • information security • mobile devices and teleworking • acceptable use of assets • human resource screening • asset management • information classification • supplier management • media handling (eg use of portable media) • access control Develop an approval process with Senior leadership Team. Develop an approved review process.
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	30 Apr 2021

2.3 Governance: Lack of technology/ information risk assessment	Audit Risk Rating - CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	High	Moderate	

Key Findings

- Alwyndor has a documented risk management plan, however it does not indicate how (or if) it should be used for managing IT/security risks. A single paragraph in its Information Security Policy that states that security risks are identified through risk assessments, however no further detail is provided.
- A broad strategic risk workshop was recently undertaken for CHB and Alwyndor, however no operational risk assessment is performed and documented within the IT and Security functions at CHB and Alwyndor.

Discussion

The audit scope called for a review of risk management processes as part of the 'governance' element of the SACSF. Results are summarised in the table in Section 2.1.

Internal Audit understand that a current strategic risk assessment is in place for Council (including Alwyndor). ISO27001/27002 further outline expectations in relation to risk assessments for information security. These are relevant to Council. The Standard outlines that relevant risk assessments help to ensure that information security can achieve its outcomes, that actions are planned to address risks and opportunities and that actions are integrated and implemented into information security management processes, as well as evaluated for effectiveness.

Information security risk assessments can be used to identify major information security risks, ensure a consistent approach to analysing potential severity and to plan treatment of these risks. Without these risk assessments, the approach to managing risks may be ad-hoc, inconsistent and incomplete. For example, some potential risks may not be identified or treated by operational staff.

Risk Exposure

- Lack of assessment of the realistic likelihood and potential consequences of risks in relation to cyber security may mean that insufficient action is taken to protect the information security of CHB and Alwyndor.
- There can be potential for IT/security risks to fall outside the organisational risk tolerance if they are not actively managed and treated.

Recommendation 5	Conduct regular risk assessments within IT/information security functions. These should occur at least annually and when there is a significant change to the environment, for example with change of key suppliers.
Agreed Actions	Develop an approved periodic risk assessment process covering the following: • Information Security Policies • Information security roles and responsibilities

	• Terms and conditions of employment • Asset management • Access control • Cryptography • Operations Security • Communications security • System acquisition, development and maintenance • Suppliers relationships • Information security incident management • Information security aspects of business continuity management • Privacy and protection of personally identifiable information • Vulnerability assessments • Penetration assessments • Friendly phishing
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	25 Jun 2021

2.4 Governance: Lack of escalation for security incidents within supplier relationships	Audit Risk Rating - CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	High	High	

Key Findings

- Alwyndor's agreement with its technology/security supplier does not currently define an escalation process if a security incident occurs. It includes a broad point that 'serious or difficult matters' will be escalated to senior staff.
- CHB does not have a contractual arrangement in place with its technology/security service providers. These providers are used on an ad-hoc basis, however the agreement requires formalisation.
- Due to the lack of approved CHB and/or Alwyndor policies and procedures, suppliers do not have any written documentation to abide by, which can leave the organisation exposed to misconduct by suppliers because there is no guidance in relation to the organisation's security requirements.

Discussion

The audit scope called for a review of supplier management practices, as part of the 'governance' principle of the SACSF.

Audit identified:

- CHB does not have a contractual agreement in place with its technology/security provider. It was reported that the provider is largely used for ad hoc services. Audit considers that expectations need to be defined, including Service Level Agreements that include response times and escalation points where relevant to problems and security incidents.
- Alwyndor has a Support Agreement in place with its supplier. This includes a section that indicates response times and severity levels, with a point that the provider will 'operat[e] to formal Service Level Agreements, guaranteeing service response times and overall performance'. SLAs do not include escalation procedures in case of security incidents. Incidents may vary greatly in their criticality and therefore the approach to managing these can also vary. Clarity of expectations in this area is important to ensure that CHB/Alwyndor have appropriate understanding, oversight and ability to manage any incident that arises.

There is opportunity to update and define expected roles and responsibilities in relation to suppliers. This is in line with better practice and is an integral part of cyber security practices. For example, define:

- principles to assess supplier risk prior to engagement
- defined escalation points for cases when security incidents occur
- expectations that suppliers agree to abide by relevant Council policies.

Further guidance in relation to supplier management is included in ISO27002 *Information Technology Security Techniques Code of practice for information security controls.* See **Recommendation 6**.

Risk Exposure

- Lack of appropriate protection of information assets accessed by suppliers, due to a lack of clear and documented agreements in relation to appropriate information use.
- Potential risks created by the use of a third-party provider is not currently assessed prior to engagement of new suppliers.
- CHB and/or Alwyndor may not be aware of the procedure to follow in security incidents if there are no escalation paths written into SLAs, which may lead to reputational risk and operational delays.

Recommendation 6	Council (including Alwyndor) to formalise supplier relationship management. This can include: ▪ developing principles to assess supplier risk prior to engagement ▪ defining escalation points for cases when security incidents occur ▪ developing expectations that suppliers agree to abide by relevant Council policies In addition, CHB can work to formalise the arrangement in place with its existing technology provider (or re-approaching the market if appropriate and then formalising with the successful provider). Further guidance in relation to supplier management is included in ISO27002 *Information Technology Security Techniques Code of practice for information security controls*
Agreed Actions	Develop and implement an approved policies and procedures to protect the organisation's systems and information that is accessible to ICT outsourcers and other external suppliers. Process to be applied to current and future providers involves: • Risk assessment • Screen and auditing • Selecting clauses in agreements based on above • Access control • Compliance monitoring • Termination of the agreement Service delivery by external suppliers to be monitored and reviewed/audited against the contracts/agreements and including service changes.
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	26 Feb 2021

2.5 Information: Lack of Incident management response and recovery plans	Audit Risk Rating - CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	High	High	

Key Findings

- There is no 'incident management response plan' in place at CHB. Alwyndor has a draft Security Incident Processing document, however it has not been approved or implemented.
- There is no formalised reporting or escalation of potential security incidents, other than to log a ticket with the Service Desk.

Discussion

The audit scope called for a review of incident management, response and recovery.

A summary of results of analysis for the 'information' element of the SACSF is included below, including information about findings and links to relevant recommendations.

SACSF Element[7]	Status – CHB	Status – Alwyndor	Findings
Information asset identification and classification	Ineffective	Ineffective	A need to implement a process to identify and classify information assets. For example, understand all information assets and also have guidance about how to classify this information. Please see **Recommendation 11** in Section 2.6.
Vulnerability management	Majority effective	Majority effective	Council provided evidence that vulnerability assessments have been conducted, however Internal Audit identified a lack of action to implement recommendations. See **Recommendation 3**.
Administrative access[8]	Ineffective	Ineffective	Within Council: Audit identified a segregation of duties issue as the ICT Infrastructure Lead has responsibilities for both systems access/ administration and system security – including firewalls/endpoints/ IT security processes. See Section 2.6. Alwyndor: there is reliance on outsourced service providers for providing administrative access. Alwyndor has a lack of understanding/oversight of service provider's actions in this space. See Section 2.6.
Incident management, response and	Ineffective	Partially effective	Council does not have specific security incident response plans in place. Alwyndor has a draft plan in place, and broad points about escalation within its contract with its supplier. Further discussion is

[7] Note – SACSF elements in relation to cloud computing, robust ICT systems and operations (used in relation to vulnerability assessment), secure software development were identified as not relevant to Council/Alwyndor.

[8] Responsible for example for creating accounts, deleting accounts, changing user system access.

SACSF Element[7]	Status – CHB	Status – Alwyndor	Findings
recovery (resilience)			included below this table. Also see **Recommendation 7**. No formalised reporting process to track incident or to escalate potential security incidents, other than to log a ticket with the Service Desk. Staff have not been educated as to what may constitute an incident, nor have IT/security staff been educated in relation to handling an incident that may require law enforcement assistance (for example, in relation to ransomware). Alwyndor has a disaster recovery plan (part of BCP) however Audit identified that it had not had input from the wider Alwyndor business. There is opportunity to confirm this plan's relevance. CHB is currently revising its disaster recovery plan. See **Recommendation 8.**
Teleworking	Ineffective	Ineffective	Working from home is permitted and at CHB connection is via a secure Citrix session. At Alwyndor connection to the corporate network is via a Virtual Private Network (VPN) connection. Strengthened policy requirements are required to explain appropriate device usage, policy in relation to the printing and secure disposing of material. See **Recommendation 4**.
Mobile Device Management	Ineffective	Majority Effective	CHB does not use Mobile Device Management (MDM) tools, whilst Alwyndor uses a recognised MDM tool which is oversighted by the service provider. See **Recommendation 9**.
System and Software Acquisition	Effective	Effective	Software is procured via an approval process (following Procurement guidelines). Users do not have local administration rights on their machines and therefore they are unable to load software. This is the same for both CHB and Alwyndor.
Compliance with the Privacy Act 1988 (Cth), including mandatory data breach reporting requirements	Ineffective	Ineffective	Carefully consider differing Alwyndor and CHB information security requirements (*Privacy Act 1988*). For example, resident information at Alwyndor may be subject to greater privacy requirements than general CHB information. See **Recommendation 11** in relation to information classification.

Risk Exposure

- An unclear approach to the management of technology and security incidents, may lead to gaps, inconsistent or ineffective approaches to addressing these incidents.
- Incidents may go undetected without appropriate monitoring and detection protocols for periods of time, that may enable a more significant cyber-attack.
- Potential destruction of forensic evidence through lack of education for staff.
- The Disaster Recovery Plan has not been finalised, which could lead to unreasonable recovery times from a security incident or a significant system outage.
- A data breach (incident) may not be identified within the timeframe specified under the Notifiable Data Breach Scheme.

Recommendation 7	Develop an Incident Management Framework that covers operations for Council, including both CHB and Alwyndor.
Agreed Actions	Develop and implement an approved incident management framework and workflow incorporating the following steps: 1. Preparation 2. Detection and reporting 3. Triage and analysis 4. Containment and neutralisation 5. Post-incident activity
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	26 Mar 2021

Recommendation 8	Ensure that the Disaster Recovery Plans for the organisation are up to date and relevant. This includes: ▪ ensuring that a disaster recovery plan has been documented for CHB, and ▪ reviewing the Alwyndor plan and receiving input from the business to ensure that it is fit for purpose.
Agreed Actions	CHB • Complete update of the Disaster Recovery Plan Alwyndor • Complete update of the Disaster Recovery Plan to include any comments from the business
Action Officer	Manager Innovation & Technology and Team Leader Technology Operations

Completion Date	CHB – 01 Dec 2020 Alwyndor – 01 Feb 2021

Recommendation 9	CHB to investigate the use of a Mobile Device Management tool which will allow the remote wiping of devices should they become compromised, lost or stolen.
Agreed Actions	CHB currently utilises Microsoft Intune Mobile Device Management (MDM) for Elected Members iPads and Depot field workers tablets. Expand the utilisation the MDM to include all laptops, CHB/Alwyndor issued mobile phones and BYOD where staff request access to CHB and Alwyndor systems. Enable Two Factor Authentication Develop and Authorise a Mobile Device Policy
Action Officer	Team Leader Technology Operations
Completion Date	29 Jan 2021

2.6 Information: Lack of information asset identification and classification	Audit Risk Rating - CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	High	Moderate	

Key Findings

- The 'ICT Infrastructure Lead' position within CHB has responsibility for both systems access/ administration and system security, which creates a lack of segregation of duties and can be a potential conflict of interest.
- There is no 'Technology Asset Register' or 'technology inventory' within CHB. A corporate asset register exists, however only contains those assets with a value in excess of $250,000. There is a need to track technology assets and the information that they can access.
- CHB does not have an information classification guidelines in place. Alwyndor has a draft Data Classification document, however it has not been approved or implemented. Information Classification is very briefly mentioned in its Information Security Policy which has not been approved either.

Discussion

The audit scope called for a review of the 'information' element of the SACSF. A summary of results is included in Section 2.5.

In assessing the 'information and classification' element of the SACSF, Internal Audit sought to understand the organisation's approach to both understanding physical IT assets, including protection, as well as the approach to classifying information assets.

Identifying and assessing assets

It is important to identify physical technology assets, because these typically provide users with access to sensitive organisational information. There is a need to ensure that these devices have appropriate controls and only provide access to the information that users need to perform their job role or function.

Internal Audit identified that there is no 'Technology Asset Register' or 'inventory' within CHB, except for some information held in the Service Desk system in relation. A corporate asset register exists, however only contains those assets with a value in excess of $250,000.

Physical assets may not be financially valuable, however it is important to track them (what they are, where they are and who has them) because they can be used to access a range of sensitive information. See **Recommendation 8**.

Information Classification of Information Assets

Information is increasingly recognised as a key asset of any organisation. Therefore, it is important to understand the information assets held. Information is also subject to a range of requirements, for example in relation to privacy, disclosure and classification.

Identification of information assets then enables the organisation to determine criticality and sensitivity of that information to the organisation. It also enables the organisation to classify the information accordingly (for example, commercial in confidence, sensitive, critical). The classification of information can be considered in the context of consequences if information leakage occurs.

Council (including CHB and Alwyndor) do not currently formally classify information. There is some understanding of confidentiality requirements, for example in relation to resident information, however there is not a documented classification framework/approach in place. There is a need to carefully consider the differing classification and broader information security requirements of both parts of the organisation. See **Recommendation 12**.

Risk Exposure

- Lack of clarity in relation to custodianship of technology assets, can create instances where technology with access to sensitive information may not be adequately managed and controlled.
- Lack of segregation of duties caused by insufficient staffing levels open the organisation to the risk of unauthorised access or unintentional modification or misuse of information assets.
- As a result of a lack of understanding of how such information should be handled, critical or sensitive information could be inadvertently disclosed.

Recommendation 10	Develop an asset register to track technology assets across the organisation, including for CHB and Alwyndor.
Agreed Actions	Implement an automated network inventory, discovery and asset management tool that gathers hardware and software information of computers and other devices on a computer network for management, compliance and audit purposes for both CHB and Alwyndor.
Action Officer	Team Leader Technology Operations
Completion Date	CHB - 29 Jan 2021 Alwyndor – 26 Feb 2021

Recommendation 11	Develop an Information Identification and Classification process and use this to classify and protect both CHB and Alwyndor data on a risk basis. For example, critical information can be subject to more rigorous protection than lower-value information.
Agreed Actions	Complete stage 2 of the Information Management Change Program (incorporating Alwyndor as an additional stakeholder).
Action Officer	Manager Innovation & Technology Services
Completion Date	30 June 2021

2.7 Personnel: a need to formalise cyber security training and security checks	Audit Risk Rating - CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	Moderate	Low	

Key Findings

- Neither CHB nor Alwyndor have formal inclusion of information security in their induction processes. However, Alwyndor is working to incorporate security awareness within its Health and Safety induction information.
- CHB staff reported some provision of technology briefings for new starters as part of induction, however this is ad hoc in nature and could benefit from being tailored to the needs of various roles.

Discussion

The audit scope called for a review of the maturity of security training and awareness activities of which induction is usually the first connection employees have with the organisation's approach to security and technology.

A summary of results of analysis for the 'personnel' element of the SACSF is included below, including information about findings and links to relevant recommendations.

SA Cyber Security Framework Element	Status – CHB	Status – Alwyndor	Findings
Education and awareness	Partially Effective	Effective	Alwyndor has a staff member that has taken an interest (informal and in addition to her role description) in promoting education and awareness. CHB has provided some recent security awareness training, however the process appears to be undocumented and ad-hoc. There is opportunity to: • Implement an induction program covering IT and security, tailored to needs of role types. See **Recommendation 12.** • Regularly schedule and conduct security awareness training. See **Recommendation 13.**
Appropriate screening/ applicable code of conduct	Partially Effective	Effective	There is a need at CHB to classify IT roles as 'prescribed' and obtain appropriate police checks. See **Recommendation 14.**

Risk Exposure

- New staff and contractors (and third parties, if relevant) may not be aware of their responsibilities (including personal accountability) in relation to information security or controls in place to protect information assets from misuse or attack.
- Lack of awareness of current scams could lead to the release of confidential information, credentials, passwords or financial information all of which could lead to a significant cyber-attacks or data breaches.

Recommendation 12	Include IT and Information Security components in Employee Induction Programs across the organisation.
Agreed Actions	Update the ICT induction process for both CHB and Alwyndor to include the following topics: • Information and Communication Technology Security • Cyber security incorporating Scam and phishing emails • Acceptable Use of Information and Communication Technology • Use of email, internet and social media • Information Management Records
Action Officer	Team Leader Technology Operations
Completion Date	29 Jan 2021

Recommendation 13	Conduct regular security awareness raising activities across the organisation. This process is ongoing and a reminder to staff about appropriate security practices. Examples may include 'cyber hygiene', awareness raising in relation to phishing and the appropriate security of devices.
Agreed Actions	Utilise the LGRS Be Security Smart Program that consists of a set of information security videos covering issues that confront organisations and users every day. The program consists of the following 20 videos: • Episode 01 - Introduction to Information Security • Episode 02 - Protecting Your Identity • Episode 03 - Passwords • Episode 04 - BYO Devices • Episode 05 - Safe Internet Use • Episode 06 - Email Security and You • Episode 07 - Scams and Social Engineering • Episode 08 - Security in The Workplace

	• Episode 09 - Information Security At Home • Episode 10 – Handling Sensitive Information • Episode 11 – Mobile Phones and Tablets • Episode 12 – Laptop Security • Episode 13 – Security Incidents • Episode 14 – Social Media • Episode 15 - Protecting Credit Card Information • Episode 16 - Personal Information • Episode 17 - Cloud Security • Episode 18 – Situational Awareness • Episode 19 – WiFi • Episode 20 – Information Classification and Labelling
Action Officer	Manager Innovation & Technology Services and Team Leader Technology Operations
Completion Date	25 Jun 2021

2.8 Lack of police checks for IT/Security staff at CHB	Audit Risk Rating- CHB	Audit Risk Rating - Alwyndor	Client Risk Rating
	High	N/a	

Key Findings

- IT roles are not seen as 'prescribed' roles hence no police checks are undertaken for IT/security staff at CHB.
- All staff at Alwyndor are required to have a clearance via the SA Department of Human Services (DHS).

Discussion

The audit scope called for a review of the appropriateness of screening practices for employees.

Audit identified that, for CHB staff, IT roles are not seen as 'prescribed' and no police checks are undertaken for these roles. The SACSF (and all leading practice cyber security frameworks) calls for appropriate security screening of these roles, as they hold positions of trust and access to sensitive and valuable information.

All Alwyndor staff are required to have a clearance via the SA DHS, Audit did not test any instances of these clearances being in place but understand that this is a mandatory process.

Risk Exposure

- IT/security staff are typically in a position of trust and have privileged levels of access to systems and information that can be critical and sensitive in nature. Without appropriate screening it is possible to employ an individual into a trusted role, who may have a record of fraudulent behaviour.

Recommendation 14	Establish a process for police checking IT/security staff at the CHB, with triggers to ensure re-review every three years.
Agreed Actions	All new employees and contractors appointed to the City of Holdfast Bay, who access to systems and information that can be critical and sensitive in nature will now be required to undertake DHS Vulnerable Persons screen test. DHS Vulnerable Persons screen test to be reviewed every three years. All current employees who access to systems and information that can be critical and sensitive in nature will now be required to undertake DHS Vulnerable Persons screen test. DHS Vulnerable Persons screen test to be reviewed every three years. All current contractors appointed to the City of Holdfast Bay, who access to systems and information that can be critical and sensitive in nature will now be required to provide DHS Vulnerable Persons screen test.

Action Officer	Manager Innovation & Technology Services and Manager People and Culture
Completion Date	01 Dec 2020

Galpins

Accountants, Auditors & Business Consultants

Appendices

Appendix 1. Control Environment Conclusion Rating Definitions

This internal audit project aimed to assess the controls established to address a key strategic risk or risks in relation to cyber security. The following table provides definition of the ratings used to assess the control environment. These assessments are made based on the work undertaken, and when considering the design and/or effectiveness of controls collectively.

For consistency, controls in place to address each element of the SACSF were also rated using the table below.

Rating	**Effective**	**Majority Effective**	**Partially Effective**	**Requires Significant Improvement**	**Ineffective**
Definition	Controls assessed were effective in mitigating the key strategic risk or risks	Controls assessed were largely effective in mitigating the key strategic risk or risks	Controls assessed were partially effective in mitigating the key strategic risk or risks	Controls assessed require significant improvement to mitigate the key strategic risk or risks	Controls assessed were ineffective in mitigating the key strategic risk or risks

Appendix 2. Risk Framework

The method of risk assessment used in this audit is based on the Better Practice Model issued by the Local Government Financial Management Group and the Local Government Association.

It measures the likelihood of each risk occurring and the consequence of the risk event. From this analysis it is then possible to determine the level of inherent risk (risk without any controls in place) and residual risk (risks when controls are in place). This method of analysis is not an exact science and quite subjective, but it is of value as an indicator and therefore assists in assessing audit risks.

Consequence / Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	E	Moderate	High	High	Extreme	Extreme
Likely	D	Low	Moderate	High	Extreme	Extreme
Possible	C	Low	Low	Moderate	High	Extreme
Unlikely	B	Low	Low	Low	Moderate	High
Rare	A	Low	Low	Low	Moderate	High

The following tables have been provided as a guide for risk management processes. Councils may wish to consider tailoring the parameters provided for their individual circumstances, or use their existing likelihood and consequenc

Likelihood Rating	Description
E. Almost Certain	Is expected to occur in most circumstances
D. Likely	Will probably occur in most circumstances
C. Possible	Might occur at some time
B. Unlikely	Could occur at some time
A. Rare	May occur only in exceptional circumstances

Impact Scale	Socio-political & Community issues	Business Impact	Public Safety	Environment
1. Insignificant	• No adverse effect on public image • Insignificant level of community concern • Negligible adverse impact upon social health and well being of the community which has little or no impact upon established community relationships and links.	• Low financial loss – impact of less than $5k • Small delays in undertaking routine needs or tasks for ½ day.	• No injuries or no significant injuries • Negligible loss or damage to property / infrastructure.	• "Nuisance" category under the SA Environment Protection Act (1993) met • Contamination – on-site release immediately contained • Slight, quickly reversible damage to few species.
2. Minor	• Minor adverse effect on public image • Minor level of community concern • Minor adverse impact upon social health & well being of the community that may have a minor impact upon established community relationships & links.	• Medium financial loss – impact of between $5k and $20k • Minor impact in undertaking routine needs or tasks for 1 day.	• First aid treatment required • Minor loss or infrastructure damage.	• "Nuisance" category under SA Environment Protection Act (1993) met • Some minor adverse effects to few species/ ecosystem parts that are short term and immediately reversible.
3. Moderate	• Moderate adverse effect on public image • Moderate level of community concern • Social health and well being of the community affected by moderately reduced opportunities for participation in community life and/or decision making, moderate incidences of increased isolation etc.	• High financial loss – impact of between $20k and $50k • Capability / production impaired, moderate impact on stakeholders & routine needs or tasks for 1 – 3 days. • Minor legal issues, non compliances and breaches of regulation.	• Medical treatment required • Moderate loss/or infrastructure damage.	• "Material" category under the SA Environment Protection Act (1993) met • Contamination – on-site release contained with outside assistance • Temporary, reversible damage, loss of habitat and migration of animal population, plants unable to survive, pollution requires physical removal, land contamination localised and can be quickly remedied.
4. Major	• Major adverse effect on public image • Significant level of community concern • Social health and well being of the community seriously affected by major community unrest and/or significant breakdown of established community relationships and links.	• Major financial loss - impact of between $50k and $100k • Loss of capability, disruption to production, major impact on stakeholders & routine needs or tasks for 3 – 5 days. • Serious breach of regulation with investigation or report to authority with prosecution and/or moderate fine possible.	• Serious & extensive injuries • Serious structural damage to infrastructure or serious loss of assets.	• "Serious" category under the SA Environment Protection Act (1993) met • Contamination – off-site release with no detrimental effects • Death of individual animals, large scale injury, loss of keystone species and widespread habitat destruction.
5. Catastrophic	• Huge effect on public image • Community outrage • Social health & well being of the community hugely affected by major community unrest and/or significant breakdown of established community relationships & links.	• Huge financial loss/exposure – impact greater than $100k • Loss of production/capability, failure to meet stakeholder's needs for more than 5 days • Projects & programs failure, inability to meet minimum acceptable standards, most objectives not met • Major breaches of regulation, major litigation.	• Fatalities • Critical loss, irreversible damage property / infrastructure.	• "Serious" category under the SA Environment Protection Act (1993) met • Toxic release off-site with detrimental effect • Death of animals in large numbers, destruction of flora species, air quality requires evacuation, permanent and wide spread land contamination, irreversible soil erosion or severe compaction, widespread introduction of weeds.

Appendix 3. Audit methodology

In conducting the engagement, the team:

- reviewed relevant internal documentation, for example any internal Cyber Security policy/procedural documentation
- conducted interviews with key stakeholders
- compared current approaches against elements outlined in the SACSF
- identified potential opportunities for improvement
- drew upon recent technical Security Review reports (completed February 2020)

Appendix 4. Documents reviewed

- Fraud and Cyber Awareness Training – LGRS brochure
- Code of Conduct
- Contract templates
- Draft policies – Alwyndor
  - IS 004 Information Security Procedure
  - IS 005 Security Incident Processing
  - IS 006 Vulnerability and Patch Management
  - IS 007 Backup and Recovery Policy
  - Information Security Policies and Procedures
  - IS 001 Information Security Policy
  - IS 002 Asset Security Management
  - IS 003 Data Classification
- Draft policies – City of Holdfast Bay
  - Acceptable Use
  - Access Control
  - Antivirus
  - Business Continuity
  - Cloud Computing
  - Communication and Mobile Devices
  - Computers for Councillors
  - Computer System and Equipment Use
  - Cyber Crime and Security Incident
  - Email
  - Encryption
  - Firewall Management
  - Hardware Management
  - Information Management
  - Internet Use
  - Laptop and Tablet Security
  - Legal Compliance
  - Network Management
  - Online Services
  - Password and Authentication
  - Personnel Management
  - Physical Access
  - PSN Protective Monitoring
  - Remote Access
  - Software Management
- Electronic Communication Policy
- Induction checklists
- IT Policy System Brochure
- Organisation Chart as of 1 July 2020
- 2020 Internal Training Calendar
- People Strategy – Our Place, Our Purpose

Appendix 5. Staff members interviewed

- Manager Strategy & Governance
- Customer Liaison Manager Alwyndor
- People and Culture Manager Alwyndor
- ICT Infrastructure Lead
- General Manager Alwyndor
- Financial Manager Alwyndor
- General Manager Strategy and Business Services
- Personal Assistant to General Manager Strategy and Business Services
- Acting Manager Innovation & Technology
- Manager People and Culture

Disclaimers

Inherent limitations

This report has been prepared for the information and internal use of the City of Holdfast Bay in accordance with the scope and objectives outlined in the Executive Summary of this report. The services provided in connection with this engagement comprise an advisory engagement which is not subject to the Australian Auditing Standards or the Australian Standards on Review and Assurance Engagements. Consequently, no express opinions or conclusions have been drawn or intended to convey assurance. Due to the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected.

Further, the internal control structure, within which the control procedures that have been subject to the procedures we performed operate, has not been reviewed in its entirety and, therefore, no opinion or view is expressed as to its effectiveness of the greater internal control structure. The procedures performed were not designed to detect all weaknesses in control procedures as they are not performed continuously throughout the period and the tests performed on the control procedures were on a sample basis. Any projection of the evaluation of control procedures to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, the City of Holdfast Bay's management and personnel. We have not sought to independently verify those sources. We are under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form unless specifically agreed with the City of Holdfast Bay. The internal audit findings expressed in this report have been formed on the above basis.

Third party reliance

This report is solely for the purpose set out in the Executive Summary of this report and for the City of Holdfast Bay's information, and is not to be used for any other purpose or distributed to any other party without Galpins' prior written consent. This internal audit report has been prepared at the request of the City of Holdfast Bay or its delegate in connection with our engagement to perform internal audit services. Other than our responsibility to City of Holdfast Bay, neither Galpins nor any member or employee of Galpins undertakes responsibility arising in any way from reliance placed by a third party, including but not limited to the City of Holdfast Bay's external auditor, on this internal audit report. Any reliance placed is that party's sole responsibility.

CONFIDENTIAL

CYBER SECURITY REVIEW - ACTION PLAN

Rec	Agreed Action	Detail of Action	Completion Date	Action Officer	Status	Comments
1	1.1	Finalise vacant positions: - Manager Innovation & Technology Services - Team Leader Technology Operations	2/11/2020	GM, S&BS	Completed	
	1.2	Define leadership, organisational structure across both CHB and Alwyndor	29/01/2021	Manager, I&T		
	1.3	Define internal staff capabilities/responsibilities across both CHB and Alwyndor and mitigate internal gaps by procuring external resources.	29/01/2021	Manager, I&T		
	1.4	Provision of Information Technology Specialist Services	11/01/2021	Manager, I&T	Completed	akto have been awarded contract for 3 years
2	2.1	Develop an approved information security strategy model for both CHB and Alwyndor that: - Assess the security requirements - Performs a gap analysis - Prioritises initiatives and build a security roadmap - Plans for the transition - Executes and maintain	25/06/2021	Manager, I&T		
3	3.1	Developed and implement a process to: - Commission an internal Cyber Security panel - Record security reviews and audit recommendations - Analyse the recommendations - Document the agreed actions including responsible person(s) and completion date/time - Review agreed actions to ensure recommendations are mitigated	26/03/2021	Manager, I&T		
4	4.1	Develop standard policies to cover the following areas for both CHB and Alwyndor: - information security - mobile devices and teleworking - acceptable use of assets - human resource screening - asset management - information classification - supplier management - media handling (eg use of portable media) - access control	30/04/2021	Manager, I&T		
	4.2	Develop an approval process with Senior leadership Team.	30/04/2021	Manager, I&T		
	4.3	Develop an approved review process.	30/04/2021	Manager, I&T		
5	5.1	Develop an approved periodic risk assessment process covering the following: - Information Security Policies - Information security roles and responsibilities - Terms and conditions of employment - Asset management - Access control - Cryptography - Operations Security - Communications security - Systems acquisition, development and maintenance - Suppliers relationships - Information security incident management - Information security aspects of business continuity management - Privacy and protection of personally identifiable information - Vulnerability assessments - Penetration assessments - Friendly phishing	25/06/2021	Manager, I&T		

Rec	Agreed Action	Detail of Action	Completion Date	Action Officer	Status	Comments
6	6.1	Develop and implement an approved policies and procedures to protect the organisation's systems and information that is accessible to ICT outsourcers and other external suppliers. Process to be applied to current and future providers involves: - Risk assessment - Screen and auditing - Selecting clauses in agreements based on above - Access control - Compliance monitoring - Termination of the agreement	26/02/2021	Manager, I&T		
	6.2	Service delivery by external suppliers to be monitored and reviewed/audited against the contracts/agreements and including service changes.	26/02/2021	Manager, I&T		
7	7.1	Develop and implement an approved incident management framework and workflow.	26/03/2021	Manager, I&T		
8	8.1	Complete update of CHB Disaster Recover Plan	1/12/2020	Manager, I&T		
	8.2	Complete update of the Alwyndor Disaster Recovery Plan to include any comments from the business.	1/02/2021	Manager, I&T		
9	9.1	Expand the utilisation the MDM to include all laptops, CHB/Alwyndor issued mobile phones and BYOD where staff request access to CHB and Alwyndor systems.	29/01/2021	Team Leader, TO		
	9.2	Enable Two Factor Authentication	29/01/2021	Team Leader, TO		
	9.3	Develop and Authorise a Mobile Device Policy	29/01/2021	Team Leader, TO		
10	10.1	Implement an automated network inventory, discovery and asset management tool that gathers hardware and software information of computers and other devices on a computer network for management, compliance and audit purposes for both CHB and Alwyndor.	CHB - 29/1/2021 AWD - 26/2/21	Team Leader, TO		
11	11.1	Complete stage 2 of the Information Management Change Program (incorporating Alwyndor as an additional stakeholder).	30/06/2021	Manager, I&T		
12	12.1	Update the ICT induction process for both CHB and Alwyndor to include the following topics: - Information and Communication Technology Security - Cyber security incoporation Scam and phishing emails - Acceptable Use of Information and Communication Technology - Use of email, internet and social media - Information Management Record	29/01/2021	Team Leader, TO		
13	13.1	Utilise the LGRS Be Security Smart Program for awareness training.	25/06/2021	Manager, I&T		
14	14.1	All new employees and contractors appointed to the City of Holdfast Bay, who access to systems and information that can be critical and sensitive in nature will now be required to undertake DHS Vulnerable Persons screen test. DHS Vulnerable Persons screen test to be reviewed every three years.	1/12/2020	Manager, I&T	Completed	
		All current employees who access to systems and information that can be critical and sensitive in nature will now be required to undertake DHS Vulnerable Persons screen test. DHS Vulnerable Persons screen test to be reviewed every three years.	1/12/2020	Manager, I&T	Completed	
		All current contractors appointed to the City of Holdfast Bay, who access to systems and information that can be critical and sensitive in nature will now be required to provide DHS Vulnerable Persons screen test.	1/12/2020	Manager, I&T	Completed	