

## ITEM NUMBER: 6.1

### ATTACHMENT 4

## CONFIDENTIAL STANDING ITEMS – AUGUST 2021 (Report No: 270/21)

*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 Audit Committee Members upon the basis that the Audit Committee consider the Report and the documents in confidence under Part 3 of the Act, specifically on the basis that the Audit Committee 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.

**CONFIDENTIAL**  
CYBER SECURITY REVIEW - ACTION PLAN

Rec	Agreed Action	Detail of Action	Audit Risk Rating – CHB	Audit Risk Rating – Alwyndor	Estimated Completion Date	Revised Completion Date	Action Officer	Status	Comments
1	1.1	Finalise vacant positions: - Manager Innovation & Technology Services - Team Leader Technology Operations	High	High	2/11/2020		GM, S&BS	Completed	
1	1.2.1	Provision of Information Technology Specialist Services	High	High	29/01/2021		Manager, I&T	Completed	Contract signed 10/12/2020. Contract will provide services to assist with the recommendations of the report.
1	1.2.2	Define leadership, organisational structure across both CHB and Alwyndor	High	High	29/01/2021	<del>5/03/2021</del> 30/07/21	Manager, I&T	Completed	01/02/21 - CIO Services have been engaged to review current structure and define future roles and capability and make recommendations. 09/03/21 - Draft IT Operations Review and Action Plan provided that recommends the leadership, organisational structure across both CHB and Alwyndor, see Section 4 of the report. 30/03/21 - IT Operations Review and Action Plan approved which defines the structure across both CHB and Alwyndor. 21/05/21 - Structure approved and in the process of filling the following vacancies: - Project Delivery Lead - ICT Infrastructure and Security Officer - Business/Change Analyst - Business Analyst/Solution Architect - Business and Information Systems Lead 06/08/21 - Structure approved and positions defined. Recruitment being undertaken for final position.
1	1.3.1	Define internal staff capabilities/responsibilities across both CHB and Alwyndor.	High	High	29/01/2021	<del>5/03/2021</del> 30/07/21	Manager, I&T	Completed	01/02/21 - CIO Services have been engaged to review current structure and define future roles and capability and make recommendations. 09/03/21 - Draft IT Operations Review and Action Plan provided that recommends the leadership, organisational structure across both CHB and Alwyndor, see Section 4 of the report. 30/03/21 - IT Operations Review and Action Plan approved which defines the structure across both CHB and Alwyndor. 21/05/21 - Structure approved and in the process of filling the following vacancies: - Project Delivery Lead - ICT Infrastructure and Security Officer - Business/Change Analyst - Business Analyst/Solution Architect - Business and Information Systems Lead 25/08/21 - Capabilities and responsibilities for all positions have been defined and are reflected in position descriptions.
1	1.3.2	Mitigate internal gaps by procuring external resources.	High	High	26/03/2021	<del>5/03/2021</del> 30/07/21	Manager, I&T	In Progress	01/02/21 - CIO Services have been engaged to review current structure and define future roles and capability and make recommendations. 09/03/21 - Draft IT Operations Review and Action Plan provided that recommends the leadership, organisational structure across both CHB and Alwyndor, see Section 4 of the report. 30/03/21 - IT Operations Review and Action Plan approved which defines the structure across both CHB and Alwyndor. 21/05/21 - Capability gaps identified. CIO Advisory services and network security services have been procured. Requirements for a Managed Service Provider (MSP) for Council and Alwyndor are being developed. 06/08/21 - Requirements defined and tender documents being finalised for MSP. Tender to be advertised by end of August 2021.
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	High	High	25/06/2021	<del>30/06/2021</del> 31/12/2021	Manager, I&T	Not Commenced	09/03/21 - Draft IT Operations Review and Action Plan provided recommends an information security strategy, see section 5.3 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 25/8/21 - Requirements identified, gaps identified and in the process of executing the plan.
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	High	High	26/03/2021	<del>31/05/2021</del> 31/12/2021	Manager, I&T	Not Commenced	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a information security strategy, see section 5.3 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 25/8/21 - Security testing and reviews to commence once changes to the network infrastructure have been completed.
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 (e.g. use of portable media) - access control	High	Medium	30/04/2021	<del>30/04/2021</del> 30/07/21	Manager, I&T	Completed	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a process to achieve this action, see section 6 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 21/05/21 - Draft policies being developed and reviewed. 25/08/21 - Policies developed. To be tabled with SLT for approval.

**CONFIDENTIAL**

**CONFIDENTIAL**  
CYBER SECURITY REVIEW - ACTION PLAN

Rec	Agreed Action	Detail of Action	Audit Risk Rating – CHB	Audit Risk Rating – Alwyndor	Estimated Completion Date	Revised Completion Date	Action Officer	Status	Comments
4	4.2	Develop an approval process with Senior Leadership Team.	High	Medium	30/04/2021	<del>30/04/2021</del> 30/07/21	Manager, I&T	Completed	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a process to achieve this action, see section 6 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 21/05/21 - Utilise current CHB approval process
4	4.3	Develop an approved review process.	High	Medium	30/04/2021	<del>30/04/2021</del> 30/07/21	Manager, I&T	Completed	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a process to achieve this action, see section 6 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 21/05/21 - Utilise current CHB review process
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	High	Medium	25/06/2021	<del>25/06/2021</del> 30/09/21	Manager, I&T	In Progress	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a process to achieve this action, see section 6 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 21/05/21 - External resource to facilitate the development of the risk assessment process is required 06/08/21 - External resource selected and initial meeting to comment week of 9/8/21. Completion date to be determined.
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	High	Medium	26/02/2021	<del>31/07/2021</del> 30/09/21	Manager, I&T	In Progress	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a process to achieve this action, see section 6 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 21/05/21 - External resource to facilitate the development of policies and procedures is required 06/08/21 - External resource selected and initial meeting to comment week of 9/8/21. Completion date to be determined.
6	6.2	Service delivery by external suppliers to be monitored and reviewed/audited against the contracts/agreements and including service changes.	High	Medium	26/02/2021	<del>31/03/2021</del> 30/07/21	Manager, I&T	Completed	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a process to achieve this action, see section 6 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 21/05/21 - Review current CHB contractor management procedures 06/08/21 - External Service providers have been reviewed to ensure providers are delivering expected services and are providing value for money. This has resulted in the reduction of service fees or removal of the provider for an improved value for money provider. This will be an ongoing process.
7	7.1	Develop and implement an approved incident management framework and workflow.	High	High	26/03/2021	30/07/2021	Manager, I&T	In Progress	09/03/21 - Draft IT Operations Review and Action Plan provided recommends a process to achieve this action, see section 5.3 of the report. 30/03/21 - IT Operations Review and Action Plan approved. 21/05/21 - Draft framework and workflow being developed. 06/08/21 - Current Service Desk system is being replaced with ██████████ which is a service management system that has been designed on the ITIL foundation framework. ██████████ is expected it be operational by end of Sept 2021.
8	8.1	Complete update of CHB Disaster Recover Plan	High	High	1/12/2020	<del>31/03/2021</del> 30/07/2021	Manager, I&T	In Progress	Draft completed. Currently being reviewed by CIO Services. 30/03/21 - IT Operations Review and Action Plan approved. The action plan recommends a re-write the Disaster Recovery plan to accurately reflect the current environment and include clear information on what constitutes and evokes the plan. 21/05/21 - Updated draft plan provided 06/08/21 - Updated draft plan provided
8	8.2	Complete update of the Alwyndor Disaster Recovery Plan to include any comments from the business.	High	High	1/02/2021	30/07/2021	Manager, I&T	In Progress	Draft completed. Awaiting approval by Alwyndor Executive. 30/03/21 - IT Operations Review and Action Plan approved. The action plan recommends a re-write the Disaster Recovery plan to accurately reflect the current environment and include clear information on what constitutes and evokes the plan. 21/05/21 - Updated draft plan being developed in conjunction with ██████████, (current Alwyndor MSP) 06/08/21 - Updated draft plan provided

**CONFIDENTIAL**

**CONFIDENTIAL**  
CYBER SECURITY REVIEW - ACTION PLAN

Rec	Agreed Action	Detail of Action	Audit Risk Rating – CHB	Audit Risk Rating – Alwyndor	Estimated Completion Date	Revised Completion Date	Action Officer	Status	Comments
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.	High	High	29/01/2021	<del>30/04/2021</del> 30/07/2021	Team Leader, TO	In Progress	Implementation expected by end April 2021. 09/03/21 - Currently have all laptops synced to █████ MDM for management in a hybrid cloud environment. Commenced testing of MDM policies for mobile phones. MDM policy set for new mobile devices and began developing a plan to deploy to existing mobile devices. 09/04/21 - All laptops are now managed fully and remote wipeable, have successfully tested mobile policies both for corporate handsets and BYOD. Are currently working on restricting access to outlook when not enrolled with MDM and a project plan to get staff setup on MDM 21/05/21 - Have deployed a successful pilot group of fully mdm managed Mobile Phones. Have engaged vendor Blackbird IT to assist with development of project to deploy mdm to all devices currently in use with minimal impact to staff. ETA of MDM deployment to all Mobile handsets 15/07/21 06/08/21 - Dependency on MFA being deployed to the organisation for all mobile devices that have previously been deployed to be managed, BlackBird IT are returning 23/08/21 to assist with deployment to all previously issued mobile devices and BYOD. Once CHB is completed the process will begin for Alwyndor
9	9.2	Enable Two Factor Authentication (2FA)	High	High	29/01/2021	<del>30/04/2021</del> 30/07/2021	Team Leader, TO	In Progress	Implementation expected by end April 2021. 09/03/21 - Currently in testing phase. Microsoft 2FA for external access at Holdfast currently enabled for IT Admins. Servers, backups and internal password safe are now 2FA enabled by █████ MFA to prevent unauthorised access. Will commence at developing policies on 2FA for all staff when on remotely accessing services. 09/04/21 - policies for staff using 2FA for accessing external systems are setup, need a pilot group and to discuss how we get staff to use their mobile device for the 2FA request 21/05/21 - Working with Vendor BlackBird IT to deploy MFA to all users when accessing CoHB systems externally, communications, documentation and project plan work begun, have a test group setup and working ETA for organisation wide implementation 01/07/21 *note will require SLT to accept that staff without work phones will require to download an authenticator app (E.g. Microsoft authenticator or google authenticator with preferred app TBD) to be able to securely access holdfast systems externally. 06/08/21 - Due to COVID lockdown the original go live date of 29/07/21 was pushed back 2 weeks until Thursday 12/08/21 , we have confirmed almost all of the end users targeted are now setup with MFA and ready to be used, once CHB is completed the process will begin for Alwyndor
9	9.3	Develop and Authorise a Mobile Device Policy	High	High	29/01/2021	<del>30/04/2021</del> 30/07/2021	Team Leader, TO	In Progress	09/03/21 - Draft mobile device policy almost complete. Will finalise and send to Manager, I&T to review. Policy can be used at both CHB and Alwyndor. 09/04/21 - have completed mobile device policy, sending to Manager IT&T today, have drafts of an acceptable use policy and incident management policy. 21/05/21 - SLT required to sign off on draft policy 06/08/21 - Policies developed and ready for submission to SLT for review and approval.
10	10.1.1	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.	High	Medium	25/01/2021	28/02/2021	Team Leader, TO	Completed	09/03/21 - Implemented █████ (trial licence) to provide auditing of hardware and software on both CHB and Alwyndor networks. Currently waiting on license purchasing to standardise the asset auditing system. Cost approximately \$1,600 per year per site. 9/04/21 - Have setup and licensed █████ at both Holdfast and Alwyndor
10	10.1.2	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.	High	Medium	26/02/2021		Team Leader, TO	Completed	09/03/21 - Implemented █████ (trial licence) to provide auditing of hardware and software on both CHB and Alwyndor networks. Currently waiting on license purchasing to standardise the asset auditing system. Cost approximately \$1,600 per year per site. 9/04/21 - Have setup and licensed █████ at both Holdfast and Alwyndor
11	11.1	Complete stage 2 of the Information Management Change Program (incorporating Alwyndor as an additional stakeholder).	High	Medium	30/06/2021	30/06/2022	Manager, I&T	Not commenced	21/05/21 - Project defined in Technology Roadmap to cover bot Council and Alwyndor and revised commencement date to be define as part of the investment prioritisation process. 25/8/21 - Work has stalled on this project due to resourcing contract. Person has been appointed to the position. This is a long term project that will progress well into 2022.
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 incorporation Scam and phishing emails - Acceptable Use of Information and Communication Technology - Use of email, internet and social media - Information Management Record	Medium	Low	29/01/2021	<del>31/03/2021</del> 30/07/2021	Team Leader, TO	In Progress	09/03/21 - A standardised template and infograph for inductions developed for both CHB and Alwyndor that includes: -- Acceptable Use of Information and Technology -- Use of email, internet and social media -- Cyber security information and how to identify phishing emails (Note; still in progress for signed off policy documents to include links for new users) 09/04/21 - Some minor tweaks to this process is being completed, almost completed 21/05/21 - Have documented induction process that can be used across Council and Alwyndor, includes booking in staff, PPT explaining required information and security and security videos have been uploaded to azure for reviewing. Now Require SLT to sign of on 'Acceptable Use Policy' which new staff will need to sign as part of induction. 06/08/21 - Updated the ICT induction process in place of CHB. Content sent to Alwyndor for to update their ICT induction process
13	13.1	Utilise the LGRS Be Security Smart Program for awareness training.	Medium	Low	25/06/2021		Manager, I&T	Completed	09/03/21 - Videos downloaded to be incorporated into the staff induction process. 09/04/21- Videos downloaded incorporated into the staff induction process.
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.	Medium	N/A	1/12/2020		Manager, I&T	Completed	

**CONFIDENTIAL**

**CONFIDENTIAL**  
CYBER SECURITY REVIEW - ACTION PLAN

Rec	Agreed Action	Detail of Action	Audit Risk Rating – CHB	Audit Risk Rating – Alwyndor	Estimated Completion Date	Revised Completion Date	Action Officer	Status	Comments
14		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.	Medium	N/A	1/12/2020		Manager, I&T	Completed	
14		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.	Medium	N/A	1/12/2020		Manager, I&T	Completed	

CONFIDENTIAL