ITEM NUMBER: 8.3

ATTACHMENT 4

CONFIDENTIAL
INTERNAL AUDIT PROGRAM REPORT
(Report No: 77/23)

Pursuant to Section 87(10) of the Local Government Act 1999 the Report attached to this agenda and the accompanying documentation is delivered to the Audit and Risk Committee upon the basis that the Committee considers the Report and the documents in confidence under Part 3 of the Act, specifically on the basis that Audit and Risk 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.

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	
1	1.2.2	Define leadership, organisational structure across both CHB and Alwyndor	High	High	29/01/2021	30/07/2021	Manager, I&T	Completed	
1	1.3.1	Define internal staff capabilities/responsibilities across both CHB and Alwyndor.	High	High	29/01/2021	30/07/2021	Manager, I&T	Completed	
1	1.3.2	Mitigate internal gaps by procuring external resources.	High	High	26/03/2021	31/12/2021	Manager, I&T	Completed	
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	30/06/2023	Manager, I&T	In Progress	The objective is to develop a **Security Strategy** based on the LGITSA and industry best practice security frameworks for CHB, encompassing Council and Alwyndor. The strategy will provide a suite of documents, toolkits, templates and processes to guide CHB in implementing a framework based on our risk appetite, size, available resources and maturity level. Developing a realistic implementation plan and effective security risk management requires implementing and ongoing management of a program of works endorsed by the Senior Leadership Team, Council Leadership Team and Alwyndor Executive Team, ensuring an ongoing commitment and approach towards managing security risk sustainably and pragmatically. The security program should aim to consider and document the following: •The security objectives of CHB and how these support the broader strategic objectives •The scope, boundaries and exclusions of the security program •The program requirements and success criteria •The security governance model and critical responsibilities and functions
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	30/06/2023	Manager, I&T	In Progress	The objective is to develop a **Security Strategy** based on the LGITSA and industry best practice security frameworks for CHB, encompassing Council and Alwyndor. The strategy will provide a suite of documents, toolkits, templates and processes to guide CHB in implementing a framework based on our risk appetite, size, available resources and maturity level. Developing a realistic implementation plan and effective security risk management requires implementing and ongoing management of a program of works endorsed by the Senior Leadership Team, Council Leadership Team and Alwyndor Executive Team, ensuring an ongoing commitment and approach towards managing security risk sustainably and pragmatically. The security program should aim to consider and document the following: •The security objectives of CHB and how these support the broader strategic objectives •The scope, boundaries and exclusions of the security program •The program requirements and success criteria •The security governance model and critical responsibilities and functions
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	30/10/2021	Manager, I&T	Completed	
4	4.2	Develop an approval process with Senior Leadership Team.	High	Medium	30/04/2021	30/11/2021	Manager, I&T	Completed	
4	4.3	Develop an approved review process.	High	Medium	30/04/2021	30/11/2021	Manager, I&T	Completed	
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	30/06/2023	Manager, I&T	In Progress	The objective is to develop a **Security Strategy** based on the LGITSA and industry best practice security frameworks for CHB, encompassing Council and Alwyndor. The strategy will provide a suite of documents, toolkits, templates and processes to guide CHB in implementing a framework based on our risk appetite, size, available resources and maturity level. Developing a realistic implementation plan and effective security risk management requires implementing and ongoing management of a program of works endorsed by the Senior Leadership Team, Council Leadership Team and Alwyndor Executive Team, ensuring an ongoing commitment and approach towards managing security risk sustainably and pragmatically. The security program should aim to consider and document the following: •The security objectives of CHB and how these support the broader strategic objectives •The scope, boundaries and exclusions of the security program •The program requirements and success criteria •The security governance model and critical responsibilities and functions

Rec	Agreed Action	Detail of Action	Audit Risk Rating – CHB	Audit Risk Rating – Alwyndor	Estimated Completion Date	Revised 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	High	Medium	26/02/2021	30/06/2023	Manager, I&T	In Progress	Policies approved by Council All policies published to Baywatch Council policies published to the website All policies provided to Alwyndor Next step to provide staff education to EM,s Council and Alwyndor staff
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	31/12/2022	Manager, I&T	Completed	Completed review of all external suppliers
7	7.1	Develop and implement an approved incident management framework and workflow.	High	High	31/12/2021	30/07/2021	Manager, I&T	Completed	
8	8.1	Complete update of CHB Disaster Recover Plan	High	High	1/12/2020	30/07/2021	Manager, I&T	Completed	
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	Completed	
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	31/12/2022	Team Leader, TO	Completed	
9	9.2	Enable Two Factor Authentication (2FA)	High	High	29/01/2021	31/12/2022	Team Leader, TO	Completed	
9	9.3	Develop and Authorise a Mobile Device Policy	High	High	29/01/2021	30/06/2023	Team Leader, TO	In Progress	Policies approved by Council All policies published to Baywatch Council policies published to the website All policies provided to Alwyndor Next step to provide staff education to EMs, Council and Alwyndor staff
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	29/01/2021	28/02/2021	Team Leader, TO	Completed	
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	28/02/2021	Team Leader, TO	Completed	
11	11.1	Complete stage 2 of the Information Management Change Program (incorporating Alwyndor as an additional stakeholder).	High	Medium	30/06/2021	Ongoing	Manager, I&T	Ongoing	The project has commenced, and the objective is to improve access to information for all staff and the information and record-keeping environment at Council by: •Enabling an agreed platform for improved collaboration of unofficial/active information •Assessing, implementing and administering business information access and security across all storage repositories •Implementing a definitive Business classification scheme and document naming standards •Establishing responsibilities of business owners and ECM Champions •Developing standards and procedures •Awareness and education •Regular information audits and performing internal usage audits •Maintaining business information repositories •Monitoring and controlling business information, including disposal schedule retention on electronic documents To be implemented at Alwyndor based on their resource availability.
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	30/07/2021	Team Leader, TO	Completed	
13	13.1	Utilise the LGRS Be Security Smart Program for awareness training.	Medium	Low	25/06/2021		Manager, I&T	Completed	
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	
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	