ECM# 9570106

City of Cockburn

Audit & Strategic Finance Committee

Minutes

For Thursday, 16 July 2020

These Minutes are confirmed.

Presiding Member's signature

Date: 19 November 2020

CITY OF COCKBURN

SUMMARY OF MINUTES OF THE AUDIT & STRATEGIC FINANCE COMMITTEE MEETING HELD ON THURSDAY, 16 JULY 2020 AT 6.00 PM

Page

CITY OF COCKBURN
MINUTES OF AUDIT & STRATEGIC FINANCE COMMITTEE
HELD ON THURSDAY, 16 JULY 2020

PRESENT

ELECTED MEMBERS

Mr L Howlett	-	Mayor
Mr K Allen	-	Councillor (Presiding Member)
Mr T Widenbar	-	Councillor
Dr C Terblanche	-	Councillor
Ms C Stone	-	Councillor

IN ATTENDANCE

Mr D Arndt	-	Acting Chief Executive Officer
Mr D Green	-	Director Governance & Community Services
Mr C Sullivan	-	Director Engineering and Works
Mrs G Bowman	-	Executive Manager, Strategy & Civic Support
Mr N Mauricio	-	A/Director Finance and Corporate Services
Ms R Pleasant	-	A/Director Planning and Development
Mr J Fiori	-	Risk and Governance Advisor
Mrs B Pinto	-	Governance Officer
Ms S D'Agnone	-	Council Minute Officer

1. DECLARATION OF MEETING

The Presiding Member declared the meeting open at 6.00pm.

"Kaya, Wanju Wadjuk Budjar" which means "Hello, Welcome to Wadjuk Land"

The Presiding Member acknowledged the Nyungar People who are the traditional custodians of the land on which the meeting is being held and pay respect to the Elders of the Nyungar Nation, both past and present and extend that respect to Indigenous Australians who are with us tonight.

The Audit and Strategic Finance Committee meeting will be electronically recorded and live streamed on the City's website, except where Committee resolves to go behind closed doors.

All recordings are retained in accordance with the General Disposal Authority for Local Government Records produced by the State Records Office.

A copy of the recorded proceedings will be available on the City's website, within two business days of the Council meeting. This will be easy to find from the front page of the City's website.

Images of the public gallery are not included in the webcast, however the voices of people will be captured and streamed.

The Presiding Member reminded everyone present to be mindful of their conduct as it will be recorded. This is a Council initiative aimed at increasing our transparency and openness, as well as making Council meetings more accessible.

2. APPOINTMENT OF PRESIDING MEMBER (If required)

N/A

3. DISCLAIMER (Read aloud by Presiding Member)

Members of the public, who attend Council Meetings, should not act immediately on anything they hear at the Meetings, without first seeking clarification of Council's position. Persons are advised to wait for written advice from the Council prior to taking action on any matter that they may have before Council.

4. ACKNOWLEDGEMENT OF RECEIPT OF WRITTEN DECLARATIONS OF FINANCIAL INTERESTS AND CONFLICT OF INTEREST (by Presiding Member)

Nil

5. APOLOGIES & LEAVE OF ABSENCE

Mr S Downing, Director Finance and Corporate Services - Apology

THE EXECUTIVE MANAGER STRATEGY AND CIVIC SUPPORT LEFT THE MEETING AT 6.02PM AND RETURNED AT 6.03PM.

6. PUBLIC QUESTION TIME

Susan Smith

Q1. As the former Independent Member of the Audit and Strategic Finance Committee, my question is in regards to the minutes of the previous meeting, and why the reappointment of the Independent Member was not discussed at that previous meeting?

The Presiding Member advised the matter was not listed on the agenda, and therefore not discussed at the meeting.

Q2. Why has the process for extending the period of the Independent Member that was approved by both the Audit and Strategic Finance Committee and Council in 2019, not been followed?

The Presiding Member advised that, as the question does not relate to an agenda item, the question would be taken on notice and responded to in writing.
Note: responses to questions raised were subsequently provided in the responses for question 5 to question 16 below.

Q3. At my first meeting in July 2019, I raised concerns over the adequacy of the Strategic Internal Audit Program. It was advised to me that a report would come back to the Audit Committee addressing those. We approved the Strategic Internal Audit Plan on the basis of allowing the program of work to continue with the queries being responded to subsequently with a report coming back. That report has never come to the Audit and Strategic Finance Committee. I would like to know how that is going to come forward?

The Acting CEO advised he would revisit the minutes from the Committee Meeting in question and that the question would be taken on notice.

Q4. Can I have it noted that I have raised it at every meeting since then and there has been no response on that matter. I can quote the minutes from July - "*receive a report…identifying the risks as part of the Strategic Risk Review and be presented to the next Audit and Strategic Finance Committee".*
It makes it difficult for this Committee to provide effective oversight without communicating to it an effective Internal Audit function that ensures ongoing maintenance and governance processes.

Whoever the Independent Member that comes forward is, their ability to assist good governance is limited by the information that comes to the Committee.

The Acting Director Finance and Corporate Services provided responses to questions asked previously by Ms Smith:

Q5. What is the time allocated for each audit?
Q6. Are there additional hours allocated for ad hoc audits that are required?

Response
WALGA preferred audit service providers are generally used to conduct audits listed in the Strategic Internal Audit Plan. The selected service provider nominates a set number of hours to conduct an audit – this is not generally a pre-determined time limit as it depends on the complexity of the audit being conducted.

Q7. What is the annual budget for internal audits?

Response
Internal audit budget 2019-2020 was $70,000.

Q8. The Risk Management Plan states '*audit services. The Internal Audit Program is overseen by the Financial Services Department*'. What are the current reporting lines? How can the Audit Committee be satisfied the Internal Audit is independent and overseen by Risk and Governance?

Response
Governance Service sets the objectives and manages the budget for the Strategic Internal Audit Plan, which is then approved by the Audit and Strategic Finance Committee.

Q9. Can the City's Internal Audit Charter please be provided to the Committee?

Response
Audit and Strategic Finance Committee Terms of Reference are recorded in OCM November 2019 minutes.

Q10. How does the Strategic Internal Audit Plan align with the Risk Register? For example, Risk 2 Technology Use and Change, is rated Substantial. I would have expected annual Security Audits.

Q11. What assurance do you have that the existing controls listed are working effectively?

Response
The City was one of 10 local governments included in the first Local Government Information Systems Audit by the Office of Auditor General. This was tabled in parliament on 25 June and a report will be presented to the November meeting addressing the findings and security gaps identified. City Officers did not have enough time to read the report and prepare a report for this meeting, given the agenda timelines.

Q12. Given the likely OSH legislative changes, I would have expected an internal audit to provide assurance that policies and procedures are in accordance with Worksafe Plan and preparation for the WA government's adoption of the model act. What assurance does Council and Executive have that the City is meeting the Worksafe Plan elements?

Response
LGIS undertook an audit of the City's safety programs and procedures in October 2019. The audit was undertaken against Worksafe's 'Worksafe Plan' requirements. LGISs awarded the City a silver certificate with nil unsatisfactory findings.

Q13. The Risk Management Plan states no appetite for non-compliance risk. Given this, would an annual external review of the Compliance Annual Return provide greater assurance?

Response
An independent audit will be scheduled for the next Compliance Annual Return (2021) and it is proposed that this will be completed on a bi-annual basis (annually is not deemed to be warranted).

Q14. The Risk Management framework refers to three lines of defence. How is this reviewed and relied upon to ensure you have appropriate assurance? Link between internal validation and assurance program.

Response
The Risk Management framework is reviewed every two years. The last review was conducted in October 2018 by Risk West and found "*the three lines of defence assurance model sections comprehensively illustrate the links between risk, planning and operations*".

Q15. You have said that the nominated contactor nominates the hours for the audit that they believe is adequate. I find that a little bit unusual. It's almost like asking whoever is building your road to say what price you would like. If you are not setting a budgeted hour or a day of audits, if you are just giving them the scope, obviously there is some kind of budget process there, so you're obviously going to be giving them some kind of guidance. But then for them to be able to choose their own hours, that from somebody who has done this for 16 years, would be a great thing for any contractor to get that offer.

The Acting Director Finance and Corporate Services advised that the internal audit function is governed by Governance Services, however in the past Finance has overseen the function. From experience, when these audit assignments are determined, it is not them determining the hours. It is more the City provides a scope, and then meets with the Auditor to go through the scope. The Auditor gives us an estimation of the hours to complete that scope. We look at whether that scope and cost fits into our budget and our requirements. Once we mutually agree that it's sufficient, we tick it off and bring it to the Audit Committee.

Q16. In the meetings that I have attended in the past year, scope and objectives have not come to the Committee once, for any audit. Also, your first comment was that the objective had been set by Governance. In all the previous audits that came up to the Committee in the last year, they were all approved by Corporate Services.

The Acting Director Finance and Corporate Services advised that was incorrect. The Strategic Internal Audit Plan has the general scope of every internal audit that has been agreed, and the last Strategic Internal Plan was developed by a working group that was overseen by Governance Services. And then the scope comes to the Audit Committee and that is ticked off. The Strategic Internal Audit Plan comes to the Audit Committee and it gets approved by the Audit and Strategic Finance Committee.

Q17. That is one of my questions about the Strategic Internal Audit Plan is why the scope and objectives for the audit is not outlined in it, and the response then was that is what we agree with at the time, the area themselves agrees. Every single report that has come up I have asked who signed off on the letter of engagement to this, and it hasn't been Governance.

The Presiding Member advised that Public Question Time does not allow for debate and that if Ms Smith required any further clarification on these matters she should submit her questions in writing to the Acting CEO.

Q18. I put my questions to the Committee in July, November, December, March, and now I am standing here and voicing them.

The Presiding Member advised that an answer is not available this evening, and that he has requested that the Acting CEO ensure these questions are answered in a timely manner.

Q19. Could the answers come to the Committee so it is on public record?

The Presiding Member advised that a response would be provided.

Questions on the Agenda - Item 11.1 – Risk Information Report

Q20. There is a statement that says the overall improvement that the City has made in managing the risk is reflected in the risk level movements (page 8). A table on page 9 shows the risk ratings are the inherit risk, not the residual risks. How has the City's management of the risks been shown in the change in risk rating of the inherent risk, in terms of the inherit risk being before your treatment plan?

The Risk and Governance Advisor advised that the current system used by the City is strictly on residual risk. That was the adoption through the system the City has, RMSS. The City deals primarily and only with residual risk. How do we know that the risk is being managed accordingly? We can see through the Risk Register where each Responsible Officer managing the risk addresses the risk action that comes up. That risk action is based on the risk rating (severity of risk). For example, if the risk is extreme it might be once a month, if it is moderate, it might be every three months, and so on and so forth, but it is strictly on residual risk.

The Australian Standard does not require the City to address inherent or residual risk, which is left for the organisation to manage.

Q21. It is not clear that is residual risk and the COVID risk in itself, you would have to say that the risk of that has been the environment factors, world-wide global environmental factors that have changed that risk. So that would be the change in the inherent not the residual, for that risk to increase. So the information report coming forward is not necessarily clear in that, to provide enough information to the committee so that they know what they are dealing with here.

The Risk and Governance Advisor advised that the COVID risk has been rated as being extreme. It was previously not a specific COVID risk, it was a strategic risk based on an emergency situation. It is fair to say that no organisation on earth would have seen the COVID pandemic coming. Therefore, when we were made aware by the Health Department of WA that there was a pandemic, we met, according to the Business Continuity Plan, and drafted a COVID Pandemic Plan, and we reviewed the risk rating of that.

The likelihood is almost certain, and the consequences are catastrophic, which makes that risk an extreme risk. Based on the current situation in Victoria, that is unlikely to change and the City will not change it until the State Government of Western Australia says otherwise.

Q22. I would agree with you on that, but the change has been in the inherent risk, not the City's management of those matters.

The Risk and Governance Advisor reiterated that the City adheres to the ISO Standard and that there is no requirement in the ISO Standards to have an inherent or residual risk. It is primarily for the user to decide and the City has chosen to stick to residual risk, and it works well for us.

Q23. The recommendation is that the Committee is to receive the report. In terms of that as a recommendation, is the recommendation saying that they should be approving it or endorsing it, or just noting it for information purposes?

The Risk and Governance Advisor advised that this is the way we report to this Audit Committee, and it is full Council that endorses the report.

Questions on the Agenda - Item 16.1 – Audit Report- Data and Information

Q24. Who signed off on the engagement letter for this engagement, and who determined the scope and objectives of the audit? I note that the Terms of Reference for the audit were preparing policies and procedures?

The Risk and Governance Advisor advised that the Strategic Internal Audit Plan sets out a scope - very succinct. As the City developed the Terms of Reference for this audit, that succinct statement is going to be taken and expanded. We then write the full Terms of Reference on what is to be taken. Then go and look at which Auditors to use. In this specific case, there is no legislation in this state that requires us to comply with a privacy policy at all. It is a progressive action that we have taken to ensure that if and when legislation in this state changes, we comply.

The Auditor has called it a 'privacy impact assessment' because it is a statement of how the City is faring thus far and what gaps there are if and when legislation is introduced. The Auditor recommended that we follow the Commonwealth *Privacy Act 1988*.

Again, we are not compelled to follow any Act, we have at the moment a privacy statement, and we have taken the initiative to draft a policy in the absence of legislation and the Terms of Reference for this audit describes that, and that is recorded in ECM (the city's record management system).

Q25. The letter of engagement that sets out the scope and objectives, and agrees the hours and budget. That went to the Council, is that what you are suggesting?

The Risk and Governance Advisor advised that there is a contract between the Auditor and the City.

Q26. I am not questioning the procurement side of this, that is a different matter. I am determining the independence of how the scope and objective and hours of the arrangement have been agreed. It appears it is more of a consulting work than an audit. Who signed the letter of engagement? When we do an audit we have an entry meeting and we have a letter of engagement that is signed off. So who put their pen to paper?

The Risk and Governance Advisor advised that that he is he Authorised Officer for audits.

Q27. What were the hours and budget for this audit.

The Risk and Governance Advisor advised that as previously stated, the budget for an internal audit is $70,000 and the budget for an external audit is $100,000.

This particular audit was budgeted at $13,000, and the invoice was for $13,860. There were three tenders for the audit, and they were all in the ballpark for that figure. We chose ES2 as it was a WALGA endorsed Auditor, and ES2 were the only ones that had experience. As previously stated, there is no legislation involved here. It is to see how we are going to meet legislation if it is ever introduced. ES2 where the only Auditors with this experience that came forward.

Q28. Would the hours correspond to about 70 hour?

The Risk and Governance Advisor advised that the question would be taken on notice as he was not certain of the exact number of hours, however there were 53 people interviewed and it was quite comprehensive.

Q29. Was there any audit sample testing from the information on the agenda and the report and the summary? It was a great consulting piece of data gathering by interview and drafting policies of City, but in terms of chewing up a fairly hefty portion of the overall audit budget, there does not seen to be any sample testing of any review of personal information held and destruction policies. It is more just information gathering. Do you know whether there was any audit sampling that has been conducted?

The Risk and Governance Advisor advised that there were numerous documents audited by the auditor, including the way we store information, and some of the information that was taken is through audio, video, USBs, manually (people come in and write information about what they want Council to do). There were tomes of evidence gathered by the Auditor for the audit, and is all recorded in ECM.

7. CONFIRMATION OF MINUTES

7.1 (2020/MINUTE NO 0007) MINUTES OF THE AUDIT & STRATEGIC FINANCE COMMITTEE MEETING - 19/03/2020

RECOMMENDATION
That Committee confirms the Minutes of the Audit & Strategic Finance Committee Meeting held on Thursday, 19 March 2020 as a true and accurate record.

COMMITTEE RECOMMENDATION
MOVED Mayor L Howlett SECONDED Cr C Terblanche

That the recommendation be adopted.

CARRIED 5/0

8. DEPUTATIONS

Nil

9. BUSINESS LEFT OVER FROM PREVIOUS MEETING (IF ADJOURNED)

Nil

10. DECLARATION BY MEMBERS WHO HAVE NOT GIVEN DUE CONSIDERATION TO MATTERS CONTAINED IN THE BUSINESS PAPER PRESENTED BEFORE THE MEETING

Nil

11. COUNCIL MATTERS

11.1 (2020/MINUTE NO 0008) RISK INFORMATION REPORT

Author(s) J Fiori
Attachments N/A

RECOMMENDATION
That Council receive the Risk Information Update Report.

COMMITTEE RECOMMENDATION
MOVED Cr C Terblanche SECONDED Mayor L Howlett

That the recommendation be adopted.

CARRIED 5/0

Background

An overview of the City's Risk Management Framework was submitted to the Audit Committee in 21 March 2019. This overview included an update of the City's risk register comprising both strategic and operational risks. A report detailing a review of the City's strategic risks was submitted to the Audit Committee in 18 July 2019.

The purpose of this report is to provide an update of the City's risk register incorporating an administrative review conducted in November 2019 and subsequent review since the 15 March 2020 declaration of the State of Emergency in Western Australian due to the COVID-19 pandemic.

Submission

N/A

Report

A. Strategic Risk Review

At its 8 August 2019 meeting, Council adopted the recommendation from the 21 March 2019 Audit Committee meeting to replace 25 strategic risks with seven identified strategic risks. These new risks now comprise the City's Strategic Risk Register.

B. Continual Improvement

Continual improvement of the risk management framework was supported by a November 2019 review of operational risks in *RMSS*, the City's on-line risk management and incident reporting system, and a better understanding of the City's risk profile.

The review of operational risks identified some repetitions in risks recorded during the *RMSS* implementation – leading to a decrease in the number from 252 to 230 operational risks in the City's Operational Risk Register.

Additionally, the City's risk profile has changed, as a result of:

- Review of operational risk profiles in November 2019 – leading to changes in the risk profile of some operational risks through improvement of controls and implementation of risk treatment plans by risk managers and risk action responsible officers; and
- Increasing the risk profile from *Moderate* to *Extreme* for strategic risk number 300 '*Business continuity and crisis management*', following the declaration of the 15 March 2020 declaration of the State of Emergency in Western Australian due to the COVID-19 pandemic.

A summary of the changes in the City's risk register following the Strategic Risk and Continual Improvement detailed above is shown in Table 1 below:

Table 1: 2019 – 2020 Comparison of risks in the City's risk register

Risk type	Risk level	21 Mar 2019		29 Jun 2020		Change in count	
						Individual	Total
Strategic risks	Low risks	3	Total number = 25	0	Total number = 7	-100%	-72%
	Moderate risks	15		3		-80%	
	Substantial risks	5		3		-40%	
	High risks	2		0		-100%	
	Extreme risks	0		*1		*+100%	
Operational risks	Low risks	121	Total number = 264	125	Total number = 230	+3.2%	-9%
	Moderate risks	133		97		-27.1%	
	Substantial risks	9		7		-22.2%	
	High risks	1		1		0%	
	Extreme risks	0		0		0%	
Total strategic and operational risks		**289**		**237**		**Reduced by 18.0%**	

*This is risk no. 300 '*Business continuity and crisis management*'.

As at 29 June 2020, the risks populating the risk register are illustrated by the number of risks superimposed in the risk matrix together with a brief description of the risk rating, as shown in Figure 1 below:

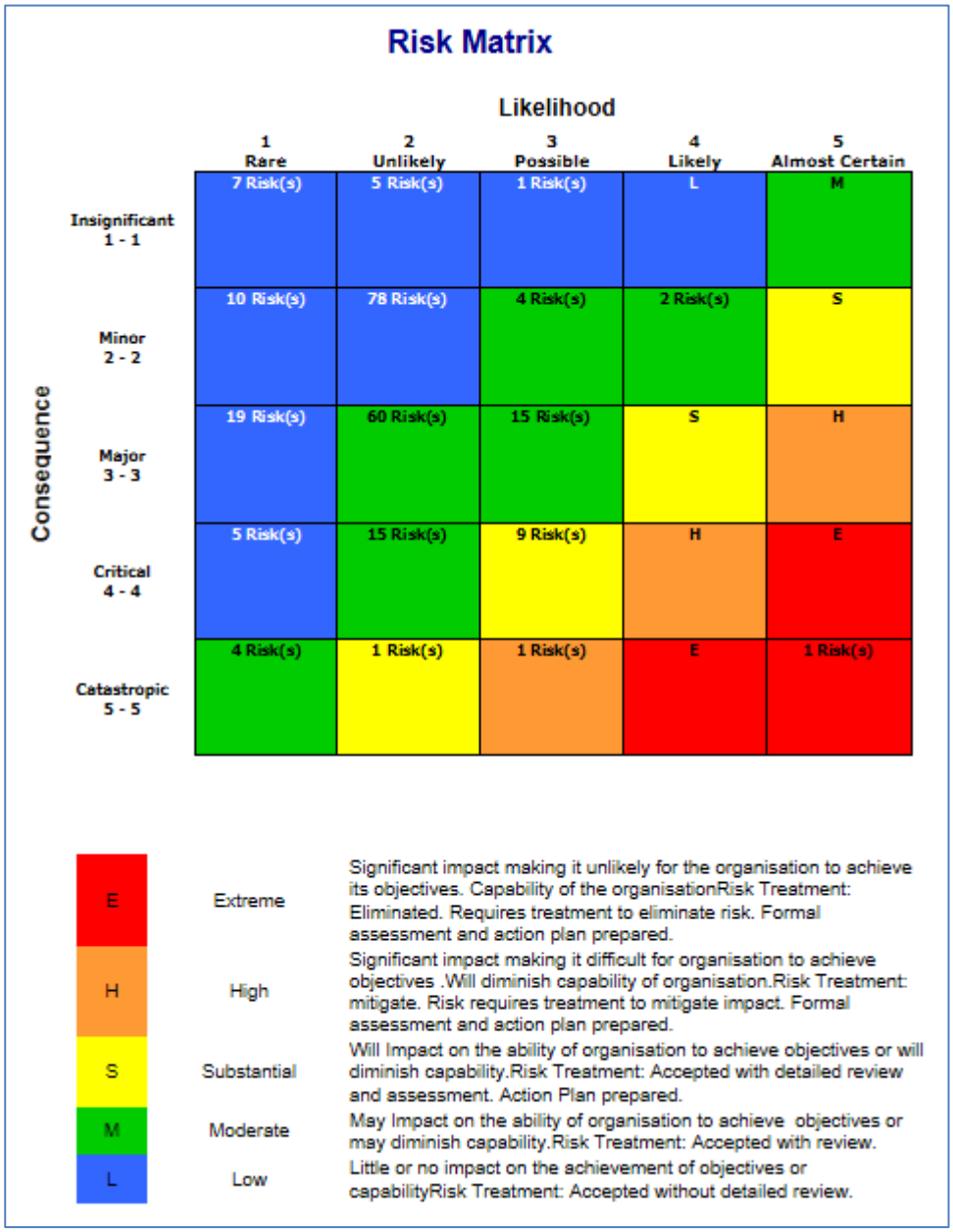


Figure 1: Risks as at 29 June 2020 superimposed on the City's risk matrix

To highlight the overall improvement that the City has made in managing the risks in the Risk Register, a comparison of the risk ratings during the period 21 March 2019 to 29 June 2020 shows the total number of risks rated:

- ***Low*** has increased from 42.91 to 52.74%;
- ***Moderate*** has decreased from 51.21 to 42.62%;
- ***Substantial*** has decreased from 4.84 to 4.22%; and
- ***High*** has decreased from 1.04 to 0.42%.

However, as detailed above earlier, the declaration of the 15 March 2020 declaration of the State of Emergency in Western Australian due to the COVID-19 pandemic has led to increasing the risk profile from ***Moderate*** to ***Extreme*** for strategic risk number 300 '*Business Continuity and Crisis Management*'.

The above summary is illustrated by the pie charts In Figure 2 below:

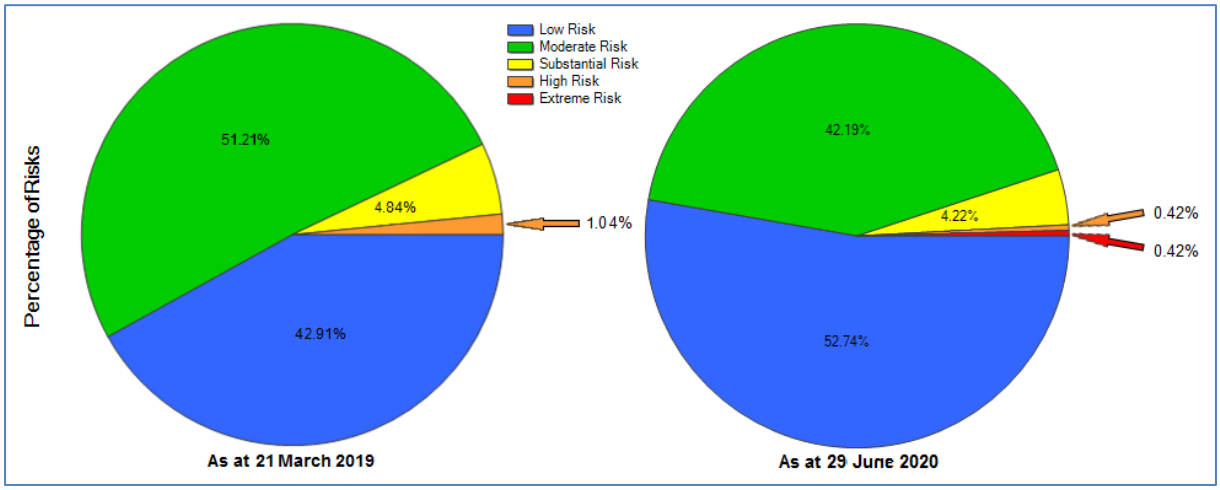


Figure 2: Comparison of risk levels in period March 2019 to June 2020

C. Summary of Strategic Risks rated ***Substantial*** and higher.

Following adoption of the seven (7) new strategic risks by Council on 8 August 2019 to replace the original 25 strategic risks, the sever (7) new risks are now in *RMSS*, and the superseded 25 risks have been archived.

As a result of the COVID-19 Pandemic, the risk profile has increased from ***Moderate*** to ***Extreme*** for strategic risk number 300 '*Business Continuity and Crisis Management*'. Three new strategic risks have been rated as ***Substantial***, and these are summarised in Table 2 below:

Table 2: New strategic risks rated *Extreme* and *Substantial*

Risk ID	Rating	Risk name	Risk description	Action plan
300	Extreme	Business continuity and crisis management	Failure to provide business continuity of the City's core services in the event of a major crisis/emergency.	1. On-going testing and review of the City's response plans; 2. On-going testing and review of the City's local emergency management plan; and 3. Develop business continuity plans for other identified critical service locations, including review of the City's *Infectious Disease Pandemic Business Continuity Plan*, March 2020.
294	Substantial	Strategic direction	Lack of clear and aligned strategic vision, direction and implementation.	1. Investigate digital platforms for information and reporting strategies (i.e. *IntraMaps* software) to increase visibility and alignment; and 2. Report and itemise individual informing strategies financial implications in the *City of Cockburn Long Term Financial Plan 2019-2020 to 2032-2033*. 3. Utilising *CAMMS* software system to implement a new strategy, management and KPI reporting system.
295	Substantial	Technology use and change	Failure to identify, manage and capitalise on the effective and efficient use of changing technology.	1. Develop and implement *City of Cockburn 2019-2023 Digital Cockburn - A Smart City*; and 2. Conduct cyber security governance audits.
296	Substantial	Project management planning	Failure to consistently plan for Capital Works projects.	1. Project development manager resource; 2. Project portfolio management phase 2

Risk ID	Rating	Risk name	Risk description	Action plan
				implementation; and 3. Better implementation of asset management action plans (programming)." 4. Review the City's existing Project Management Communications software system(s) and develop specifications and a procurement plan. The *Project Portfolio Management* (PPM) solutions roll out is ongoing with additional users upskilled/trained and allocated access in the production live environment. Furthermore, there is project management culture improvement in understanding and appreciation of the *Quality Management Triangle*. In addition, there has been increased improvement and automation of Project Management information reporting with Executive Management Report (EMR) and detailed project dashboards. Continued upskilling and development is planned through the year. The COVID-19 pandemic has impacted the roll out momentum as taken away upskilling and shadowing engagements with participants. Time, focus and workload remains the biggest challenge for users' roll out which will need emphasis to ensure PPM users remain engaged, especially with this high knowledge management level required to be retained, else will require retraining.

D. Summary of Operational Risks rated ***Substantial*** and higher

Following the review of the risk register in November 2019, only one operational risk was found to be rated ***High*** and seven operational risks were found to be rated ***Substantial***, as summarised in Table 3 below:

Table 3: Operational risks rated *High* and *Substantial*

Risk ID	Rating	Risk name	Risk description	Action plan
208	High	Community Services major projects	Failure to coordinate recreation and community safety services major projects on behalf of the City.	All new Capital Works Projects in the Community Services Directorate to be processed through the new Project Performance Management (PPM) (on line) System
38	Substantial	Port Coogee Marina - Environment	Failure to provide a safe & secure environment at the Port Coogee Marina.	Development and continual review of *City of Cockburn Port Coogee Marina Safety and Emergency Management Pla*n, October 2018.
62	Substantial	Free public wireless internet	Inability to provide safe and secure free public wireless internet at Cockburn community facilities.	Public Wi-Fi is kept logically separate from production data. Terms and Conditions in place to mitigate liability.
121	Substantial	Seniors Centre food services	Failure to provide food safety requirements and customers' expectations in regards to Seniors Centre.	1. Qualified Staff in the kitchen; 2. Food safety training completed with all volunteers; 3. Regular Health Inspections completed by City; 4. Monthly surveys completed by members and feedback taken into consideration; 5. Suggestion from members taken on board for example we held an Italian day 15 August 2018 with Italian food; and 6. Suggestion box is monitored and feedback taken on board provided to the members.

169	Substantial	Bushfire legislation	Failure to meet bushfire legislation obligations.	1. All inspections have been made in the rural areas; and 2. Funds are on budget to employ a specialist staff member for this role to ensure compliance and consistency.
246	Substantial	Community support	Failure to obtain community support for strategic planning functions.	1. Procedures and policies. Training and development; and 2. Detailed consultation planning for projects.
285	Substantial	Landfill capping	Failure to fund the capping of existing exposed landfill cells.	1. The short term costs associated with the implementation of these plans is progressing well; and 2. The HWRP Financial Model requires that significant funds are available to meet the City's obligations under our Licence requirements in capping and post closure for 19-20.
287	Substantial	Cyber security	Failure to secure the City's data and information systems.	1. Attended Government Innovation summit to understand the City's level of innovation and embracing of new technologies in relation to other government organisations; 2. The City is already on track with efforts in digitising its services; 3. Also in the process of creating a digital strategy to provide a framework for innovation, thinking digital first, and the inclusion of Smart Cities; and 4. Implemented the City's *Information and Cyber Security Policy* in September 2019.

Strategic Plans/Policy Implications

Leading and Listening

Deliver sustainable governance through transparent and robust policy and processes.

Budget/Financial Implications

Nil

Legal Implications

N/A

Community Consultation

N/A

Risk Management Implications

Failure to adopt the recommendations will result in the inability to support an integrated and effective approach to risk management and lack of guidance on the arrangements for designing, implementing, monitoring and continually improving risk management process.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

12. PLANNING & DEVELOPMENT DIVISION ISSUES

Nil

13. FINANCE & CORPORATE SERVICES DIVISION ISSUES

Nil

14. ENGINEERING & WORKS DIVISION ISSUES

Nil

15. COMMUNITY SERVICES DIVISION ISSUES

Nil

16. EXECUTIVE DIVISION ISSUES

16.1 (2020/MINUTE NO 0009) AUDIT REPORT - DATA AND INFORMATION

Author(s) J Fiori

Attachments 1. ES2 - City of Cockburn - Privacy Impact Assessment - Final Report

RECOMMENDATION
That Council adopts the findings and recommendations of the Privacy Impact Assessment Audit Report as attached to the Agenda.

COMMITTEE RECOMMENDATION
MOVED Cr C Terblanche SECONDED Mayor L Howlett

That the recommendation be adopted.

CARRIED 5/0

Background

Rated a ***Moderate*** risk, this audit to assess the City's privacy protection posture against any legislative/regulatory requirements or best practices and to review compliance with the City's own privacy-related policies was scheduled for completion in 2019-2020 in accordance with the *City of Cockburn Strategic Internal Audit Plan 2019 – 2020*.

Bringing this audit report through the Audit and Strategic Finance Committee to Council marks the completion of this audit objective and advises what measures have or will be taken to address or further mitigate identified risks to the City.

Submission

N/A

Report

ES2, a WALGA preferred Perth-based West Australian enterprise security and solution service provider was engaged in December 2019 to undertake an audit to determine what type of personal and sensitive information is held by the City and what the privacy considerations for the held data are. ES2 conducted the audit, in accordance with AS ISO 31000:208 *Risk Management - Guidelines*, between February and March 2020, interviewing 52 City Officers from 37 business units, and presented a final report to the City in May 2020.

Audit Scope

The scope of this audit was to assess the compliance of the City's privacy protection process against:

- any legislative/regulatory requirements;
- the City's own privacy-related documentation; and
- Western Australian public sector best practice.

In the context of this audit these meanings apply:

- *Confidentiality* - the protection of information sharing without the express consent of the owner; and
- *Privacy* - freedom from intrusion into private personal matters.

It is necessary to reflect that the information collected by the City is dynamic in nature and may become personal data sometime after it has been collected. An outcome of this audit will be awareness of the private data and Personally Identifiable Information (PII) that the City handles, where it is kept, how it is utilised and the risk associated with that information.

The findings of this audit should enable the City to develop appropriate documented processes for the collection, use, disclosure and securing of private data and PII in accordance with the requirements of the proposed Western Australian Government (the State) privacy and responsible information sharing legislation announced as a Government Media Statement on 5 August 2019. These appropriate processes should be supplementary to the City's Governance and Risk Management Frameworks.

Another outcome of this audit is to guide the City when reviewing the City's privacy statement, and privacy collection notices, and to develop a privacy policy, which are key components of privacy compliance.

In order for the City to approach privacy compliance with proposed State legislation, this audit of the City's privacy protection process is to be conducted by an independent external auditor, to identify and report on the personal information held by the City and the way in which that information is handled.

Audit Observations

In the absence of applicable State legislation, ES2 labelled this audit *Privacy Impact Assessment* and examined how the City's Officers handle PII, and how this may be affected by future legislation.

The auditor found that there are many areas of the City's operations where good practices are in place and are cognisant of the need to protect the reputation of the City.

The audit identified 25 recommendations, many of which need to be applied City-wide. Each recommendation was assessed in relation to the risk it was mitigating. Risk levels were determined by the auditor using a risk matrix contained in the City's Risk Management Framework.

Significant findings were:

- A Council Privacy Policy needs to be developed and implemented (a draft City privacy policy has been developed and is currently being reviewed); and
- In some processes, the City is at risk of being non-compliant with the Payment Card Industries (PCI) requirements to protect credit card information.

The 25 recommendations made by the auditor, assessed in relation to the risk being mitigated, were as follows:

- Three (3) were rated as ***High*** risk;
- Ten (10) were rated as ***Substantial*** risk; and
- Twelve (12) were rated as ***Moderate*** risk.

All recommendations are listed in the table below:

Recommendation	Risk Impact	Risk	Action Plan
5. Supplier Security City develops and implements supplier security policy, including due diligence requirements for cloud services, to assure the use of cloud services does not compromise the position of the City with regard to the protection of privacy information entrusted to the organisation.	The current threat environment has: • supply chain attacks as being one of the most common approaches by attackers; and • the potential is for incidents to occur which require third party actions or investigation.	16 High	• Specific supplier security policy is not required - this should be captured within the City's proposed *Privacy Policy* specific to data security requirements within the City's systems.
11. Secure Destruction City develops, approves and implements policy or procedure for secure destruction. This document needs to define the acceptable means of destruction based on the classification or sensitivity of the document or media in question. This instruction needs to ensure that information cannot be compromised through inappropriate destruction or disposal processes.	Should information be retrieved through inadvertent disposal processes there is considerable potential for: • damage to the City's reputation; and • public embarrassment for the City.	16 High	• Possible inclusion of PII review at next policy review (2 years); • Hardware Destruction Guideline to be developed by ICT.

Recommendation	Risk Impact	Risk	Action Plan
25. USB Scan City develops and implements Anti-malware scanning procedures for those departments where information is received from customers via a USB device. This will provide considerable protection from the potential for malicious software or a virus to become installed on the City's IT equipment.	With current processes, there is a threat that the use of uncontrolled USB devices could result in: • virus infection of the City's systems; • malicious software may be surreptitiously installed; • damage to the City's reputation; and • public embarrassment for the City; and • attract high level of media attention.	16 High	• Investigating various USB device control systems (group Policy).
1. Risk Documentation Releasing Personally Identifiable Information (PII) to be documented as a risk and be treated, regardless of legislative requirement.	Breaches are possible and happen far too often. Has the potential to: • do damage to the City's reputation; • do damage to customers; and • result in legal action being taken against the City.	12 Substantial	• As part of the *City of Cockburn Risk Management Framework* [ECM Document ID 8882597], all recommendations emanating from the ES2 audit report *City of Cockburn Data and Information Audit (Privacy Impact Assessment)* May 2020, will be accepted as opportunities for improvement, converted to risks and assigned their own risk owners and risk treatment officers. • The risks will be entered into *RMSS* to ensure these are being managed and mitigated in accordance with the City's established risk management framework.
6. Freedom of Information (FOI) City develops documented policy and process for dealing with FOI requests, prior to any information release, to protect the City against release of Personally Identifiable Information (PII).	Without governance overview prior to any information released, the City may inadvertently release information which contains PII, with the potential to: • do damage to the City's reputation; • do damage to customers; and • result in legal action being taken against the City.	12 Substantial	• The City complies with the requirements of the *Freedom of Information Act 1992* and *Freedom of Information Regulations 1993*. • The City will develop and implement a FOI procedure, together with providing organisational training on its usage, to mitigate against the risk of releasing PII.

Recommendation	Risk Impact	Risk	Action Plan
7. Privacy Policy City develops, publishes and communicates a Privacy Policy to cover all of the City's dealings with PII. Regardless of the requirement for compliance, this is a requirement to reduce the potential risk to the City's reputation should PII be inadvertently compromised. Additionally, the Policy would provide a much needed consistency in the way that the City's business units handle and store PII.	In the event that PII is mishandled, through the lack of consistent Privacy Policy, the following could result: • damage to the reputation of the City; and • public embarrassment for the City.	12 Substantial	• The terms of reference for this audit report included providing a template for developing a privacy policy for the City. • In the absence of WA legislation, a draft City privacy policy has been developed - assistance of an external service provider will be considered.
8. Video Recording City develops procedures to ensure PII is either blocked from video and audio recordings unless the PII subjects provide written approval for their information PII to be published along with the audio and video of Council meetings. May be achieved by prior notification of the recording, publishing of the recording being provided to all meeting participants, or by requiring all meeting participants to sign agreement that any information spoken during the meeting will be published on the Internet.	In the event that PII is published via Council vision and audio without the consent of the subject, the following could result: • damage to the reputation of the City; and • public embarrassment for the City.	12 Substantial	• Draft Live Streaming Procedure has been developed with the assistance of Manager Corporate Communications, Digital Communications Officer, Communications Assistant, Civic Support Officer, Media and Communications Officer, Customer - Service Coordinator and the Governance Services Team.
9. *Dropbox* City discourages the use of *Dropbox* City-wide in favour of using the more secure option of OneDrive. In particular it needs to be prohibited for the use or storage or transfer of PII.	In the event of an information security breach with the *DropBox* cloud application, the following could result: • damage to the reputation of the City; and • public embarrassment for the City.	12 Substantial	• Proposed *Mimecast* Large File Send (2GB Limit); • *OneDrive Business* with Multi-Factor Authentication (MFA) and Data Loss Prevention (DLP) controls is proposed by ICT.
17. Credit Cards All credit card transactions be centrally organised and conducted by a single City of Cockburn Department.	The decentralised storage and handling of credit card information impacts on the City by increasing the potential for: • a breach of credit card information.	12 Substantial	• Centralised handling of credit card payments proposed by Financial Services. • All application forms are sent to the Revenue team to process.

Recommendation	Risk Impact	Risk	Action Plan
18. Payment Card Industries (PCI) Compliance City undertakes a PCI assessment to establish the level of compliance with the PCI-DSS. This assessment should include the use of the Card Recognition scanning software: (https://www.groundlabs.com/card-recon/) which will scan the entire network to identify all locations where Credit Card information exists. This will go a long way to identifying the levels of risk posed to the City should credit card information be breached and made public.	Credit card information is contained in a number of undesirable locations within the City's infrastructure, increasing the potential for: • a breach of credit card information.	12 Substantial	• Credit card information on physical forms is redacted by service units and the Records Services. • Risk level for the City does not warrant a card recognition scan.
19. Policy Content The Privacy Policy that is recommended to be developed to support the City includes all anticipated PII use that the City collects. The policy is published and used to advertise use of collected PII to all persons that entrust that information to the City.	The Privacy Policy is used to define the limitations of the City's use of PII. Failure to comply with the City's own published Privacy Policy would possibly result in: • damage to the reputation of the City; and • public embarrassment for the City.	12 Substantial	• The development of, implementation and associated training for, City privacy policy will be commenced by Q1 2020-2021 FY.
22. Policy Coverage The *Privacy Policy* that is recommended to be developed to support the City, include the personal information pertaining to City employees in order to assure their protection the same as the protection of customer information.	The privacy policy is used to define the limitations of the City's use of PII, inclusion of employee information within the cover of PII. Any breach of personal information of employees can possibly result in: • damage to the reputation of the City; and • public embarrassment for the City.	12 Substantial	• Development of a formal HR policy is proposed by HR Services.
23. Policy Improvement City updated and improved *Childcare Services Privacy Policy* in conjunction with the development of the overall City of Cockburn proposed *Privacy Policy*. The wording within the policy must be definitive and easily understood to remove any conjecture and ensure that the policy is enforceable and that failure to comply with policy can be dealt with through the City's disciplinary process.	The privacy policy in place to cover Childcare Services needs to be reviewed and updated to make it enforceable. Failure to comply with policy through misinterpretation or lack of content can possibly result in: • damage to the reputation of the City; and • public embarrassment for the City.	12 Substantial	• Existing *Childcare Services Privacy Policy* is in place, and will be reviewed as appropriate.

Recommendation	Risk Impact	Risk	Action Plan
4. Software Application - *Lucky Orange* In compliance with the *City of Cockburn Information and Cyber Security Policy* conduct a review of the *Lucky Orange* service to identify the potential risk to the City through its use. Particular emphasis needs to be placed on the applications coverage of privacy information and financial information.	Non-compliance with the requirements: • for the handling; and • protection of credit card information.	9 Moderate	• Records Services have investigated retrospectively redacting existing records; • Undertake Payment Card Industry (PCI) self-assessment proposed by Financial Services; • Review existing processes and remove credit card boxes from all processes.
14. Social Media A 'two-person rule' process be implemented to ensure that all information published in the name of City of Cockburn on Social Media be reviewed and approved prior to publication/posting.	In the event that personal information is inadvertently published on Social Media in the name of the City of Cockburn it is possible that this would result in a: • public complaint; and • attract moderate media attention.	9 Moderate	• Develop a checklist for checking posts in addition to colleagues citing them.
13. Infringement Collection The City utilises an offshore collection agency for the recovery of library assets - Library Service users should be informed of this. When a customer signs up for Library Services the customer needs to be informed that in the event of an infringement their personal information will be passed to a US (foreign) based asset recovery agency. Customers must agree to this prior to membership.	Where customers have not agreed to their personal information being sent to an offshore organisation, it is possible that a breach would result in: • a public complain; and • attract moderate media attention.	9 Moderate	• When applying for a library membership applicants must agree to: *'Conditions of Membership*' which contains the statement: 'It is your responsibility to return items by the due date, irrespective of whether or not you receive a reminder notice from the library. If loans become 4 weeks overdue you will be invoiced for the replacement cost of the items and your borrowing rights suspended until items are returned or paid for. Failure to respond within 14 days of the date of this invoice may result your account being referred to a materials recovery agency. In this event, your name, contact details, and amount owing will be passed on to a US based materials recovery agency and an additional recovery fee will be

Recommendation	Risk Impact	Risk	Action Plan
			applied to your account.
15. Volunteers The City reviews online forms to include a 'permission to share information' component. This would then act as the authority from the subject to distribute their personal information to relevant volunteer organisations. Volunteer organisations receiving information must be subject to an NDA in order to assure that they are aware of the potential damage that could be caused if this information was subject to a security breach.	In the event that personal information of a volunteer is inadvertently released or breached by a third party that the City had passed this information onto, then it is possible this would: • result in a public complaint; and • attract moderate media attention. The above unwanted events would increase exponentially where more than one person's information is included in a breach.	9 Moderate	• The Volunteer Resources Centre does not distribute or share, volunteer personal information with other relevant organisations; • On-line and manual systems in place are set up in such a way that where sharing is needed the volunteers provides their details directly to the third party; • A privacy statement is included on the web page accessed; • There are documented procedures / work instructions and team members training regarding systems.
21. Security Classification The City of considers implementing an Information Security Classification Framework (ISCF) across the City's information enterprise architecture. An ISCF scheme groups information based on the potential damage / impact / consequence to the City should that information be subject to a breach of confidentiality. The City should implement a simple ISCF, whose main aim is to be able to identify that information which requires the most protection, including PII. Once the classification levels have been determined then appropriate protection, storage and handling processes per classification can be established. The recommended ISCF is to be aligned to the one implemented by the Australian government, with levels that include *Official* and *Official*	Without implementing a ISCF scheme it is: • difficult for City staff to understand the impact should a piece of information be subject to a security breach; and • it is likely that a breach of PII may not be identified and may attract moderate media attention.	9 Moderate	• Implement information classification framework. • Retrospectively apply to existing data.

Recommendation	Risk Impact	Risk	Action Plan
Sensitive as defined in the; • *Australian Government Information Security Manual*, Australian Cyber Security Centre, Canberra, June 2020; and • *Protective Security Policy Framework*, Attorney-General's Department, Canberra, October 2018.			
24. Electronic Systems Information, Communication & Technology Services works with the Youth Services team to overcome issues with confidence in IT system confidentiality. PII needs to be stored electronically in order to assure that it receives the appropriate level of protection. Paper based files should be transferred to an electronic system and then destroyed.	Having all information stored on paper provides an opportunity for: • theft; • unauthorised copying • loss of information in the event of fire; and • loss of availability of information or loss of confidentiality due to theft, or fire. The above events may attract moderate media attention.	9 Moderate	• Youth Services Manager and support staff to meet with Records Management to identify a secure way of including client records into the Organisation ECM system that provides assurance of strictest confidentiality levels. While providing access to support staff on a daily as required basis. • City to investigate Purchasing a stand-alone electronic system for the sole purpose of client records. • Contract in an admin officer to periodically (annually) scan recently closed client files and archive securely in the City's secure electronic system.
16. Access Security Authorise the use of computers that provide access to systems which contain PII, by requiring unique set of login credentials for each user. This ensures that all actions performed by a computer user are accountable and traceable to a specific person.	If a person is able to anonymously access PII by using a generic and untraceable access account, there is the potential for PII to be breached resulting in: • public complaints; and • media attention.	9 Moderate	• Existing process recommends named user access for all accounts, but is not enforced. • Enforce unique named accounts.
10. *S* Drive Conduct a campaign of information storage awareness training. This training should concentrate of what information is or is not	Use of the *S* Drive is likely to result in a breach that is limited to within the confines of the City's departments - limiting the consequence of any resulting damage.	8 Moderate	• Existing Records Management Policy in place; • Existing Employee Record Keeping

Recommendation	Risk Impact	Risk	Action Plan
suitable for storage on the *S* Drive and how information should be managed. The minimum recommended content for training would be: • What information needs to be stored on *ECM* or in T*echnologyOne*; • Housekeeping of information within *ECM*. • What information must not be stored even temporarily on the *S* Drive; • What information may be stored on the *S* Drive; • User's responsibilities with regard to the retention of information; • User's responsibilities with regards to the destruction of hard copy information; and • Training should apply to all staff and management of the City.			Guidelines in place; • Existing Knowledge Management Project in place.
12. *F* Drive Review the *F* Drive to establish if here is any PII stored on the drive - if there is, then migrate this PII to ECM as a priority.	Use of the *F* Drive is likely to result in a breach that is limited to within the confines of the City's departments - limiting the consequence of any resulting damage.	8 Moderate	• Implement *ECM Connected Content* for Contracts; • Procurement in process of moving all records into ECM.
20. *Outlook* Storage Conduct a campaign of information storage awareness training to discourage users from using Microsoft *Outlook* as a file storage system.	Use of *Outlook* as a storage location is likely to result in a breach of PII that is limited to within the confines of the City's departments, limiting the consequence of any resulting damage.	8 Moderate	• Continue with existing Knowledge Management Project.
2. Opt-Out Compliance with the Australian government's *Privacy Act 1988* (Cth), by permitting persons to opt out of receiving direct marketing. This is most often achieved by including: • an 'unsubscribe' link in an email or a process whereby a person can reply to an email; or • SMS message with 'Unsubscribe' or 'Stop'.	Based on the City's current practices, possible non-compliance with: • the Australian government's *Privacy Act 1988* (Cth); or • any future implementation within WA.	6 Moderate	• Add to the risk register for Corporate Communications to check with Managers and Supervisors that any e-newsletters or use of SMS includes opt out option.

Recommendation	Risk Impact	Risk	Action Plan
3. Non-Disclosure Agreement (NDA) Develop and implement NDA to ensure that collected PII is not shared outside of the City of Cockburn (outside of the sphere of the proposed City *Privacy Policy*), to assure that the collected PII information is handled and protected in the manner intended through the proposed *Privacy Policy*.	Non-compliance with: • *Privacy Policy* (assuming that City's *Privacy Policy* is developed and approved); and Damage to City's reputation, if: • *Privacy Policy* has been developed and approved.	6 Moderate	• Confidential clauses and Intellectual Property requirements are part of existing contracts and agreements. • Specific NDA / Contract are developed as required (e.g. with Universities, GIS, etc.).

Improvement Opportunities

All 25 recommendations from this audit have been identified as risks to the City, and as opportunities for improvement.

Risk owners and Risk Treatment Officers have been assigned to the identified risks. The risks will be managed and their progress monitored by entering them into RMSS, the City's online Risk Management Systems.

Strategic Plans/Policy Implications

Leading and Listening

Deliver sustainable governance through transparent and robust policy and processes.

Budget/Financial Implications

N/A

Legal Implications

N/A

Community Consultation

N/A

Risk Management Implications

Managing these audit findings as risks in RMSS, and implementing appropriate control measures, or risk treatments, will ensure compliance with future proposed State privacy and responsible information sharing legislation. Simultaneously, this audit will provide an opportunity to improve controls to ensure the City is not inadvertently exposed to any undesired risk.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

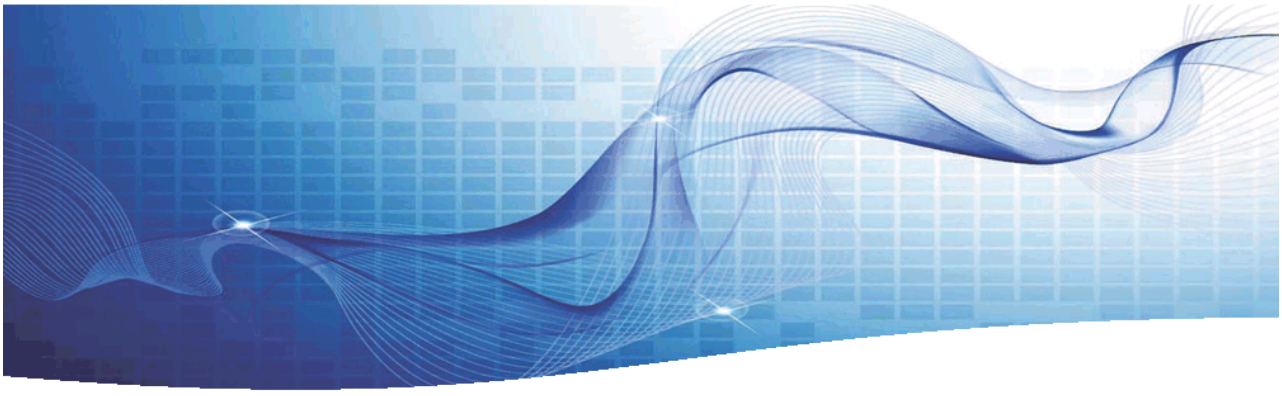
ENTERPRISE SECURITY ENTERPRISE SOLUTIONS

Report

City of Cockburn

Data and Information Audit

(Privacy Impact Assessment)



Published: 04/05/2020

Ref: 20-WA-COC-SE-10

ES2 PEOPLE ES2 KIDS ES2 IR INCIDENT RESPONSE

Document Set ID: 9373590
Version: 1, Version Date: 21/05/2020

Data and Information Audit (Privacy Impact Assessment)

Document Information

Author/Custodianship

Author:	Steve Simpson
Custodian:	ES2
Type:	Report

Document Version History

Version	Date	Change By	Amendment
0.1	12/03/2020	Steve Simpson	Initial Draft Findings Report
0.2	13/03/2020	Christie Wright	QA review of Draft Findings
0.3	25/03/2020	Bernadette Pinto	Review accuracy of Findings
0.4	05/04/2020	Steve Simpson	Initial Draft of Report
1.0	06/04/2020	Christie Wright	Reviewed for Release
1.1	24/04/2020	Steve Simpson	Revised at client request
2.0	28/04/2020	Christie Wright	Reviewed for Release
2.1	04/05/2020	Steve Simpson	Revised at client request
3.0	05/05/2020	Christie Wright	Reviewed for Release

Project Information

Client:	City of Cockburn	**ES2 PM:**	Christie Wright
Project Name:	Data & Information Audit (Privacy Impact Assessment)	**ES2 Stream:**	Security
Client Contact:	Joseph Fiori	**Prepared By:**	Steve Simpson
ES2 Ref	20-WA-COC-SE-10	**Date Produced:**	05/04/2020

Data and Information Audit (Privacy Impact Assessment)

Table of Contents

Data and Information Audit (Privacy Impact Assessment)

1. Executive Summary

ES2 were engaged by the City of Cockburn (the City) to conduct an audit of Privacy Data and Information owned by or entrusted to the City. This audit process is known as a Privacy Impact Assessment (PIA) and examines how the City's departments and employees handle Personally Identifiable Information (PII), how this relates to current legislation and how it may be affected by future legislation.

This engagement has been carried out over a number of weeks through February and March 2020 and has encompassed two presentations and nine workshops. A total of 52 members of City staff were interviewed, covering 37 departments and functions, and providing valuable input into this engagement. The main points of contact within the City were Risk & Governance Advisor and Governance & Risk Officer who organised all interviewees, workshops and presentations. Their assistance has gone a long way to aiding in the accuracy and success of this engagement.

Whilst this engagement concentrates mainly on the areas where improvement to the protection of Personally Identifiable Information has been identified, there are many areas of the City's operations that are following good practices and are putting considerable effort into protecting the reputation of the City.

This report has identified a total of 25 recommendations, many of which need to be applied across the City's enterprise. Each recommendation was assessed as to the risk it was remediating. A summary of all recommendations made within this report has been included at Appendix D. Risk levels were determined by the assessor using the City's risk matrix. The following graph represents the quantities of recommendations per risk level:

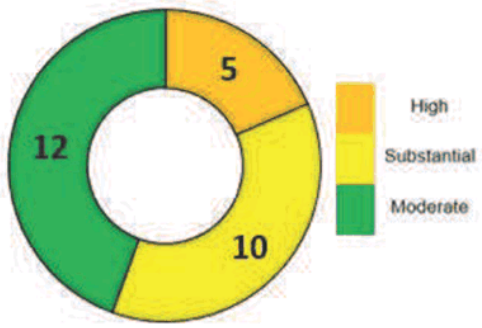


Figure 1 - Recommendations by Risk

In conclusion, the City has been entrusted with a significant amount of PII by its customers and there are a number of areas of the City where improvements can be made to the way that PII is stored, processed and transmitted. The majority of these can be implemented fairly simply with changes to procedures being the main area covered in recommendations.

Whilst not within the scope of this engagement the assessor identified a number of areas where the City is at risk of being non-compliant with the Payment Card Industries (PCI) requirements to protect credit card information. This is a topic that ES2 recommends that the City addresses to further reduce risk.

2. Introduction

2.1. Background

As the result of proactive security measures identified in the *City of Cockburn Strategic Internal Audit Plan 2019 – 2022*, ES2 were engaged by the City of Cockburn to conduct a Privacy of Data and Information Impact Assessment (PIA). The high-level aim of the PIA is to gain a detailed understanding of the receipt, handling, governance and disposal of information that would be considered to be Personally Identifiable Information (PII) under the auspices of the Australian Privacy Act 1988.

2.2. Scope and Approach

The approach used by ES2 consisted of conducting a large number of stakeholder workshops and interviews. In addition, some documentation that was provided by interviewees was analysed in order to get the greatest understanding of the organisations use of Personally Identifiable Information (PII). At a high level the below process was followed through this engagement:

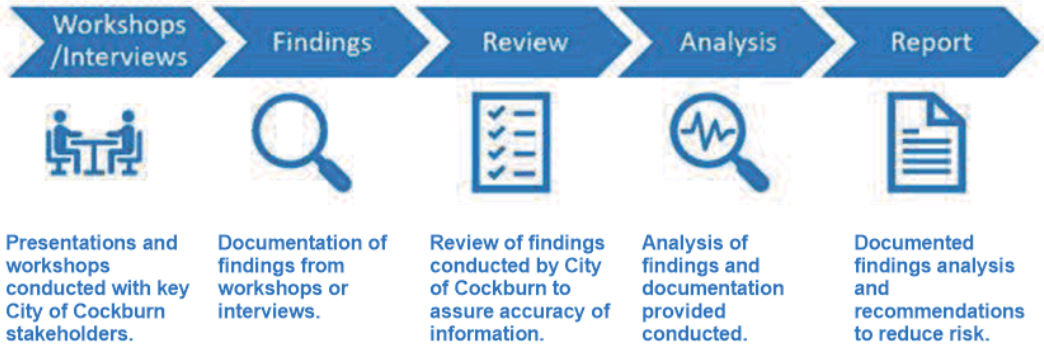


Figure 2 – ES2 PIA Approach

The overall aim of this engagement was - to establish and document the information flows of the project, process or procedure that privacy information is collected for; identify what PII is used for, who it is obtained from and disclosed to, who will have access; and any other necessary information:

- Identify what PII is being collected.
- Identify how PII is being collected.
- Identify what PII is necessary for City of Cockburn requirements.
- Review *City of Cockburn Privacy Statement*
- Identify the stakeholders relevant to PII use.
- Understanding of PII data flows:
  - PII content;
  - Data use;
  - Departments and personnel involved; and

- Security of the information (Access, treatment, transfer, retention, destruction and Disclosure).

This audit will consider how the City collects information and in what format, through various media to include but not be limited to:

- Personal information of the City's citizens/electorate as collected through automated or manual means.
- Employees' personal and confidential information collected through the processes and conditions of employment.
- Telephone recorded messages advising the user about monitoring the call for the purpose of 'customer service training' including monitoring employees' responding to customer enquiries.
- Collection or communication of data via third party services such as *mailchimp*; *google analytics*, *lucky orange*, *DocuSign*, *Kentico* etc.
- Privacy requirements concerning CCTV surveillance cameras installed for recording various activities throughout the City.
- Social media monitoring which may include personal information, sensitive information and what may at first appear as innocuous information, but when combined or correlated with other sources, the information disclosed is private.
- Smart mobile devices which may collect location data (for marketing purposes) and hardware identifiers (for installation of City approved apps).
- Community surveys involving the collection of personal and sensitive data.
- Use of data collected via websites to personalise information presented via the website.

2.3. Risk Levels

Recommendations within this report have been allocated a preliminary risk level based on the City's Risk Matrix provided for this purpose.

Each recommendation within this report has been numbered for ease of reference and the preliminary risk level has been included within this numbering sequence. The following are **examples** of recommendation identification to demonstrate their meaning:

- **[R1-L]** – identifies that the Recommendation number is one (1) and that the recommendation is addressing a risk estimated as being Low.
- **[R2-M]** – identifies that the recommendation number is two (2) and that the recommendation is addressing a risk estimated as being Moderate.
- **[R3-S]** – identifies that the recommendation number is three (3) and that the recommendation is addressing a risk estimated as being Substantial.
- **[R4-H]** – identifies that the recommendation number is four (4) and that the recommendation is addressing a risk estimated as being High.
- **[R5-E]** – identifies that the recommendation number is five (5) and that the recommendation is addressing a risk estimated as being Extreme.

Risk is a subjective topic, the risk estimates within this report is the opinion of the assessor. The City of Cockburn with its vast local knowledge on the topic is likely to have differing opinions with some

risks. Where differences occur, City officers are recommended to act on their own knowledgeable assessment.

The working sheets for the ES2 risk calculations have been included at Appendix B to this report to aid in the City's understanding of the levels of risk associated with recommendations.

2.4. Workshops and Interviews

During the length of this engagement the following City officers were interviewed and provided valuable input into this report:

Table 1 - Interviewees

No.	Name	Role
1	Brett Fellows	Manager Information Services
2	Elliot Tempest	Cyber Security Officer
3	Sam Seymour-Eyles	Manager Corporate Communications
4	Leezelle Cornejo	Digital Communications Officer
5	Bernie Pinto	Governance & Risk Officer
6	Joseph Fiori	Risk and Governance Advisor
7	Anton Lees	Manager Parks & Environment
8	Mike Haynes	Recovery Park Coordinator
9	Lyall Davieson	Waste Manager
10	Lisa Mainwaring	Rates Coordinator
11	Chantelle D'Ascenzo	Rates and Revenue Manager
12	Tony Natale	Strategic Procurement Manager
13	Linda Seymour	Manager Libraries
14	Alex Green	Volunteer Development Services Officer
15	Melissa Bolland	Grants and Research Coordinator
16	Sam Standish	Marina Manager
17	Caroline Lindsay	Marketing and Communications Coordinator
18	Brett McEwin	Cockburn Aquatic and Recreation Centre Manager
19	Michal Callister	Customer Success Coordinator
20	Travis Moore	Manager Recreation & Community Safety
21	Chetan Poutula	Community Safety Project & Innovation Officer

No.	Name	Role
22	Mike Emery	Ranger & Community Safety Services Manager
23	Tamara Bold	Senior Customer Services Officer
24	John West	Manager Building Services
25	Stephanie Walding	Club Development Officer
27	Ashlin Gardner	Community Engagement Advisor
28	Dean Burton	Coordinator Recreation Services
29	Bree D'Sa	Property & Lands Officer
30	Colleen Miller	Customer Service Coordinator
31	Kayley Bazely	Accounts Payable Officer
32	Olivia Milevski	Accounts Payable Coordinator
33	Emma Machura	Records Manager
34	Yawley Yukich	Library Technology Coordinator
35	Michelle Champion	Youth Services Manager
36	Chris McEniery	GIS System Analyst
37	Paul Hogan	Cockburn Community Care Manager
38	Colleen Crowley	Financial Counselling Coordinator
39	Sandra Taylor	Child Care Services Manager
40	Renae Greenway	HR Business Partner
41	Vanda Bacich	Civic Support Officer
42	Adrianne Vasile	PA to Mayor and Elected Members
43	Phil Oorjitham	Environmental Health Coordinator
44	Colin Macmillan	Engineering Works Manager
45	Julie McDonald	Senior Centre Coordinator
46	Sandra Galati	Civic Administration Officer
47	Simone Sieber	Community Development Coordinator
48	Joan de Castro	Children's Development Officer

No.	Name	Role
49	Sinta Ng	Accounting Services Manager
50	Natalie Turner	Disability Access & Inclusion Officer
51	Marlee Kickett	Aboriginal Community Development Officer
52	Celina da Costa	Statutory Planning Coordinator

2.5. Terms and Abbreviations

The following terms and abbreviations have been used within this document:

Table 2 - Terms and Abbreviations

Term/ Abbreviation	Definition
APP's	The Australian Privacy Principles
ARC	Aquatic and Recreation Centre
CCTV	Closed Circuit Television
CRM	Customer Relationship Management System
CSA	Child Support Agency
Customer	For the purposes of this document refers to the ratepayers and electorate members under the jurisdiction of the City of Cockburn.
ECM	Enterprise Content Management System
ECR	Enterprise Cash Receipting System (*Technology One*)
EFT	Electronic File Transfer
FOI	*Freedom of Information act Act 1992*
GDA	General Disposal Authority
GIS	Graphic Information Services/Systems
HR	Human Resources
LGIS	Local Government Insurance Scheme
NDA	Non-Disclosure Agreement
OAIC	Office of the Australian Information Commissioner

PA	Personal Assistant
PCI	Payment Card Industry
PCI DSS	PCI Data Security Standard
PIA	Privacy of Data and information Impact Assessment
PII	Personally, Identifiable Information
Subject	The term 'subject' is used to describe the person who PII refers to.
The Act	For the purposes of this document refers to the Australian *Privacy Act 1988* (Cth)
The City	For the purposes of this document refers to the City of Cockburn
WALGA	Western Australian Local Government Association

3. Privacy Requirements

3.1. What is Personal Information?

The Office of the Australian Information Commissioner (OAIC) website defines personal information in the following high-level statement:

> *Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.*

3.2. Global Privacy Law Features

Australia is one of 37 countries that are members of the Organisation for Economic Co-operation and Development (OECD). The Council of the OECD has recommended that member countries take into account in their domestic legislation the privacy principles set out in the 1980 OECD 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data'. Australia has expressed its intention to participate in the recommendation. These principles are implemented through the Australian Privacy Principles (APPs). ES2 feel that it is unlikely that WA would implement a state privacy law that did not include these basic principles.

There are eight OECD Privacy Principles:

1. Collection limitation principle
    a. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data quality principle
    a. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.
3. Purpose specification principle
    a. The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use limitation principle
    a. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 3 except:
        i) with the consent of the data subject; or
        ii) by the authority of law.
5. Security safeguards principle
    a. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness principle
    a. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual participation principle
    a. An individual should have the right:
        i) to obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to him;
        ii) to have communicated to him, data relating to him
            1. within a reasonable time;
            2. at a charge, if any, that is not excessive;
            3. in a reasonable manner; and
            4. in a form that is readily intelligible to him;
    b. to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
    c. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. Accountability principle
    a. A data controller should be accountable for complying with measures which give effect to the principles stated above.

3.3. Australian Privacy Principles

The Australian Government's *Privacy Act 1988* (Cth) was amended in 2014 to include the 13 Australian Privacy Principles (APPs):

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

The OAIC and the APP's define the following information as being considered to be PII:

Information or an opinion about an identified individual, or an individual who is reasonably identifiable; whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

The term 'personal information' encompasses a broad range of information.

A number of different types of information are explicitly recognised as constituting personal information under the *Privacy Act 1988* (Cth). For example, the following are all types of personal information:

- 'sensitive information' (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information);
- 'health information' (which is also 'sensitive information');
- 'credit information';
- 'employee record' information (subject to exemptions); and
- 'tax file number information'.

Although not explicitly recognised as personal information under the *Privacy Act 1988* (Cth), information may be explicitly recognised as personal information under other legislation. For example, under the *Telecommunications (Interception and Access) Act 1979* (Cth), certain telecommunications data (sometimes referred to as 'metadata') is taken to be personal information for the purposes of the *Privacy Act 1988* (Cth).

However, information does not have to be explicitly recognised as personal information to constitute personal information under the *Privacy Act 1988* (Cth). The types of information that are personal information are unlimited and can vary widely.

Further, the definition of personal information is not limited to information about an individual's private or family life but extends to any information or opinion that is about the individual, from which they are reasonably identifiable. This can include information about an individual's business or work activities.

Personal information can range from sensitive and confidential information to information that is publicly available. The definition also makes clear that information will be personal information even if it is incorrect.

Common examples of personal information include information about a person's private or family life including:

- A person's name, signature, home address, email address, telephone number, date of birth, medical records, bank account details and employment details.
- Information about a person's working habits and practices:
- A person's employment details, such as work address and contact details, salary, job title and work practices
- Certain business information – for example, information about a loan taken out by a sole trader to purchase tools for their business, or information about utility usage.

Commentary or opinion about a person:

- In certain circumstances, a referee's comments about a job applicant's career, performance, attitudes and aptitude constitutes personal information. Similarly, a trustee's opinion about a bankrupt's affairs and conduct can be personal information about both parties.
- An opinion about an individual's attributes that is based on other information about them such as an opinion formed about an individual's gender and ethnicity based on information such as their name or their appearance.
- Information or opinion inferred about an individual from their activities, such as their tastes and preferences from online purchases by credit card or their web browsing history.

3.4. WA Privacy Law

The Western Australian government have opted not to align to the Australian government's *Privacy Act 1988* (Cth). As such the *Privacy Act (1988)* (Cth) is not enforceable to WA Government State or Local Government Agencies or Departments. The WA Government's Department of Premier and Cabinet (DPC) have published the following privacy position statement (published on the WA Government website at - https://www.wa.gov.au/government/announcements/interim-privacy-position):

> *Until such time as more substantial guidance and/or legislative measures are available, the interim privacy position for the Western Australian public sector is that agencies should ensure their actions are consistent with applicable Australian Privacy Principles, set out in Schedule 1 to the Privacy Act 1988 (Cth) with primary emphasis upon Principle 6 - "use or disclosure of personal information".*
>
> *Where agencies are operating under statutes that contain specific provisions about the use or sharing of data, they should continue to comply with these.*
>
> *This position applies to personal information, as defined in the Privacy Act 1988 (Cth):*
>
> *"personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *a. whether the information or opinion is true or not; and*
>
> *b. whether the information or opinion is recorded in a material form or not."*

This statement is updated from time to time, the current version is dated May 2018. A key component of this statement is that 'agencies should ensure their actions are consistent'. As such there is no mandatory position enforcing the protection of PII across state or local government departments and agencies.

This statement also states, 'Until such time as more substantial guidance and/or legislative measures are available,'. this implies that there is a plan in place to develop WA specific privacy legislation and it is believed that this has been on the DPC agenda for some time. However, within the experience of ES2, there has not been much movement towards such a development. As such, ES2 encourages through its security engagements that all WA Government agencies and departments align as close as possible to the Federal legislation, the *Privacy Act 1988* (Cth), as being 'best practice' for the protection of PII. It is also worth noting that this Federal legislation deals with employee records differently between public and private sector organisations. The APPs require that public sector

organisations protect the PII of their employees the same as they would a customer or third party. ES2 encourages all organisations to incorporate the same security controls over employee PII as is placed on third party PII.

However, the lack of mandated compliance for WA government agencies and departments with legislation does not prevent or in any way mitigate the reputational damage that would ensue should an agency or department suffer a breach of PII. Reputational damage to local government could be considerable and could through association impact other or all local government establishments.

[R1-S] Risk Documentation Recommendation - ES2 recommends that the potential damage to the reputation of the City of Cockburn that would result from a breach of Personally Identifiable Information be documented as a risk to the City of Cockburn and should be treated, regardless of the requirement under legislation.

4. Findings

The following tables outline the information that was gathered during the Privacy of Data and Information Impact Assessment conducted at the City. Tables include comments from the assessor regarding each of the business units included, an assessment of the potential risk to the City and recommendations suggested to reduce the risk and increase the overall security posture of the City:

4.1. Corporate Communications

	Findings
Types of Information:	■ Customer contact details. ■ City of Cockburn employee contact details. ■ Photographs.
How Received:	■ Received through official internal channels / requests for inclusion in official communications. ■ Some information will be received via the human live chat function that will be available on the City of Cockburn website in future may include Artificial Intelligence (AI). ■ Photographs.
Where Stored:	■ ECM is used to store official records. ■ Corporate Communications store some photographs in *TechnologyOne* with others stored on the *S* drive. ■ *TechnologyOne* is also used by many departments.
Shared with:	■ Shares customer contact information with external parties including, *Survey Monkey*, *Engagement HQ* and *Mail Chimp*, both used as a means of reaching customer. ■ *Lucky Orange* used as a means of visually confirming the actions of a user on the website. Used for conflict resolution. ■ Consultants for research purposes.
Notified Issues:	■ Tries to maintain and track of all the City's databases and information sources. There is currently no single view of the customer. ■ Unsure if Non-Disclosure Agreement (NDA) exists with *Survey Monkey*, *Mail Chimp* and *Lucky Orange*. ■ *Lucky Orange*.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ Responsible for the City's internal and external communications. ■ Corporate communications manage the City's websites. ■ Permission slips are obtained and used whenever possible before a photograph is used. ■ Disparity between databases has in the past resulted in issues where communication has been sent to a deceased customer. ■ *Lucky Orange* is a US (foreign) based organisation.
Assessor's Comments	■ Following the review, there remain questions regarding the use of direct marketing to customers as there is no means for the customer to opt out of

	surveys or other communications from the corporate communications team. ■ NDA's need to be in place with any agency or third party before PII is shared with them. Through this the City performs its due diligence in ensuring that the third party is aware of the sensitivity and the is to protect City of Cockburn ■ The *Lucky Orange* cloud service is an area of concern, no demonstration was able to be provided to assure that the application was not accessing any form of PII. Of further concern is that the City's Information Services business unit was not aware of the City's use of this tool.

[R2-M] Opt-Out Recommendation - To comply with the Australian government's *Privacy Act 1988* (Cth), persons must be permitted to opt out of receiving direct marketing. This is most often achieved by including an 'unsubscribe' link in an email or a process whereby a person can reply to an email or SMS message with 'Unsubscribe' or 'Stop'.

[R3-M] NDA Recommendation - Ensure that no PII is shared outside of the City of Cockburn (outside of the sphere of the proposed policy) needs to be subject to an NDA to assure that the information is handled and protected in the manner assured through the policy that it was collected.

[R4-M] *Lucky Orange* Recommendation - Recommend that the City's Cyber Security Officer reviews the *Lucky Orange* service in order to make an informed assessment on the potential risk to the City of Cockburn through its use. Particular emphasis needs to be placed on the applications coverage of privacy information and financial information.

[R5-H] Supplier Security Recommendation - Whilst not entirely related to privacy. ES2 recommends that City of Cockburn develops and implements a supplier security policy document which includes due diligence requirements for cloud services in order to assure the use of cloud services does not compromise the position of the City with regard to the protection of privacy information entrusted to the organisation.

4.2. Risk and Governance

	Finding
Types of Information:	■ Personal Information (in various forms).
How Received:	■ Requests received via email or in person. ■ Personal Information received through official, internal channels.
Where Stored:	■ Requests stored in ECM.

Data and Information Audit (Privacy Impact Assessment)

Shared with:	■ The Governance & Risk Officer does on occasion have to deal with third parties to gain permission for the release of information or to provide grounds under which a request is being refused.
Notified Issues:	■ There is currently no policy or instruction to document or govern the control of the release of information under the *Freedom of Information Act 1992*. ■ There is no organisational level privacy policy. ■ The privacy statement only covers information that is received via the website and email. ■ Council meetings are currently recorded (audio) however there are plans to record using audio and visual and make these recordings available for public viewing. Council meetings often contain the PII of persons making requests. ■ In accordance with the requirements of the *Local Government Act 1995*, the City will be conducting Council eMeetings using *'BeingThere'* as the platform. ■ The Governance team is aware that public (free) versions of *Dropbox* are sometimes used by departments for the sharing of information.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information. ■ Redaction achieved using *Adobe Acrobat Professional* where necessary.
Departmental Comments:	■ Deals with all requests for information under the *Freedom of Information Act 1982* (FOI). ■ An average of 30 – 35 requests per year.
Assessor's Comments	■ Whilst responses to FOI requests are well managed, there is a need for a policy or other working instruction to be created to govern responses to requests for information that takes into consideration the legal aspects of content that may include PII. ■ There is a lack of corporate privacy policy to govern the receipt, handling, sharing, storage and eventual destruction of PII. The current privacy statement that is published in the City's website only covers information that is collected via the City's internet facing web sites. ■ Council meetings need to have conditions applied to ensure that PII is not revealed without having prior consent of the subject. ■ *Dropbox* poses a general information security concern to the City, not just to PII and should be subjected to Information Security Governance controls.

[R6-S] FOI Recommendation - ES2 recommends that the processes surrounding the response to Freedom of Information requests be subject to governance. In order to protect the City, there needs to be policy and process documented surrounding the City's response to requests for the release of information subject to the FOI (all PII is redacted in accordance with the FOI Act 1992. So is there need for a policy to capture this?). This instruction needs to ensure that PII is identified prior to any information release.

[R7-S] Privacy Policy Recommendation - ES2 recommends that the City of Cockburn develops, publishes and communicates a Privacy policy to cover all of the City's dealings with Personally Identifiable Information. Regardless of the requirement for compliance, this is a requirement to reduce the potential risk to the City's reputation should such information be inadvertently compromised. Additionally, the Policy would provide a much-needed consistency in the way that the City's departments handle and store PII.

[R8-S] Video Recording Recommendation - ES2 recommends that procedures be developed to assure that PII is either blocked from video and audio recordings unless the PII subjects have provided written approval for their information to be published along with the audio and vision of Council meetings. This can be achieved through prior notification of the recording and publishing of the recording being provided to all meeting participants or by requiring all meeting participants to sign to agree that any information spoken during the meeting will be published on the Internet.

[R9-S] *Dropbox* Recommendation - ES2 recommends that the use of *Drobox* be discouraged across the City's operations in favour of using the more secure option of *OneDrive*. In particular it needs to be prohibited to be used for the storage or transfer of PII.

4.3. Parks and Environment

	Finding
Types of Information:	■ PII associated with sustainability grants. ■ PII associated with new suppliers. ■ PII associated with full time employees, casual labour and consultants used. ■ PII associated with property developers and community groups. ■ Maintains a school contact list with contact details for headmaster/Principal. ■ Details of persons that have left a bond when taking a facility key.
How Received:	■ Requests received via email or in person. ■ Recruitment information received via email or in person.

	■ Personal Information received through official, internal channels.
Where Stored:	■ Information generally stored in ECM or *TechnologyOne* with some information put into the *S* Drive. ■ Schools contact list is stored on the S Drive.
Shared with:	■ PII is not shared with any external organisation or party.
Notified Issues:	■ Consultants often transfer information via *Dropbox*.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ Deals with up to 5,000 customer requests per year, each has associated PII. ■ Deals with community events.
Assessor's Comments	■ The use of *Dropbox* needs to be discouraged. ■ Use of the *S* Drive to store PII needs to be discouraged in favour of storing information in ECM or *TechnologyOne*.

[R9-S] ***Dropbox*** **recommendation** (***please see page 20 above***)

[R10-M] ***S*** **Drive Recommendation** - ES2 recommends that the City of Cockburn conduct a campaign of information storage awareness training. This training should concentrate on what information is or is not suitable for storage on the *S* Drive and how information should be managed. The minimum recommended content for training would be:

- What information needs to be stored on the ECM or in *TechnologyOne*
  - Housekeeping of information within the ECM
- What information must not be stored even temporarily on the *S* Drive
- What information may be stored on the *S* Drive
- Users' responsibilities with regards to the retention of information.
- Users' responsibilities with regards to the destruction of hard copy information.

Training should apply to all staff and management of the City of Cockburn.

4.4. Recovery Park Operations

	Finding
Types of Information:	■ PII associated with procurement processes. ■ PII associated with the recruitment of casual or flexi-time staff. ■ Vehicle number plates and weights.
How Received:	■ Procurement processes received through official, internal channels

	■ Recruitment information received through internal channels or email direct from subject. ■ Registration numbers are manually typed in to *TechnologyOne* and associated with other PII (names etc.). ■ In paper form (as part of trailer passes etc.).
Where Stored:	■ *TechnologyOne*, with some information temporarily stored on the *S* Drive.
Shared with:	■ Information is not shared with third parties.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Photos destroyed/deleted after being associated with *TechnologyOne* files. ■ Hard copy documents destroyed after being scanned, destruction is achieved in the City's landfill.
Departmental Comments:	■ There is the ability to take photos however this is not used. Photos may on occasion be taken by a phone if there is an absolute necessity (for compliance reasons). Once taken photos are appended to notes and then deleted.
Assessor's Comments:	■ There is considerable risk of compromise through the current means of destruction of documents that may contain PII, all data destruction must be conducted following a pre-defined and approved procedure. ■ The *S* Drive is being used to store information including PII.

[R11-H] Secure Destruction recommendation – ES2 recommends that a secure destruction policy or procedure be developed, approved and implemented by the City of Cockburn. This document needs to define the acceptable means of destruction based on the classification or sensitivity of the document or media in question. This instruction needs to ensure that information cannot be compromised through inappropriate destruction or disposal processes.

[R10-M] *S* Drive recommendation (*please see page 21 above*)

4.5. Waste Management

	Finding
Types of Information:	■ Names and addresses of where to deliver new bins or training on new bins.
How Received:	■ Via internal channels, usually following a request for a new bin or as part of a programmed roll out.
Where Stored:	■ *S* Drive.

Shared with:	■ This information is not shared.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ No other comments noted.
Assessor's Comments:	■ PII should not be stored on the *S* Drive. ECM needs to be the default information storage location.

[R10-M] ***S* Drive recommendation (*please see page 21 above*)**

4.6. Rates & Revenue

	Finding
Types of Information:	■ Electoral Roll contains all personal details. ■ Banking Details. ■ Investigation work may contain sensitive information. ■ Pensioners' details. ■ Local election information. ■ Animal data. ■ Infringement data (including number plate).
How Received:	■ Completed forms ■ Via email from other local governments or government departments
Where Stored:	■ Electoral Roll stored on *S* Drive (locked down to access by the rates department only) and on *TechnologyOne*. ■ The Electronic Cash Receipting system (ECR) receipting system (part of *TechnologyOne*). ■ The majority of information is stored in ECM. ■ Physical paper records are boxed up and sent to Grace Removals for archive and eventual destruction.

Shared with:	■ Information is passed to a 3rd party debt collection agency (WALGA approved supplier). Information including phone, email, name and address.
	  ■ Information is extracted from *TechnologyOne* via a set process.
	  ■ Information can also be shared using a shared internet portal.
	■ Information shared with printing service suppliers.
	  ■ Printers are given information regarding how they are to handle information on completion of print work.
	  ■ Information is passed to the print contractor via a shared portal

	■ The same print company is used to print the electronic rates forms that are emailed to customers this email is transferred in *pdf* as an email attachment. ■ Some information is shared with KPMG such as PII that relates to deferred rates. ■ Some information is shared with *Lucky Orange*. ■ PII of customers is often shared between local governments and other government departments (i.e. Rates and Revenue team may contact Water Corp for information on a person). That information is then provided to the City in an email. ■ Developers may request information which may be provided upon production of a Statutory Declaration.
Notified Issues:	■ Unclear what information is shared with *Lucky Orange*. ■ The Rates and Revenue team sometimes handles customer credit card information.
When/How Destroyed:	■ Destroyed as per the *State Records Act 2000*
Departmental Comments:	■ The Rates and Revenue team also deals with invoices for City owned infrastructure such as pavilions. ■ There is a plan in place to set stricter debt recovery because customers are providing these contractors with their current financial information. ■ Rates are normally paid online using *Securepay*.
Assessor's Comments	■ *S* Drive is not an appropriate location for the storage of PII, especially not such large quantities. ■ *Lucky Orange* poses an uncalculated risk to the City of Cockburn as this has not been subject to assessment and approval by the City's Cyber Security Officer. ■ NDA's need to be in place for every situation where PII is shared with a person or party external to the City of Cockburn this must include sharing with auditors (such as KPMG) and with other local government authorities many of whom will not have their own Privacy Policy or have a policy that differs from that of City of Cockburn. The NDA needs to ensure that the third party understands the limitations for the use of PII that was collected under the auspices of the City of Cockburn Privacy Policy (once defined).

[R10-M] *S* Drive Recommendation (*please see page 21 above*)

[R4-M] *Lucky Orange* Recommendation (*please see page 18 above*)

[R3-M] NDA Recommendation (*please see page 18 above*)

4.7. Procurement

	Finding
Types of Information:	■ Maintains a database of suppliers which may include their corporate banking details and the PII of the organisations points of contact. ■ Some sensitive information including details of inclusion of indigenous people working within that company. ■ Information regarding supplier referees.
How Received:	■ Supplier information received either directly from the supplier or via WALGA.
Where Stored:	■ Mostly using the CRM database. ■ *Pay Database* is used for claims reimbursement for employees, contractors and councillors. ■ Some information is stored in ECM. ■ Temporary information such as that generated when investigations are carried out is stored on the *S* drive (which is restricted to access only by members of the procurement team). ■ There is substantial information still stored on the *F* Drive.
Shared with:	■ Where disputes are concerned, some information may be shared with users.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Records are maintained for two years then deleted.
Departmental Comments:	■ Information stored is limited to that information that is necessary in order to make an assessment of the supplier organisations allowing an assessment of their suitability to provide their services to the City. ■ Information regarding indigenous persons is a requirement as part of the Reconciliation Action Plan (RAP). ■ The CRM database is weeded out regularly to ensure that only necessary information is retained.
Assessor's Comments	■ An NDA needs to be in place whenever PII is shared externally to the City of Cockburn.

	■ Whilst there is not a great deal of *S* drive use here this should be further controlled with user education. ■ Information on the *F* Drive needs to be reviewed and any PII must be transferred to ECM or deleted if no longer needed. ■ There is an unanswered question regarding how dispute information is shared with users. The response to this needs to be assessed to establish if the information is being appropriately protected throughout this process.

[R3-M] NDA Recommendation ***(please see page 18 above)***

[R10-M] ***S*** **Drive Recommendation** ***(please see page 21 above)***

[R12-M] ***F*** **Drive Recommendation** – ES2 recommends that the *F* drive be reviewed to establish if there is any PII stored on the drive. If there is, then this needs to be migrated to ECM as a priority.

4.8. Library Services

	Finding
Types of Information:	■ Names addresses and contact details of library members. ■ Infringement information.
How Received:	■ Online membership applications. ■ In person paper-based membership applications.
Where Stored:	■ A membership database is used which is a third-party application that is hosted in Melbourne. The Library management system is called '*Spydus*' whose global presence is called '*Civica*'. ■ There is a database of events which is accessible via the Internet.
Shared with:	■ 3rd party recovery agency. ■ Sharing achieved through the *Spydus* application. ■ Only the name and contact details are passed on (never details of the asset that is on loan). ■ On occasion, the police may request information and provide a *Notice to Produce* to the library. ■ Non personal information is shared using social media interactions such as blogs on Instagram ■ Some PII is passed to City staff so that customer surveys can be sent out.
Notified Issues:	■ Recovery agency is US based.
When/How Destroyed:	■ *Spydus* archives after two years of inactivity for an account (unless money is owing). After these two years member details are deleted.

Departmental Comments:	■ Infringement lists are kept within *Spydus*, when these are 2 months overdue or when a person owes more than $40 then a recovery agency is used. This is a specialist library recovery agency which interfaces with the library system and who focus on the recovery of the asset. ■ The events database allows customers to register their interest in an event.
Assessor's Comments:	■ There is an open question regarding infringement information that is stored on the Spydus database being visible via the internet. The database appears to have good security however the question of what is visible remains unanswered. ■ The US (foreign based) collection agency must be required to sign a Non-Disclosure Agreement with the City of Cockburn. ■ There is the potential for PII to be published inadvertently onto the Internet through official social media posts. ■ When the police require information from the library through the use of a *Notice to Produce* then they should be required to sign for the information. The form signed should include a Non-Disclosure statement to ensure that they understand that the information is being entrusted to them under condition that further dissemination is not to occur without notification to the subject.

[R13-M] Infringement Collection Recommendation – ES2 recommends that since City of Cockburn utilises an offshore collection agency for the recovery of library assets that users of the library service should be informed of this. When a customer signs up for library services they need to be informed that in the event of an infringement their personal information will be passed to a US (foreign) based asset recovery agency. Customers must agree to this prior to membership.

[R3-M] NDA Recommendation ***(please see page 18 above)***

[R14-M] Social Media Recommendation – ES2 recommends that a 'two person rule' process be implemented to ensure that all information published to Social Media in the name of City of Cockburn be reviewed and approved prior to publication/posting.

4.9. Volunteer Resource Centre

	Finding
Types of Information:	■ Contact and other personal information pertaining to volunteers doing work within the City of Cockburn controlled areas. ■ Volunteer information includes racial groupings, languages spoken, criminal record checks and if low income.
How Received:	■ Online forms may be used by members of the public to volunteer. When the form is complete the website emails it to the Resource Centre.

Where Stored:	■ Database called *VIKTOR* (run by Volunteering WA) is used. ■ *VIRA* is a component of *VIKTOR*.
Shared with:	■ Volunteers may be introduced to Not for Profit (NFP) organisations that require volunteers. ■ Volunteers can access *VIKTOR* on-line to view their own information and can request changes or can make changes. ■ With consent, information may be sent to a specific volunteer group in order to let the person consider joining.
Notified Issues:	■ Volunteers do not specifically authorise the sharing of information with NFP's.
When/How Destroyed:	■ Inactive volunteer personal accounts are removed periodically.
Departmental Comments:	■ Volunteers often do not inform the Resource Centre when they leave or are no longer a volunteer. If they do inform then their information can be set to inactive.
Assessor's Comments:	■ The online form should require that potential volunteers authorise the sharing of their information with appropriate third parties relating to volunteer activities. ■ Volunteer organisations receiving PII from the City of Cockburn should be subject to an NDA.

[R15-M] Volunteer Recommendation – ES2 recommends that online forms be adjusted to include a permission to share information component. This would then act as the authority from the subject to distribute their personal information to relevant volunteer organisations. Volunteer organisations receiving information must be subject to an NDA in order to assure that they are aware of the potential damage that could be caused if this information was subject to a security breach.

[R3-M] NDA Recommendation ***(please see page 18 above)***

4.10. Grants and Research

	Finding
Types of Information:	■ Personal information pertaining to persons that are requesting grants.
How Received:	■ Information provided by use of an online form. ■ Form has a link to the privacy statement.
Where Stored:	■ Information is stored within ECM and on the *S* Drive.
Shared with:	■ No information under the control of Grants and Research is passed to any third party.

Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Information can be archived within the *Smarty Grants* application when no longer needed. ■ Information is left in archive and not deleted.
Departmental Comments:	■ Managing the Cockburn community fund with an online funding system (*Smarty Grants* subscription service over east) only a few people within City can access this and they can only access information regarding the grants that they manage.
Assessor's Comments	■ Information stored on the *S* drive needs to be reviewed to ensure that no PII is stored there. Any identified needs to be transferred to appropriate parts of the ECM.

[R10-M] ***S* Drive Recommendation** ***(please see page 21 above)***

4.11. Port Coogee Marina

	Finding
Types of Information:	■ Details of boat owners. ■ Boat registration details. ■ Boat insurance details. ■ Sometimes hold bank details and may need to make payment refunds. ■ CCTV imagery.
How Received:	■ Information provided in person. ■ Information provided in email.
Where Stored:	■ Marina specific software called *Marina Focus* is used to contain all information pertaining to the business unit. ■ Some information is stored on the *S* Drive.
Shared with:	■ Information is not shared with third parties.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ CCTV (just over 40 cameras) maintain 30 days online archive.
Assessor's Comments:	■ There is an unanswered question regarding PII being handled by the Port Coogee Marina regarding how information is deleted when it is no longer needed. ■ Information stored within the *S* drive needs to be reviewed to ensure that there is no PII located there.

[R10-M] *S* Drive Recommendation *(please see page 21 above)*

4.12. Cockburn ARC

	Finding
Types of Information:	■ Individual and family membership. ■ Swim school details and membership.
How Received:	■ Information received in person or through online portal.
Where Stored:	■ Leisure Management software used *LINKS*. ■ Some data is exported from *LINKS* for internal (City) use. ■ *My Wellness Technogym.com* application is for members to monitor their ongoing fitness and engagement with gym equipment. ■ *Kentico*, website content management system, is used for ARC website. ■ ECM is also used to store personal information. ■ The *Aconex* system is used as a platform to coordinate with builders and contractors. On completion this information is downloaded and put on to ECM.
Shared with:	■ Credit card information is shared directly to a bank. ■ Information shared with *Mailchimp* as a means of mass communication to members. ■ Information shared internally within the City as required.
Notified Issues:	■ The individual computers at the ARC have generic logins, however each system accessed requires an individual login.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ Credit card information is taken via an EFTPOS machine and a PCI certified solution that uses tokenisation to send information to the bank. ■ Information can be removed from *LINKS* on request by the PII subject.
Assessor's Comments	■ The fact that individual systems access is achieved by individual login is good, however the generic logins to the devices that host the individual systems pose a threat as they can provide the platform to launch an attack against the individual systems. ■ Systems used to handle PII need to have been subject to a due diligence supplier security process to assure the system is going to handle PII securely.

[R5-H] Supplier Security Recommendation *(please see page 18 above)*

[R16-M] Access Security Recommendation - Access to computers that then provide access to systems which contain PII needs to be achieved using a unique set of login credentials for each person accessing the computer. This ensures that all actions performed by a computer user are accountable and traceable to a specific person.

4.13. Community Safety & Innovation

	Finding
Types of Information:	■ CCTV imagery (video not audio), this includes body cameras. ■ Facial recognition (being rolled out). ■ Some medical information. ■ Some bank statements. ■ Holds information regarding when a property will be empty, such as when an owner is going on holiday. ■ Details of contractors.
How Received:	■ Received direct from camera equipment. ■ Received via email. ■ Received in person.
Where Stored:	■ Information is stored on hard disk drives with a separate dedicated storage area for this (separate to the City's IT network). ■ The Service Unit has a dedicated part of ECM where information can be stored with additional privacy.
Shared with:	■ On occasion video footage needs to be passed on to legal entities. ■ Information passing to police is often shared via email.
Notified Issues:	■ New technology such as facial recognition needs governance.
When/How Destroyed:	■ Images are retained based on the type and location of camera.
Departmental Comments:	■ Responsible for all CCTV cameras, including parking cameras and body cameras. ■ Audio capability of CCTV cameras has been disabled. ■ Facial recognition being implemented going forward, this is currently under trial. The process tokenises a person's ID for reference without associating directly to a person. ■ The video footage from body cameras is stored in an encrypted form. ■ Some of the Service Unit team have been granted access to policy systems (online portals). Access for these is authenticated over the phone. ■ Notice to Produce may be received from WA Police.

	■ Some of the information held would be considered to be very sensitive. ■ Video is retained according to a defined policy which aligns to the requirements of the State Records Act 2000.
Assessor's Comments:	■ City of Cockburn needs to ensure that whenever video footage is passed to a third party that the third-party signs for the media and acknowledges the City's privacy requirements (NDA).

[R3-M] NDA Recommendation (*please see page 18 above*)

4.14. Ranger Services

	Finding
Types of Information:	■ Customer information. ■ Credit Card details. ■ Animal (and owner) details. ■ Driver infringement details (nomination of alternate driver etc.)
How Received:	■ Majority is received via email from members of the public including credit card. ■ Department of Transport vehicle checks are received via email. ■ Credit card information is sometimes received via email.
Where Stored:	■ Information is manually stored in ECM. ■ No information is stored on the *S* Drive.
Shared with:	■ On occasion, information is requested by and shared with other local governments. In such cases information is normally shared via email.
Notified Issues:	■ Credit card information often received via email.
When/How Destroyed:	■ Emails received with credit card information are deleted as soon as the payment has been dealt with.
Departmental Comments:	■ Infringements are paid by credit card or online transaction. ■ The Ranger Service has an EFTPOS machine that is used for payment of animal licenses etc.
Assessor's Comments	■ This department is receiving and handling credit card information independently. This function is best kept central, the most likely best location for this function is with the Rates and Revenue team. ■ Whilst outside the scope of a PIA, it was identified that credit card information is often received via email. This puts the City's entire email system within the scope of a Payment Card Industry (PCI) assessment. An assessment against the PCI Data Security Standard (PCI-DSS) would identify areas across the City of Cockburn enterprise that store, process and transmit credit card information.

[R17-S] Credit Card Recommendation – ES2 recommends that all credit card transactions be centrally organised and conducted by a single City of Cockburn Department.

[R18-S] PCI Recommendation – ES2 recommends that the City of Cockburn undertake a PCI assessment to establish the level of compliance with the PCI-DSS. This assessment should include the use of the Card Recon scanning software (*https://www.groundlabs.com/card-recon/*) which will scan the entire network to identify all locations where Credit Card information exists. This will go a long way to identifying the levels of risk posed to the City should credit card information be breached and made public.

4.15. Building Services

	Finding
Types of Information:	■ Personal details.
How Received:	■ Information gained from the rates database.
Where Stored:	■ All stored in ECM or *Trapeze* system.
Shared with:	■ Reporting is statistical based with no PII. ■ May issue copies of plans on request (proof of ownership is required). ■ Freedom of Information requests sent internally to Governance Services.
Notified Issues:	■ No issues notified. ■ May be some (minimal) credit card information received via email.
When/How Destroyed:	■ Some information is retained indefinitely. ■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ Responsible for the stature side of buildings including occupancy permits, strata certificates, demolition permits, property audits, pool inspections and general compliance requirements ■ Payment is achieved via the payment gateway.
Assessor's Comments:	■ This department is receiving and handling credit card information independently. This function is best kept central, the most likely best location for this function is with the Rates and Revenue department. ■ Whilst outside the scope of a Privacy Impact Assessment, it was identified that credit card information is occasionally received via email. This puts the City's entire email system within the scope of a Payment Card Industry (PCI) assessment. An assessment against the PCI Data Security Standard (DSS) would identify areas across the City of Cockburn enterprise that store, process and transmit credit card information.

[R17-S] Credit Card Recommendation (*please see page 33 above)*

[R18-S] PCI Recommendation (*please see page 33 above)*

4.16. Recreation Services

	Finding
Types of Information:	■ Details regarding sporting and recreation clubs including personal details of the contacts for such organisation (this information is generally available from the club's website). ■ Bank account details. ■ Details pertaining to sports and recreation related grants.
How Received:	■ Information in pdf form is sent or received via email. ■ Information captured via website.
Where Stored:	■ Residual information in S Drive. ■ Information in the process of being transferred to ECM. ■ *Intellileisure* used for books. ■ *TechnologyOne* (property and rating) used for invoicing. ■ New online booking system (*Optimo*) is to be introduced.
Shared with:	■ Information shared with *Mailchimp* as an opt-in opt-out communication service.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ At the end of its lifecycle, information is either archived as a record or is placed in the secure disposal bins.
Departmental Comments:	■ Individuals or groups may submit booking forms in PDF format or as word documents. These are then used to complete information in *Intellileisure*. ■ Bonds are required for some function rooms. Bond information is dealt with through the NAB pre-authorisation system. Credit card details are not written down or kept.
Assessor's Comments:	■ Personally, Identifiable Information in the *S* Drive needs to be identified and transferred to the ECM and then removed from the *S* Drive. ■ The *Mailchimp* solution needs to be assessed to ensure that they are a secure supplier and should be subject to a Non-Disclosure Agreement.

[R10-M] S Drive Recommendation (*please see page 21 above)*

[R5-H] Supplier Security Recommendation (*please see page 18 above)*

[R3-M] NDA Recommendation (*please see page 18 above)*

4.17. Community Engagement

	Finding
Types of Information:	■ Personal details.
How Received:	■ Via *Bang the Table* forum. ■ Via email or letter.
Where Stored:	■ Platform called *Bang the Table* (feedback forum) is used to receive information regarding submission. ■ Community Development *S* drive temporarily then into ECM.
Shared with:	■ Information is not shared outside of Community Engagement.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Information deleted from the *S* drive after input into ECM.
Departmental Comments:	■ The *Bang the Table* application is a third-party application that is moderated.
Assessor's Comments	■ The *Bang the Table* application should be subject to a supplier security process to ensure that it meets the City of Cockburn security requirements.

[R5-H] Supplier Security Recommendation (*please see page 18 above)*

4.18. Property and Lands

	Finding
Types of Information:	■ Names and addresses required for land documents.
How Received:	■ Often received from solicitors as an email or an email attachment

Data and Information Audit (Privacy Impact Assessment)

	■ Information gleaned from Landgate.
Where Stored:	■ *S* Drive used for temporary storage. ■ ECM used in the main storage.
Shared with:	■ Not responsible for the destruction of customer contact information.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Responsible for managing land or crown reserves. ■ Preparation of land documents.
Departmental Comments:	■ Has access to Landgate to gain details of land ownership and other mapping.
Assessor's Comments	■ The *S* Drive needs to be reviewed to understand if there is any residual PII stored on the drive.

[R10-M] *S* Drive Recommendation (*please see page 21 above)*

4.19. Customer Services

	Finding
Types of Information:	■ All levels of personal information including opinions. ■ Occasionally sensitive PII.
How Received:	■ Information retrieved from ECM (property and rating system). ■ Information provided over the phone. ■ Information provided in face to face meetings. ■ Information provided in email form.
Where Stored:	■ Stored in ECM. ■ *S* Drive is used but not for customer information ■ *Statutory Declarations* pertaining to animals signed by customer service ops are stored in ECM by the rangers or by records.
Shared with:	■ In cases where a boundary fence line is under dispute then information regarding the name and address of the person on the other side of the boundary may be provided to the neighbour. In such cases the information is passed over the phone or in person. The customer services operator must authenticate the requestor to guarantee that they are the owner of one side of the boundary. Where this occurs, the operator annotates the property and rating system notes to show the release of information. ■ Information is shared with a third-party organisation called *Research Solutions*. This includes an agreement and a non-disclosure agreement. This company is WALGA approved. The company performs research via telephone.
Notified Issues:	■ No issues were notified.
When/How Destroyed:	■ Telephone recordings are retained for three months before deleted.
Departmental Comments:	■ Team of 13 dealing in the main with phone calls from customers but also dealing with face to face engagements through the reception. ■ Opinions may include notes where the customer service team has experienced trouble during face to face meetings or from abusive telephone calls. ■ The recording of telephone calls stops when a call is transferred to another internal number within the City. ■ Sensitive information is rare and is not a target at all. However sometimes it is mentioned over the phone by customers so ends up on the telephone recordings.
Assessor's Comments	■ The sharing of information with *Research Solutions* needs to be included within the proposed privacy policy. It is only by this measure that all customers can be informed that their information will be used in such a research activity. ■ Customers need to have the ability of Opt out of the research component.

[R2-M] Opt-Out Recommendation (*please see page 18 above*)

[R19-S] Policy Content Recommendation – ES2 recommends that the privacy policy that is developed to support the City of Cockburn include all anticipated use of the PII that the City collects. The policy is published and used to advertise the use of collected PII to all persons that entrust that information to the City.

4.20. Accounts Payable

	Findings
Types of Information:	■ Payment details (destination account). ■ Customer details. ■ Third party details. ■ Insurance contact details. ■ Photographs of people (and injuries). ■ Dash cam video.
How Received:	■ Received in person. ■ Received via email. ■ Supplier information from the Strategic Procurement team.
Where Stored:	■ Mostly stored in ECM and *FinanceOne*. ■ Some stored in *Outlook*. ■ Accounts Payable has some information stored on the *S* Drive.
Shared with:	■ Information is not shared.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ Deal with Accounts Payable and Insurance teams (such as public liability insurance). ■ Payment details (not credit card) are stored. Payment is achieved via EFT ■ All insurance claims must be provided in writing which can be an email or may on occasion be someone coming to the front desk in person or completing a form. Name address contact details, potentially vehicle details and may include photograph. Photographs may include people and injuries such as when a person trips on a pavement and get hurt. Video is also received at times usually video from a dash cam. All this information would then be passed to LGIS (Local Government Insurance Scheme) a third party. Passed to them via ECM link or via email. Information going to insurer may include opinion. ■ The clearing of outlook and the *S* drive has been an ongoing project.

Assessor's Comments	■ The clearing of PII from outlook and the S drive needs to continue. The use of outlook as a means of storing information needs to be discouraged across the organisation.

[R10-M] *S* Drive Recommendation (*please see page 21 above)*

[R20-M] ***Outlook* Storage Recommendation** – ES2 recommends that The City of Cockburn conduct an IT educational campaign to discourage users from using *Microsoft Outlook* as a file storage system.

4.21. Records Management

	Finding
Types of Information:	■ All types of PII. ■ HR information.
How Received:	■ Through internal and external postal correspondence. ■ Some email (most goes to customer service). ■ Occasionally by fax.
Where Stored:	■ Correspondence scanned into ECM and through that to Property and Rating. ECM is then used for tasking of internal resources/departments. ■ HR records are secured so that only HR staff can access them. ■ Hardcopy stored in archive boxes stored in a locked room. ■ Inactive hardcopy records are stored at Grace Removals offsite.
Shared with:	■ Grace Removals for archive purposes.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ No disposal electronically. ■ Paper based destruction. ■ There is a General Disposal Authority (GDA) for the retention of local government records.
Departmental Comments:	■ The records management team has eight (8) full time employees plus some casual workers. ■ Information classification is in place and is integrated with ECM, this is all based on access control. Security is set on groups rather than individuals. ■ No PII stored on the *S* Drive.
Assessor's Comment:	■ Information is classified from a records perspective rather than from an information security or sensitivity perspective.

[R21-M] Security Classification Recommendation – ES2 recommends that City of Cockburn considers the implementation of an information security classification scheme across the City's information enterprise.

An information security classification scheme groups information based on the potential damage/impact/consequence that would impact the City should that information be subject to a breach of confidentiality.

ES2 recommends that the City implements a simple classification scheme, the main aim being to be able to identify that information which requires the most protection including PII. Once the classification levels have been determined then appropriate protection, storage and handling processes per classification can be established.

This recommendation is to implement a process in alignment to that implemented by Federal Government with levels that include Official and Official Sensitive as defined in the Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF).

4.22. Human Resources

	Finding
Types of Information:	■ Employee information.
How Received:	■ Gathered during recruitment process (via *Big Red Sky*). ■ Occasional updates from employees.
Where Stored:	■ Most information is stored in ECM which has a specific HR and Payroll component.
Shared with:	■ External agencies such as the Child Support Agency (CSA) may make legal requests for information from a person's employer. ■ Sometimes requests are received from other employees or internal departments. In such cases HR officers are trained to assess the appropriateness of sharing information in a secure manner.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Employee records are kept for seven (7) years (under law and in accordance with the retention policy) after the departure of an employee under the control of the records department. ■ Not responsible for the destruction of customer contact information or employee information.
Departmental Comments:	■ Contractor information is held by the Strategic Procurement team. ■ Where a candidate does not get offered a job, their information is retained to aid future applications from this person. ■ There are some (cloud) systems that are made available for pre-employees to access such as *Fit2 Work* and others that are used for pre-employment checks.

Assessor's Comments:	■ Although the personal details of employees are exempt from the Federal government's *Privacy Act 1988* (Cth), there is still considerable impact on an organisation should the personal information of employees be subject to a security breach the impact on the reputation of the City is the same as if it were customer information.

[R22-M] Policy Coverage Recommendation – ES2 recommends that the policy document to be developed, authorised and published should include the personal information pertaining to employees of the City of Cockburn in order to assure their protection the same as the protection of customer information.

4.23. Child Care Services

	Finding
Types of Information:	■ Personal information regarding childcare educators. ■ Children's Personal information.
How Received:	■ Information, including children's enrolment information, is received in paper form. ■ Information received through the '*Harmony*' web portal.
Where Stored:	■ Paper versions of information are stored to assure completeness of the history. These are stored in a locked filing cabinet. ■ Paper based children's information is transferred to an online process (ECM). ■ ECM is used for email and general communication.
Shared with:	■ Information is received and shared in accordance with Commonwealth Government requirements. ■ Share information with the education and care regulatory unit.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Children's enrolment forms are shredded after being input into ECM.
Departmental Comments:	■ Childcare services are third party regulators with regards to the selection of educators. (If someone has registered to care for children, they are referred to as Childcare educators). ■ The *Harmony* web portal is Commonwealth approved software. ■ Application fees from educators, plus payments to the educators from parents are achieved through *Harmony* web. ■ Childcare services work closely with the Department of Education, Skills and Employment. ■ When an educator or a child leaves the services programs then their information is archived.

	■ The Commonwealth Government has provided Childcare Services with a Privacy Policy (11.2) that applies to the City of Cockburn Family Day Care (FDC) Service and the FDC Educators.
Assessor's Comments	■ The Commonwelath Privacy Policy states compliance with the *Education and Care Services National Law (WA) Act 2012* and the *Education and Care Services National Regulations 2012* and is based on the Australian Privacy Principles. Therefore, this should be compatible with any future Privacy Policy as published by the City of Cockburn. ■ Whilst the policy is good it needs to have terms defined to assure a common understanding (for example the terms personal information and sensitive information are used without definition). ■ Policy wording needs to be more mandatory (following normative rules *Will*, *Shall*, *Must* etc.). ■ There is no indication within the policy of who has authorised the policy to be in place.

[R23-S] Policy Improvement Recommendation – ES2 recommends, that the childcare services privacy policy be updated and improved in conjunction with the development of the overall City of Cockburn proposed privacy policy. The wording within the policy must be definitive and easily understood to remove any conjecture and ensure that the policy is enforceable and that failure to comply with policy can be dealt with through the City's disciplinary process.

4.24. Financial Counselling Service

	Finding
Types of Information:	■ Customer personal information. ■ Financial information. ■ Credit card information.
How Received:	■ Information provided on two written forms. ■ Further information may be provided during face to face consultation. ■ Credit card information is communicated via email.
Where Stored:	■ Forms are scanned then stored on the Financial Counselling Services *H* drive. ■ *H* drive contains credit card information.
Shared with:	■ Credit card information and loan number is exchanged with debt collectors or banks via email along with other relevant financial information. ■ Shared with relevant government agencies via ATO online, MyGov, AFSA and the Commonwealth ombudsman. Covered by legislation.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Written forms are handed back to the customer once scanned.

Departmental Comments:	■ This is a grant funded office outside the City's control.
	■ The office comes under the:
	  ■ *Social Security Act 1991* (Cth); and
	  ■ *National Consumer Credit Protection Act 2009* (Cth).
	■ This is (by law) a free service, provided to City of Cockburn residents.

Assessor's Comments:	■ This department is outside the scope of this engagement but has been included here for completeness, since information was willingly provided. ■ There is an outstanding question regarding what separate legislation applies to financial counselling services and what security requirements accompany that legislation. ■ There is a concern with the local storing of credit card information on the *H* drive and being transmitted via email. This is one of the most attractive forms of information to attackers and requires additional protection in alignment with the PCI-DSS. This department is probably too small to require full certification to PCI-DSS, however the department must align with and comply with the requirements of PCI-DSS in order to assure the protection of Credit Card Information and as such would benefit from the conduct of a PCI assessment.

[R18-S] PCI Recommendation (*please see page 33 above*)

4.25. Cockburn Care

	Finding
Types of Information:	■ Staff personal details. ■ Staff Police clearance details. ■ Staff photos. ■ Client information which may include psychosocial issues. ■ Bank account details for direct debit payments. ■ Medicare numbers, pension cards, client notes, medical information, social history, gender, sexual orientation, ethnic origin. ■ Guardian or limited guardian information.
How Received:	■ Details not provided.
Where Stored:	■ Service management system '*Alchemy* 'SMS is locally installed. This is used to store the majority of information. ■ Staff photos on *S* drive. ■ ECM and *TechnologyOne* used for information storage. ■ MyAgedCare system through MyGov. ■ Incident reports are recorded on a specific part of the *S* Drive where only other aged care assessors can access as part of the healthcare system.

Shared with:	■ Information shared with allied health. General Practitioners (GPs) may broker services to other specialist health agencies, family members or the police. ■ Where clients do not want information to be shared then warning alerts can be set up to prevent sharing.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Information remains on the SMS system indefinitely. ■ Paper files get archived through Records.
Departmental Comments:	■ No credit card information stored. ■ Service agreements are held with clients authorising the sharing of their information when the sharing is in the interest of the client. ■ There is a privacy policy in place. ■ The Commonwealth Government has provided Cockburn Care Services with a Privacy Policy that applies to the City of Cockburn Care Services. ■ Staff sign an additional confidentiality agreement.
Assessor's Comments:	■ There is an unanswered question regarding how Cockburn Care receive PII. When Identified this needs to be reviewed and incorporated into the proposed privacy policy. ■ PII on the *S* Drive should be reviewed and transferred to ECM. ■ All transfer of information should be subject to an NDA being in place between the City and the third party.

[R10-M] *S* Drive Recommendation *(please see page 21 above)*

[R3-M] NDA Recommendation *(please see page 18 above)*

4.26. GIS

	Findings
Types of Information:	■ Names and addresses regarding property ownership (private and City property). ■ Graffiti pictures may contain known tags or names that could identify a person.
How Received:	■ Telephone. ■ Online. ■ Via police.
Where Stored:	■ Stored in an *SQL* database accessible only to GIS team members.
Shared with:	■ Shared with the police under the control of the City's Rangers.

Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ No additional comments.
Assessor's Comments:	■ There is an unanswered question regarding if and when information with the *SQL* database is deleted and what the retention period for this is. ■ Recommendations as per those applied to the City Rangers.

4.27. Youth Services

	Findings
Types of Information:	■ Personal information of young people and their parents or other family members. ■ Bond payment requires the scanning of the front of the persons credit card. ■ May include scan of ID cards. ■ May include information pertaining to details of the young person's home/homeless state or if itinerant. ■ Incident reports may contain sensitive information regarding challenging behaviour.
How Received:	■ Through paper forms.
Where Stored:	■ Youth Services officers have a dedicated and secured room that requires proximity card to access and. provides a secure area restricted only to Youth Services officers. ■ Lockable cabinets within the secure room. Cabinets are locked outside of normal working hours or when unattended. ■ No information is stored in electronic form other than email. ■ Referrals are kept in hard copy form.
Shared with:	■ Police when required.
Notified Issues:	■ Electronic systems have been provided to youth service in the past, however there were issues over staff trusting the confidentiality as a result of a couple of incidents that the department experienced.
When/How Destroyed:	■ Details not provided.
Departmental Comments:	■ Youth Services provides support for vulnerable and at-risk young people. ■ Example of confidentiality agreement provided. ■ Example of duty of care form provided. ■ Copy of notification of *Freeze* on youth records from WA Government provided. ■ Policy on reporting child sexual abuse provided. ■ Policy on storing confidential client records provided. ■ Youth Services bond procedure provided.

	■ Youth Services deals with the hiring of the youth centre facility which may require that a bond be left.
Assessor's Comments	■ There is an outstanding question with regards to retention and destruction of hard copy information. ■ The Youth Services business unit appears to be well organised with regards to PII although all information is kept on hard copy only which is a risk.

[R24-M] Electronic Systems Recommendation – ES2 recommends that the City of Cockburn Cyber Security Officer works with the Youth Services team to overcome issues with confidence in IT system confidentiality.

PII needs to be stored electronically in order to assure that it receives the appropriate level of protection.

Paper based files should be transferred to an electronic system and then destroyed.

[R3-M] NDA Recommendation (*please see page 18 above*)

4.28. Civic Support

	Finding
Types of Information:	■ Personal information of organisers/hosts. ■ Contact information of attendees. ■ Contact information of caterers. ■ Dietary requirements and/or food allergies for attendees. ■ Contact details for attending dignitaries.
How Received:	■ Information may be extracted from internal databases. ■ Information may be provided verbally over the telephone. ■ Information is mainly provided via email.
Where Stored:	■ Information is initially stored on the *S* Drive that is dedicated to the Civic Support team, until the event itself. ■ When the event has occurred then information moves on to ECM.
Shared with:	■ Names and dietary requirements are shared with catering organisations. Attendees are notified that this information will need to be shared. ■ Internally the Mayor and the City CEO have access to guest lists. ■ Occasionally an Elected Member or MP may request a list of VIPs attending a function. In such an instance, the information is provided as name only.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ *S* Drive contents are deleted once transfer to ECM is complete.

Departmental Comments:	■ Organising of major events and manages the amenities of the City's function spaces including booking. ■ Management of guest lists including details of dignitaries, public figures (Politicians and Elected Members). ■ Managing the catering and other contacts for such events. ■ The guest list for the Cockburn Pioneers lunch is dealt with outside of ECM.
Assessor's Comments:	■ The Civic Support Department appear to have a good level of control over PII within their area. ■ There would be benefit to the department to have non-disclosure agreements with the third parties that receive PII from the department.

[R10-M] *S* Drive Recommendation (*please see page 21 above*)

[R3-M] NDA Recommendation (*please see page 18 above*)

4.29. PA to Mayor & Councillors

	Finding
Types of Information:	■ Master list of all function invitees. ■ Mayors brief may include names and contact details. ■ Personal and contact information of ratepayers communicating with the Mayor or councillors. ■ Personal details including dietary requirements.
How Received:	■ Received from Civic Support Services or through other internal channels.
Where Stored:	■ Temporarily stored on the *S* drive then moved to ECM.
Shared with:	■ Not shared outside of the Mayor and Elected Members.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ *S* Drive information deleted once transfer to ECM is complete.
Departmental Comments:	■ Provides Personal Assistant services to the Mayor and councillors.
Assessor's Comments	■ The PA to the Mayor and Councillors has a good level of control over the PII entrusted to the department.

4.30. Environmental Health

	Finding
Types of Information:	■ Food premises owners. ■ Includes opinions (assessments) of hygiene levels, infectious disease, electrical safety and environmental health and safety. ■ Photos and videos taken during inspections (evidence). ■ Some (minimal) legacy credit card information.
How Received:	■ From internal sources of information. ■ Additional information gained during site inspection process. ■ Complaints received.
Where Stored:	■ Most information is stored in *TechnologyOne*. ■ *S* Drive is used extensively for ad-hoc storage of information but not for personal information. ■ Complaints received are stored on *TechnologyOne*/ECM.
Shared with:	■ Information only revealed if there is a compelling reason to share such as for protection or for legislative compliance. ■ Police are used as a support function when required but minimal information is passed. ■ Requests for information may be received when a business or premises is being purchased. This is known as an application for historic information. Any information provided does not include personal information. ■ Most sharing instances are statistical only with no personal information included. ■ The Department of Health maintain a name and shame register which the City is sometimes asked to contribute to. ■ Information pertaining to environmental issues (asbestos, noise, air monitoring) that is requested by external parties does not always go through the Freedom of Information process.
Notified Issues:	■ City FOI processes not always followed for the release of information.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ Information regarding the ownership of food premises including more than 600 names and contact details. ■ The Environmental Health Services officers are aware of the sensitive and private nature of the data collected. ■ Department had previously stored credit card information. However, this has not been moved to the online systems managed by Accounts Payable. There is no 100% guarantee that legacy environmental health information does not contain credit card information however this is not on the *S* Drive. ■ Anonymous complaints are not accepted. ■ Every event with more than 500 people is considered a public event and would warrant an environmental health inspection.
Assessor's Comments:	■ The Environmental Health department has a good level of control over the PII entrusted to the department.

	■ NDA's should be used where PII is shared with third parties.

[R3-M] NDA Recommendation *(please see page 18 above)*

4.31. Engineering Works

	Finding
Types of Information:	■ Contact information relevant to contracts managed by Engineering Works. ■ Business financial information (costings/pricings). ■ Résumé information of potential employees. ■ Graffiti photos (may include identifiable tag or names). ■ Disability, language and age information. ■ Locations and movements of road sweepers and the persons operating them.
How Received:	■ Résumés received via email, or in person. ■ Reports of damage or issues received mainly via the Customer Contact Centre or from Elected Members whom have been approached directly. ■ Information received from the Customer Contact Centre about any engineering work being conducted anywhere within the City. ■ Location and movement or road sweepers obtained through GPS tracking system.
Where Stored:	■ All complaints or requests for work are lodged into *TechnologyOne*. ■ The *S* drive is used for more incidental or ad-hoc information that is not structured enough to use *TechnologyOne* or ECM. Eventually some information is migrated to *TechnologyOne* or ECM.
Shared with:	■ Where information regarding damage or issues is not within the City's jurisdiction then the caller is informed that their information will be forwarded to the relevant authority. ■ Where third party support is required to conduct a large job, approval is sought from the reporting person before their information is passed to the third party.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ The résumés of unsuccessful employment candidates are destroyed.
Departmental Comments:	■ Engineering works owns a number of contracts which contain confidential costings/pricings and contact information. ■ Where graffiti is on private property then waivers are sought and signed by the owner before access is permitted. ■ All contracts include confidentiality clauses.

	■ GPS in road sweepers are used to map which areas have been swept and when. All drivers must sign to show that they understand and accept the fact that they are being incidentally tracked during their working day.
Assessor's Comments	■ The Building Services Department have a good level of control over the PII entrusted to the department.

4.32. Seniors Centre

	Finding
Types of Information:	■ Personal information regarding senior citizens that use the centre (approx. 1200 members). ■ Legacy (over three years old) credit card information. ■ Home pickup information (times). ■ Details of the volunteer bus and van drivers including copies of their driver's license. This information also includes Next of Kin and medical information. ■ Photos and videos of weekly events. ■ Men's Shed membership information.
How Received:	■ Hard copy membership forms. ■ Electronic membership forms. ■ Visitors log provides names and reasons for attendance.
Where Stored:	■ Membership details stored in *Intellileisure* database system. ■ Hard copy forms are stored in a locked room until they are archived to records. ■ Likelihood that there is legacy credit card information stored on the *S* Drive. ■ Facility hire information stored on the S Drive but is being slowly transferred to ECM. ■ Driver details and licenses stored on the *S* Drive. ■ The *Vera* application is used to manage volunteers. ■ Staff pay details is stored on the *S* drive in a protected document which was created for the Centre Manager by the IT team. ■ Photos and videos are stored on the *S* Drive.
Shared with:	■ Home information is passed to drivers so that they can collect senior citizens when required. Drivers are instructed to delete this information from their emails after use. ■ Where photos or videos are shared on the web approval is sought from the person(s) concerned.
Notified Issues:	■ There is PII stored on the *S* Drive.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ No credit card information stored in the last three years, however prior to that there may be some which would be stored on the *S* Drive. ■ All drivers have signed a confidentiality agreement. ■ All processes are currently being reviewed.

	■ Weekly events have photos and videos taken which are stored on the *S* drive. ■ Contractors sign in on the register on the volunteer desk. ■ Sometimes has Men's Shed information.
Assessor's Comments:	■ Residual credit card information must be identified and electronically destroyed. ■ Information on the *S* Drive needs to be transferred to ECM and deleted. ■ All drivers need to be subject to Non-Disclosure agreements.

[R10-M] *S* Drive Recommendation *(please see page 21 above)*

[R3-M] NDA Recommendation *(please see page 18 above)*

[R18-S] PCI Recommendation *please see page 33 above)*

4.33. Civic Administration

	Finding
Types of Information:	■ Personal and contact information of persons attending citizenship ceremonies. ■ Citizenship personal information (and certificate number) can be sensitive - this is provided by the Department of Home Affairs.
How Received:	■ Information received via email in an *Excel* spreadsheet
Where Stored:	■ The spreadsheet from the Department of Home Affairs is stored in ECM where changes can be tracked. ■ Certificates are kept in a locked safe (unless there are too many then they are secured within a locked room.)
Shared with:	■ The Department of Home Affairs manages all confidential information and provide the civic administrators with details of those to undertake the ceremony. ■ Seating plans are documented with names. These plans go to the Amenities Team and to the Mayor and Deputy Mayor and Electoral Office. Not published online. Report internally includes new citizens' country of origin. ■ Press release for the national citizenship ceremony when conducted on Australia Day will include statistics. Individual persons may be named upon their consent. This is more for award winners i.e. community citizen of the year (national Australia day awards).

	■ During the ceremony officers from the Australian Electoral Commission attend in order to enrol new citizens on the Electoral Roll. ■ After each ceremony a list of new citizen attendees is sent to Parliamentary Representatives, together with a waiver as to what can or can't be done with the information.
Notified Issues:	■ No issues notified
When/How Destroyed:	■ Spreadsheet deleted from ECM by Civic administration once ceremony has been completed
Departmental Comments:	■ The main responsibility of Civic Administration is managing the monthly citizenship ceremonies ■ Each person on the list is emailed (via BCC) to invite to the ceremony request to bring photo ID on the day, to confirm if an oath or an affirmation is required and if guests are being brought. ■ These email invites are often stored within *Outlook* in a separate folder as a temporary knowledgebase. This is not a personal email address. The reply emails do often include more PII.
Assessor's Comments:	■ The Civic Administration Department have a good level of control over the PII entrusted to the department.

4.34. Community Development

	Finding
Types of Information:	■ Names, addresses, phone and email contact details for customers attending workshops or networking events. ■ Contact details for other groups being supported. ■ Information regarding a network of religious groups and individuals within those groups.
How Received:	■ Received via telephone or email.
Where Stored:	■ Stored in spreadsheets on the *S* Drive that is only accessible by Community Development staff. ■ Spreadsheets registered in ECM. ■ Religious group information is stored on the *S* Drive.
Shared with:	■ On rare occasions information may be verbally passed to Police during an investigation. Usually only a name is communicated.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Details are deleted when people leave (if notified).
Departmental Comments:	■ No paper records are maintained. ■ No credit card information is stored or used.
Assessor's Comments:	■ *S* Drive use for PII must be minimalised in order to reduce risk and to follow a defined security process.

[R10-M] S Drive Recommendation (*please see page 21 above)*

4.35. Children's Development

	Finding
Types of Information:	■ Children's name, date of birth, allergies etc. (sometimes more personal or sensitive information which may include details of restraining orders of parent or other family member). ■ Information about families, number of children, signature etc. ■ School P and C, or P and F, email details are sometimes provided. ■ Some playgroups have provided the Children's Development team with their personal contact details.
How Received:	■ Paper based enrolment form. ■ Annual event (teddy bears picnic), registration form emailed to Children's Development Officer.
Where Stored:	■ School P and C, or P and F, email details when provided are kept in a spreadsheet that is used as a contact list which is annually updated. ■ Parent workshops are held twice per year, the attendance lists are deleted afterwards with only statistics retained.
Shared with:	■ No third-party sharing of information other than using *Mailchimp* for distributing a regular newsletter. ■ There are occasional discussions with authorities regarding children that police are aware of or are actively monitoring. These communications are mainly verbal or contained within internal emails.
Notified Issues:	■ Still have paper copies, this need to be checked to ensure they are now on ECM, then paper is to be shredded.
When/How Destroyed:	■ Paper is shredded after uploading information into ECM.
Departmental Comments:	■ Still have paper copies, which need to be checked to ensure they are now on ECM, following this the paper is to be shredded. ■ No credit card information is stored or handled.
Assessor's Comments:	■ There is an unanswered question for the Children's Development team regarding the location where the P and C spreadsheet is stored. ■ The use of *Mailchimp* needs to be reviewed along with previous recommendations on this topic.

[R5-H] Supplier Security Recommendation (*please see page 18 above)*

4.36. Disability Access and Inclusion

	Finding
Types of Information:	■ Personal information of specific membership. ■ Documented business cases include both fact and opinion. ■ The extent of a person's disability is recorded.
How Received:	■ Completion of online forms. ■ Paper based forms. ■ Emails.
Where Stored:	■ Stored in ECM and *S* drive plus there are some paper files.
Shared with:	■ Sometimes the department has to deal with homeless or drug users and may need to pass minimal information to the Police. However, this information is not stored within any of the City's systems. ■ ACROD passes dealt with on a State basis. The City may link members to the State website on this, but no information is passed.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ Facilitate the Disability Reference Group, this group has a specific membership. ■ The group has been established for all disabled adults. ■ No credit card information is held or handled. ■ When a group member leaves then their information is annotated that they are no longer a member. ■ Membership can be revoked, under the unreasonable customer policy.
Assessor's Comments	■ The use of the *S* drive for the storage of PII needs to be reviewed and controlled centrally.

[R10-M] *S* Drive Recommendation (***please see page 21 above)***

4.37. Aboriginal Community Development

	Finding
Types of Information:	■ Name, date of birth and racial origin.
How Received:	■ Received on paper-based form or electronic forms that are then emailed to the department.
Where Stored:	■ Stored on ECM. ■ Once in ECM the email is deleted, contact details added to a contact list spreadsheet which is stored on the *S* Drive.

	■ A list of group members that wish their information to be shared is kept on the *S* Drive.
Shared with:	■ Some information may be requested from within the members of the Aboriginal reference group. Aboriginal Community Development Officer liaises when this arises to ensure that all parties agree to the sharing of information. ■ Some requests, such as requests for skip bins or other facilities that the City is able to provide are received by group members. In these cases, some information needs to be shared with internal City departments but does not go external to that. ■ Some group members, such as entertainers or welcome to country speakers, request for their information to be shared. There is a list of these on *S* Drive.
Notified Issues:	■ No issues notified.
When/How Destroyed:	■ Email deleted after information is transferred to ECM.
Departmental Comments:	■ This department deals with the Aboriginal Reference Group including Torres Strait Islanders.
Assessor's Comments:	■ The Aboriginal Community Development Department have a good level of control over the PII entrusted to the department.

4.38. Statutory Planning

	Finding
Types of Information:	■ Contact details (owners name, signature, applicants name, signature, both email and contact details).
How Received:	■ Applications via online portal, straight to *TechnologyOne*/ECM. ■ Delivered in person. ■ Information is received by Australia Post with USB. ■ Some information may be received via email.
Where Stored:	■ Hard copy information arrived is scanned by records and stored in *TechnologyOne*/ECM. ■ Information received via USB is copied into *TechnologyOne*/ECM then records return the USB to the applicant. ■ Where information has been received via mail, an admin officer registers the document in ECM and is tasked to the Rates and Revenue Team for action – credit card details are redacted prior to being stored in ECM.
Shared with:	■ Application information is deemed to be confidential. Any requests have to go through the Freedom of Information process. ■ Statutory Planning does not pass on personal information to any external parties.

	■ Some projects may be advertised on '*Comment on Cockburn*' but specific plans may be code/PIN protected to restrict access on a need to know basis.
Notified Issues:	■ USB devices received by post are not currently scanned for Malicious Software (*Malware*) prior to being entered onto the City's IT systems.
When/How Destroyed:	■ Not responsible for the destruction of customer contact information.
Departmental Comments:	■ The Statutory Planning team deals with short term development projects. Including people that are submitting building and other applications. ■ Statutory Planning team operates a paperless office. ■ No *S* Drive use. ■ Credit Cards can be used for application costs, online payment goes straight to the Rates and Revenue Team. ■ No credit card information received via email.
Assessor's Comments:	■ Whilst outside the scope of this PIA, the use of unscanned USB devices is a concern that needs to be addressed.

[R25-H] USB Scan Recommendation – Whilst outside the scope of this PIA, ES2 strongly recommends that anti-malware scanning procedures be documented and implemented for those departments where information is received from customers via a USB device. This will provide considerable protection from the potential for malicious software or virus to become installed on the City's IT equipment.

Appendix A: Example Privacy Policy

In addition to the conducing of the Privacy of Data and Information Impact Assessment, the City of Cockburn has requested that this engagement include a degree of assistance with the development of a Privacy Policy for the City. The following is a generic head start to aid in the development of that policy. This will need to be adjusted in order to make it specific to the City's situation. In particular, this example is of a publicly facing privacy policy such as can be displayed on a website or service. Many organisations also have a full internal privacy policy which would be of benefit to the City of Cockburn, the internal policy may include this external policy as an appendix:

The Privacy Act

The City of Cockburn has elected to align with the Australian Privacy Principles (APP's) set out in the Australian government's *Privacy Act 1988* (Cth) and associated amendments, which provide guidelines and rules for the collection, use, storage, protection and disclosure of Personally, Identifiable Information (PII) and sensitive information.

Your Personally Identifiable Information is important to the City of Cockburn

The City of Cockburn is committed to protecting your privacy. The City recognises that you have a right to control how your personal information that you entrust to us is collected and used. The City understands as a local government body that the handling of personal information is important and that your provision of that information is an act of trust and is something that it takes seriously. The City of Cockburn is not bound by the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth) and associated amendments but does recognise their value and as such is aligning our privacy processes to meet the auspices of this Act.

Collecting Personally Identifiable Information

The City of Cockburn collects personal information about its customers and stakeholders in many ways through its role as a local government authority in order to provide you with the services that you are entitled to. All personal information collected whether through electronic or manual means is afforded the protection that it deserves.

The City's website and other media allows you to make comments, give feedback and provide information including personal information through the use of various methods. Information is also manually collected from a number of sources including information being provided to our customer services department or any of the services provided for you.

The City of Cockburn will only use your Personally Identifiable Information for the purposes that it was collected.

Use of Personally Identifiable Information

Some functions of the City of Cockburn require that information be shared with third-party organisations and services. Such instances only occur where a process of due diligence has been undertaken and where the third-party has signed a non-disclosure agreement with the City.

Your Access to your Information

You have the right to know what information the City stores about you (subject to some exceptions permitted by law) and you have the right to ensure that this information is accurate. You can contact the City of Cockburn Privacy Officer[1] through the contact details at the end of this policy to achieve this. Depending on the complexity of your request a small charge may be applicable.

Policy Review

The City of Cockburn will from time to time review and revise all policies including this privacy policy. Reviews will be annual as a minimum, following changes to legislation or business direction or following significant changes in technology.

The City of Cockburn's Internal Privacy Policy will expand on each of the areas above written in a manner that targets the policy at City of Cockburn staff. The policy may need to include specific sections for departments to include the following:

- The types of information that constitutes PII and/or sensitive PII to make sure that all the City's staff are aware of the types of information that need to be protected.
- Collection limitations, what is approved methods of collection and what is not acceptable. The means of collection will in most instances need to include some notification from the information, provided that their information can be used for the purposes of which it was collected. Also, the subject should give their permission to distribute that information where reasonably necessary to do so.
- The policy needs to define how information must be protected once it has been collected. Where it can be stored and how it may be transferred between locations (where permitted). It is also important to specify specific areas where PII cannot be stored, this is likely to include the *H* Drive, *F* Drive, the *S* Drive, local drives on computers and laptops and removable media items such as USB sticks or USB hard disk drives.
- The policy needs to include levels of authority where this is appropriate, such as the levels of authority necessary before information can be transferred to another agency or to another local government organisation.
- How staff members are able to identify if a computer system or cloud service has been approved by City of Cockburn to be used to store, process or transmit PII.
- Retention periods for different types of PII in different situations.
- Approved destruction techniques for paper based PII, where it is stored on removable media (if approved) and destruction when stored on network or computer media.
- Detail of privacy related appointments including the City Privacy Officer and if appropriate conditions for delegation of authority.
- Detailed procedures to deal with requests from the public with regard to the quantities or accuracy of their PII.

[1] Needs to include an email address here. The Privacy officer is most likely a position combined with the City's Governance & Risk Support Officer due to the overlap in roles.

Data and Information Audit (Privacy Impact Assessment)

Appendix B: Privacy Risk Working Sheet

The following risk calculations define how the risk levels for recommendations within this report were derived. All calculations are based on the City of Cockburn risk matrix:

ID	Consequence	Likelihood	Risk	Comment /Justification
R1	Critical - 4	Possible – 3	Substantial-12	**Risk Documentation Recommendation** Could cause damage to the reputation of the city and damage to customers with the potential to result in legal action being taken against the City. Breaches are possible and happen far too often.
R2	Minor – 2	Possible – 3	Moderate-6	**Opt-Out Recommendation** Non-compliance with the Australian government's *Privacy Act 1988* (Cth) (or any future implementation within WA). Non-compliance is possible with current practices.
R3	Minor – 2	Possible – 3	Moderate-6	**NDA Recommendation** Non-compliance with policy (assuming that privacy policy is developed and approved), without policy then the same level would be achieved in loss of reputation. Likelihood of non-compliance assessed at being possible.
R4	Major – 3	Possible – 3	Moderate-9	***Lucky Orange* Recommendation** Non-compliance with the requirements for the handling and required protection of credit card information could as a minimum result in the need for investigation. Likelihood is assessed to be possible based on discussions held during the workshops.

Data and Information Audit (Privacy Impact Assessment)

ID	Consequence	Likelihood	Risk	Comment /Justification
R5	Critical – 4	Likely – 4	High-16	**Supplier Security Recommendation** The current threat climate has supply chain attacks as being one of the most common approaches by attackers. The potential is for incidents to occur which require third party actions or investigation. The current threat environment makes this a likely occurrence given time.
R6	Critical – 4	Possible – 3	Substantial-12	**FOI Recommendation** It is possible that in the event that PII is revealed through an FOI release may result in damage to the reputation of the City and public embarrassment.
R7	Critical – 4	Possible – 3	Substantial-12	**Privacy Policy Recommendation** It is possible that in the event that PII is mishandled through the lack of consistent policy could result in damage to the reputation of the City and public embarrassment
R8	Major – 3	Likely – 3	Substantial-12	**Video Recording Recommendation** It is likely that in the event that PII is published via council vision and audio without the consent of the subject that damage and public embarrassment may impact the reputation of the City.
R9	Critical – 4	Likely – 3	Substantial-12	***Dropbox* Recommendation** It is likely that in the event of an information security breach with the *DropBox* cloud application that this would result in damage and public embarrassment to the City.
R10	Minor – 2	Likely – 3	Moderate-8	**S Drive Recommendation** Use of the *S* Drive is likely to result in a breach that is contained within the confines of the City's departments limiting the Consequence of any resulting damage.
R11	Critical – 4	Likely – 3	High-16	**Secure Destruction Recommendation** There is considerable potential for damage to reputation and public embarrassment likely should information be retrieved through inadvertent disposal processes.

Data and Information Audit (Privacy Impact Assessment)

ID	Consequence	Likelihood	Risk	Comment /Justification
R12	Minor – 2	Likely – 3	Moderate-8	***F* Drive Recommendation** Use of the *F* Drive is likely to result in a breach that is limited to within the confines of the City's departments limiting the Consequence of any resulting damage.
R13	Major – 3	Possible – 3	Moderate-9	**Infringement Collection Recommendation** Where customers have not agreed to their personal information being sent to an offshore organisation, it is possible that a breach would result in a public complaint and moderate media attention.
R14	Major – 3	Possible – 3	Moderate-9	**Social Media Recommendation** In the event that personal information is inadvertently published on Social Media in the name of the City of Cockburn it is possible that this would result in a public complaint and moderate media attention.
R15	Major – 3	Possible – 3	Moderate-9	**Volunteer Recommendation** In the event that personal information of a volunteer is inadvertently released or breached by a third party that the City has passed this information to then it is possible this would result in a public complaint and moderate media attention. This would increase exponentially where more than one person's information is included in a breach.
R16	Major – 3	Possible – 3	Moderate-9	**Access Security Recommendation** If a person is able to anonymously access PII by using a generic and untraceable access account, there is the potential for PII to be breached resulting in public complaints and media attention.
R17	Critical – 4	Possible – 12	Substantial-12	**Credit Card Recommendation** The decentralised storage and handling of credit card information increases the potential for a breach of credit card information and therefore increases the potential for impact on the City.

Data and Information Audit (Privacy Impact Assessment)

ID	Consequence	Likelihood	Risk	Comment /Justification
R18	Critical – 4	Possible – 12	**Substantial-12**	**PCI Recommendation** This review has identified that credit card information is contained in a number of undesirable locations within the City's infrastructure. The breach of credit card information has the potential for critical levels of consequence.
R19	Critical – 4	Possible – 3	**Substantial-12**	**Policy Content Recommendation** The privacy policy is used to define the limitations of the City's use of PII. Failure to comply with the City's own published policy would possibly result in damage to the City's reputation and cause Public embarrassment.
R20	Minor – 2	Likely – 4	**Moderate-8**	***Outlook* Storage Recommendation** Use of *Outlook* as a storage location is likely to result in a breach of PII that is limited to within the confines of the City's departments limiting the Consequence of any resulting damage.
R21	Major – 3	Possible – 3	**Moderate-8**	**Security Classification Recommendation** Without the employing of a security classification scheme it is difficult for City staff to understand the impact should a piece of information be subject to a security breach. Without such a scheme it is likely that a breach of PII may not be identified resulting in moderate impact and moderate media attention.
R22	Critical – 4	Possible – 3	**Substantial-12**	**Policy Coverage Recommendation** The privacy policy is used to define the limitations of the City's use of PII, inclusion of employee information within the cover of PII. Any breach of personal information of employees can possibly result in damage to the City's reputation and cause Public embarrassment.
R23	Critical – 4	Possible – 3	**Substantial-12**	**Policy Improvement Recommendation** The privacy policy in place to cover the childcare services needs to be reviewed and updated to make it enforceable. Failure to comply with policy through misinterpretation or lack of content would possibly result in damage to the City's reputation and cause Public embarrassment.

Data and Information Audit (Privacy Impact Assessment)

ID	Consequence	Likelihood	Risk	Comment /Justification
R24	Major – 3	Possible – 3	Moderate-9	**Electronic Systems Recommendation** Having all information stored on paper provides an opportunity for theft or copying and in the event of a fire there is the risk that all information would be lost. There is a possibility that theft or fire could result in the loss of confidentiality or availability of information which would result in moderate impact to the City and moderate media attention.
R25	Critical – 4	Likely – 4	High-16	**USB Scan Recommendation** There is a threat that the use of uncontrolled USB devices could result in the virus infection of the City's systems or that malicious software may be surreptitiously installed. With current processes this is considered to be a likely scenario which could have critical consequences including damage to the City's reputation and public embarrassment with a high level of media attention.

Data and Information Audit (Privacy Impact Assessment)

Appendix C: City of Cockburn Risk Matrix

CITY OF COCKBURN RISK MATRIX, RISK ACCEPTANCE CRITERIA, EXISTING CONTROLS RATINGS AND OSH HIERARCHY OF CONTROL

RISK ASSESSMENT MATRIX

Measures of Consequence and Likelihood											Likelihood / Probability				
								Project			Rare 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
Consequence / Severity		OSH / Injury / Well-being	Financial Impact	Brand Reputation	Operations / Delivery Disruption	Environment Health	Compliance	Quality	Cost	Time	Theoretically such an event is possible but not expected to occur during an operation / asset life / project.	Possible that such an event may occur once during operation / asset life / project.	Such an event may occur more than twice during an operation / asset life / project.	Such events may occur frequently during an operation / asset life / project.	Such events are expected to occur routinely during an operation / asset life / project.
	Insignificant 1	No injuries.	< $50,000 or < 5% of OP. Little or no impact on asset.	Low impact. Low profile. No complaint.	Little impact. Business as usual. < 5% variation against PI.	An insignificant environmental event that can be immediately corrected under the control of the City.	Minor breach of policy / process requiring some response with little impact on other criteria.	Majority of milestones and objectives being achieved with minor variation to scope and/or quality reported. Minor impact absorbed through project.	< 5% of Project Budget or < $50,000 whichever is lower.	< 5% of Project Timeline or < 30 days, whichever is lower.	1 Low	2 Low	3 Low	4 Low	5 Moderate
	Minor 2	First aid treatment.	$50k ≤ to < $250k or 5% ≤ to <10% of OP. Minor loss or damage.	Low impact. Low profile. Low media attention. Possible complaint.	Minor impact. Easily dealt with. Still business as usual. 5 ≤ to < 10% variation against PI.	A minor environmental event that can be corrected through system improvements within the City.	Compliance breach of policy / process requiring additional work or minimal damage control.	Minor impact on milestones and objectives being achieved with minor variation to scope and/or quality reported. Disruptive impact on project deliverables expected.	5% ≤ to < 10% of Project Budget or $50k ≤ to < $250k, whichever is lower.	5% ≤ to <10% of Project Timeline or 30 ≤ to < 60 days, whichever is lower.	2 Low	4 Low	6 Moderate	8 Moderate	10 Substantial
	Major 3	Medical treatment. No lost time injury (LTI).	$250k ≤ and < $1m or 10% ≤ to < 25% of OP. Major damage to asset.	Moderate impact. Moderate media attention. Public complaint.	Some objectives affected. Can continue business as usual, with minor controls executed. 10 ≤ to < 25% variation against PI.	A moderate environmental event that can be remediated but requires multiple stakeholder input.	Compliance breach requiring investigation, mediation or restitution and breach of legislation or regulations.	Major impact on milestones and objectives being achieved with minor variation to scope and/or quality reported. Serious impact on project deliverables expected.	10% ≤ to < 25% of Project Budget or $250k ≤ to < $1m, whichever is lower.	10% ≤ to < 25% of Project Timeline or 60 ≤ to < 90 days, whichever is lower.	3 Low	6 Moderate	9 Moderate	12 Substantial	15 High
	Critical 4	Partial disablement or severe injury. LTI < 10 days.	$1m ≤ and < $5m or 25% ≤ to < 50% of OP. Significant loss of asset.	Damage to reputation. Public embarrassment. High media attention. Several public complaints. Third party legal action.	Some major objectives cannot be achieved. Business can still deliver, but not to expected level. 25 ≤ to < 50% variation against PI.	A significant environmental event where rehabilitation involves multiple stakeholders and various levels of the community and government.	Compliance breach involving external investigation or third party actions resulting in tangible loss or reputation damage to the City and breach of legislation or regulations.	Major impact on milestones and objectives being achieved with significant variation to scope and/or quality reported. Critical impact on project deliverables expected.	25% ≤ to < 50% of Project Budget or $1m ≤ to < $5m, whichever is lower.	25% ≤ to < 50% of Project Timeline or 90 ≤ to < 120 days, whichever is lower.	4 Low	8 Moderate	12 Substantial	16 High	20 Extreme
	Catastrophic 5	Death or permanent disablement. LTI ≥ 10 days.	≥ $5 million or ≥ 50% of OP. Complete loss of asset.	Irreversible damage to reputation. Very high level of public embarrassment. Very high media attention. Many public complaints.	Most objectives cannot be achieved. Business cannot operate. ≥ 50% variation against PI.	A severe environmental event requiring multiple stakeholders, all levels of the community and government to remediate.	Compliance breach involving regulatory investigation and / or third party actions resulting in tangible loss or significant reputation damage to the organisation and breach of legislation or regulations.	Catastrophic impact on milestones resulting in the failure to achieve one or more objectives of the project.	≥ 50% of Project Budget or ≥ $5 million, whichever is lower.	≥ 50% of Project Timeline or ≥ 120 days, whichever is lower.	5 Moderate	10 Substantial	15 High	20 Extreme	25 Extreme

Data and Information Audit (Privacy Impact Assessment)

Appendix D: Summary of Recommendations

The following table provides a one stop location for all the recommendations that have been made within this report:

ID	Recommendation Title	Recommendation
[R1-S]	**Risk Documentation Recommendation**	ES2 recommends that the potential damage to the reputation of the City of Cockburn that would result from a breach of Personally Identifiable Information be documented as a risk to the City of Cockburn and should be treated, regardless of the requirement under legislation.
[R2-M]	**Opt-Out Recommendation**	To comply with the Australian government's *Privacy Act 1988* (Cth), persons must be permitted to opt out of receiving direct marketing. This is most often achieved by including an 'unsubscribe' link in an email or a process whereby a person can reply to an email or SMS message with 'Unsubscribe' or 'Stop'.
[R3-M]	**NDA Recommendation**	Ensure that no PII is shared outside of the City of Cockburn (outside of the sphere of the proposed policy) needs to be subject to an NDA to assure that the information is handled and protected in the manner assured through the policy that it was collected.
[R4-M]	***Lucky Orange* Recommendation**	Recommend that the City's Cyber Security Officer review the *Lucky Orange* service in order to make an informed assessment on the potential risk to the City of Cockburn through its use. Particular emphasis needs to be placed on the applications coverage of privacy information and financial information.
[R5-H]	**Supplier Security Recommendation**	Whilst not entirely related to privacy. ES2 recommends that City of Cockburn develops and implements a supplier security policy document which includes due diligence requirements for cloud services in order to assure the use of cloud services does not compromise the position of the City with regard to the protection of privacy information entrusted to the organisation.
[R6-S]	**FOI Recommendation**	ES2 recommends that the processes surrounding the response to Freedom of Information requests be subject to governance. In order to protect the City, there needs to be policy and process documented

Data and Information Audit (Privacy Impact Assessment)

ID	Recommendation Title	Recommendation
		surrounding the City's response to requests for the release of information subject to the FOI. This instruction needs to ensure that PII is identified prior to any information release.
[R7-S]	**Privacy Policy Recommendation**	ES2 recommends that the City of Cockburn develops, publishes and communicates a Privacy policy to cover all of the City's dealings with Personally Identifiable Information. Regardless of the requirement for compliance, this is s a requirement to reduce the potential risk to the City's reputation should such information be inadvertently compromised. Additionally, the Policy would provide a much-needed consistency in the way that the City's departments handle and store PII.
[R8-S]	**Video Recording Recommendation**	ES2 recommends that procedures be developed to assure that PII is either blocked from video and audio recordings unless the PII subjects have provided written approval for their information to be published along with the audio and vision of council meetings. This can be achieved through prior notification of the recording and publishing of the recording being provided to all meeting participants or by requiring all meeting participants to sign to agree that any information spoken during the meeting will be published on the Internet.
[R9-S]	***Dropbox* Recommendation**	ES2 recommends that the use of *Dropbox* be discouraged across the City's operations in favour of using the more secure option of *OneDrive*. In particular it needs to be prohibited for the use or storage or transfer of PII.
[R10-M]	***S* Drive Recommendation**	ES2 recommends that the City of Cockburn conduct a campaign of information storage awareness training. This training should concentrate of what information is or is not suitable for storage on the *S* Drive and how information should be managed. The minimum recommended content for training would be: ■ What information needs to be stored on the ECM or in *TechnologyOne*. ■ Housekeeping of information within the ECM. ■ What information must not be stored even temporarily on the *S* Drive. ■ What information may be stored on the *S* Drive. ■ User's responsibilities with regards to the retention of information. ■ User risibilities with regards to the destruction of hard copy information.

Data and Information Audit (Privacy Impact Assessment)

ID	Recommendation Title	Recommendation
		Training should apply to all staff and management of City of Cockburn.
[R11-H]	**Secure Destruction recommendation**	ES2 recommends that a secure destruction policy or procedure be developed, approved and implemented by the City of Cockburn. This document needs to define the acceptable means of destruction based on the classification or sensitivity of the document or media in question. This instruction needs to ensure that information cannot be compromised through inappropriate destruction or disposal processes.
[R12-M]	***F* Drive Recommendation**	ES2 recommends that the *F* drive be reviewed to establish if there is any PII stored on the drive. If there is, then this needs to be migrated to ECM as a priority.
[R13-M]	**Infringement Collection Recommendation**	ES2 recommends that since City of Cockburn utilises an offshore collection agency for the recovery of library assets that uses of the library service should be informed of this. When a customer signs up for library services they need to be informed that in the event of an infringement their personal information will be passed to a US (foreign) based asset recovery agency. Customers must agree to this prior to membership.
[R14-M]	**Social Media Recommendation**	ES2 recommends that a 'two-person rule' process be implemented to ensure that all information published to Social Media in the name of City of Cockburn be reviewed and approved prior to publication/posting.
[R15-M]	**Volunteer Recommendation**	ES2 recommends that online forms be adjusted to include a 'permission to share information' component. This would then act as the authority from the subject to distribute their personal information to relevant volunteer organisations. Volunteer organisations receiving information must be subject to an NDA in order to assure that they are aware of the potential damage that could be caused if this information was subject to a security breach.
[R16-M]	**Access Security Recommendation**	Access to computers that then provide access to systems which contain PII needs to be achieved using a unique set of login credentials for each person accessing the computer. This ensures that all actions performed by a computer user are accountable and traceable to a specific person.

Data and Information Audit (Privacy Impact Assessment)

ID	Recommendation Title	Recommendation
[R17-S]	**Credit Card Recommendation**	ES2 recommends that all credit card transactions be centrally organised and conducted by a single City of Cockburn Department.
[R18-S]	**PCI Recommendation**	ES2 recommends that the City of Cockburn undertake a PCI assessment to establish the level of compliance with the PCI-DSS. This assessment should include the use of the Card Recognition scanning software *(https://www.groundlabs.com/card-recon/)* which will scan the entire network to identify all locations where Credit Card information exists. This will go a long way to identifying the levels of risk posed to the City should credit card information be breached and made public.
[R19-S]	**Policy Content Recommendation**	ES2 recommends that the privacy policy that is developed to support the City of Cockburn include all anticipated use of the PII that the City collects. The policy is published and used to advertise the use of collected PII to all persons that entrust that information to the City.
[R20-M]	***Outlook* Storage Recommendation**	ES2 recommends that The City of Cockburn conduct an IT educational piece to discourage users from using *Microsoft Outlook* as a file storage system
[R21-M]	**Security Classification Recommendation**	ES2 recommends that City of Cockburn considers the implementation of an information security classification scheme across the City's information enterprise. An information security classification scheme groups information based on the potential damage/impact/consequence that would impact the City should that information be subject to a breach of confidentiality. ES2 recommends that the City implements a simple classification scheme, the main aim being to be able to identify that information which requires the most protection including PII. Once the classification levels have been determined then appropriate protection, storage and handling processes per classification can be established.

Data and Information Audit (Privacy Impact Assessment)

ID	Recommendation Title	Recommendation
		This recommendation is to implement a process in alignment to that implemented by Federal government with levels that include Official and Official Sensitive as defined in the Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF).
[R22-M]	**Policy Coverage Recommendation**	ES2 recommends that the policy document to be developed, authorised and published should include the personal information pertaining to employees of the City of Cockburn in order to assure their protection the same as the protection of customer information.
[R23-S]	**Policy Improvement Recommendation**	ES2 recommends, that the childcare services privacy policy be updated and improved in conjunction with the development of the overall City of Cockburn proposed privacy policy. The wording within the policy must be definitive and easily understood to remove any conjecture and ensure that the policy is enforceable and that failure to comply with policy can be dealt with through the City's disciplinary process.
[R24-M]	**Electronic Systems Recommendation**	ES2 recommends that the City of Cockburn Cyber Security Officer works with the Youth Services team to overcome issues with confidence in IT system confidentiality. PII needs to be stored electronically in order to assure that it receives the appropriate level of protection. Paper based files should be transferred to an electronic system and then destroyed.
[R25-H]	**USB Scan Recommendation**	Whilst outside the scope of this PIA, ES2 strongly recommends that anti-malware scanning procedures be documented and implemented for those departments where information is received from customers via a USB device. This will provide considerable protection from the potential for malicious software or virus to become installed on the City's IT equipment.

17. MOTIONS OF WHICH PREVIOUS NOTICE HAS BEEN GIVEN

Nil

18. NOTICES OF MOTION GIVEN AT THE MEETING FOR CONSIDERATION AT NEXT MEETING

Nil

19. NEW BUSINESS OF AN URGENT NATURE INTRODUCED BY MEMBERS OR OFFICERS

Nil

20. MATTERS TO BE NOTED FOR INVESTIGATION, WITHOUT DEBATE

Nil

21. CONFIDENTIAL BUSINESS

Nil

22. CLOSURE OF MEETING

The meeting closed at 6.39pm.