



information
and privacy
commission
new south wales

AUDIT AND RISK COMMITTEE MINUTES

Date: Friday, 25 November 2022

Meeting Number: 59

Location: *Microsoft Teams*
Information & Privacy Commission NSW
Meeting Rooms McKell L15-Exec01-14 & McKell L15-Exec02-14
Level 15, McKell Building
2-24 Rawson Place
Haymarket NSW 2000

Time: 14:30-17:00

Members: Ms Marcia Doheny (Chairperson) (MD)
Mr Malcolm Clinch (MC)
Mr Peter Scarlett (PS)

In attendance: Ms Elizabeth Tydd, Information & Privacy Commission (ET)
Ms Samantha Gavel, Privacy Commissioner, Information & Privacy Commission (SG)
Ms Judy Malpas, O'Connor Marsden (JM)
Ms Sonia Minutillo, Information & Privacy Commission (SM)
Ms Pamela Robertson-Gregg, O'Connor Marsden (PR)
Ms Yasmine Salameh, Information & Privacy Commission (YS)
Ms Neharika Gossain (A/Director), Department of Customer Service (NG) (for finance discussion)

Minutes: Lynley Mattes, Information & Privacy Commission (LM)

Apologies: Mr Ian Naylor, Information & Privacy Commission (IN)
Ms Somaiya Ahmed, Audit Office (SA)
Ms Olive Ferino, Audit Office (OF)
Mr Michael Tzimoulas, Department of Customer Service (MT) (for finance discussion)
Ms Jessica Kavanagh, Information & Privacy Commission (JK)

ITEM

1. Chair Welcome

The Chair welcomed the attendees.

2. Attendance

Apologies received from Ian Naylor, Jessica Kavanagh, Michael Tzimoulas, Somaiya Ahmed & Olive Ferino.

3. A. Declarations of Interest

Nil.

B. Disclosures

Nil.

4. A. Minutes of previous meeting of 9 June 2022 & 21 September 2022

Endorsed by the Committee and confirmed for publishing.

B. Rolling Action Report

SM detailed 57.01 & 57.02 are ongoing and summarised in the papers.

5. A. Update from the Chair

The Chair spoke to the amendments to the Government Sector Finance Act (section 31 of Schedule 1 to the GSF Act) that creates significantly more transparency and accountability in relation to grants administration. This is a legislative obligation and a step forward to increasing public trust in government which is a very positive change. Another notable point of interest was Michael Coutts-Trotter's (MCT) speech (Chair to send to Lynley for distribution out of session) on integrity as a central element of the public sector in order to build and maintain public trust in government.

[Action Item: LM to distribute link to IPAA NSW | 2022 Annual State of the Sector event with Michael Coutts-Trotter](#)

B. Update from the CEO/Information Commissioner

ET recommends everyone read MCT's speech for its significant value.

The CEO/Information Commissioner took her paper as read and added that a meeting was held with DPC this week about the operation of a new Parliamentary initiative regarding an electronic system to manage documents subject to a Standing Order 52 (requirement for production).

ET spoke briefly to the AI Regulatory Landscape Scan and advised that it was attached, uploaded on the website and will be of benefit to the current and future government.

ET spoke to the submissions that IPC provided regarding the new recommendations made for reform of Grants Administration in NSW.

MC queried the assessment of NSW under the Right to Information Index by the entity located in Canada. ET advised that sub jurisdictions are not normally assessed and explained what NSW does well, although opportunities remain.

Discussion was had around the previous Philippines delegation and the initiatives they are working on in that country. ET advised that she participated in a TED Talk style event with the FOI team yesterday (which had over 600 attendees on Facebook stream).

C. Update from the Privacy Commissioner

The Privacy Commissioner noted her need to leave the meeting post this report and spoke to the proposed legislation to amend the PPIP Act for a mandatory data breach scheme. Parliament passed the bill without amendment. Particularly the bill is in harmonisation with the Commonwealth Mandatory Notification Scheme and is a credit to all the people who have participated in this work. The scheme will take place 12 months after assent which means the scheme will most likely commence next December.

Data breaches continue to be a challenge to the IPC. A lot of lessons have been learned across NSW government from the ServiceNSW breach. PS asked how do we learn from these breaches and how do we do better in the future? SG advised that the Chief Information and Security Officers' (CSOO) are deploying advice and she attended a presentation the other day. IPC's PAW in May this year focused on the learnings of breaches and Tony Chapman and the CISO's group will be wanting to do the same. PS noted that there is the technical issue and personal issues to these breaches, and it seems like there is potential for gaps to be fallen into and it's not clear how it is pulled together at a whole of government level. SG replied that DCS is leading agencies with their Essential 8 and other initiatives.

The Chair queried item 4 and the voluntary reporting of data breaches: 1. What do you do & 2. Does this create any risk for the IPC? SG provided a summary of the approach taken when a notification is received. The majority of breaches seen at the IPC, relate to human error and are fairly common (ie. email breaches) to which the IPC provide advice on ways agencies can improve the use of emails to mitigate and prevent simple but common email breaches ([Fact Sheet - Tips for reducing data breaches when sending emails](#) on the website). The IPC provides advice and the agency needs to equip themselves to manage the breach. ET spoke to the risk lens and the risks that may need to be managed relevant to our role (e.g. how do we know that the remediation has been effective?). Is it regulatory? Is the IPC's role one of assurance of an effective solution e.g. and how is that solution effective? SG noted that we do work closely with Cyber Security NSW and there are other ways to help inform us of these outcomes.

SG wished the ARC a merry Christmas and looks forward to seeing everyone in the New Years.

SG left the meeting at 15:00.

6. A. Financial Dashboard (October 2022)

MC queried how IPC is looking to control the pass-through costs. YS advised that they regularly review the costs as they come through and see them when they are approved for payment. Documentation is usually requested at that time to understand what costs are being paid for. The IPC is trying to improve this process. YS advised that some of the charges allocated to the IPC are part of DCS charges and confirmation is then sought as to what these charges are and how they relate to the IPC.

ET reiterated that our budget from Treasury allows for \$200k allocation for corporate services charges and that this was provided for under the MOU which has now lapsed. However, the charges are approximately \$600k. DCS today have advised that they have confirmed our advice that the charges are \$370k in addition to the 200K and ET queried what the charges were? NG advised the GovConnect charges are \$370k. The corporate services charges are \$200k and on top of that there are GovConnect charges of \$370k in 2021/22 which is where the charges are increasing each year, so she has advised the Chief Operating Officer (COO), Mandy Young of this situation for action.

ET queried if this is a model of sustainability and if other independents were affected? NG reported that she has only been in the role for 4 weeks but her main task has been to understand the GovConnect charges and what are driving the increases in these charges. ET noted that the charges to the head service recipient would also be increasing, and the drivers should be for DCS to take forward with the COO. DCS should take ownership and explore solutions. NG confirmed that she is meeting with GovConnect and the Chief Information Officer (CIO) to better understand the GovConnect charges. ET informed NG that the IPC has been investigating this important issue for the last 18 months as costs have been escalating since the MoG in 2019 and would like an outcome as soon as possible.

The Chair queried how the DCS corporate services charges are budgeted for but the GovConnect charges are not budgeted for and the charges can increase with no notice. NG responded that there is a base GovConnect charge budgeted for which is in addition to the corporate services charge of \$200k. What is happening is an increase which results in a variance which is what they are trying to understand what is driving these increasing costs.

PS queried whether there is a Service Catalogue? It was advised that the IPC were not originally provided a Service Catalogue but has recently been received a copy which has been reviewed for currency. ET stressed that the relationship is between DCS and the supplier and asked how do we work with DCS to go to Treasury to request funding for these additional and escalating corporate service charges that are out of the control of the IPC.

NG confirmed that at a cluster level they will need to go to Treasury with the three-year forecast. Amazon Web Services (AWS) are a large proportion of the cost which used to be funded by Treasury in capital-based projects. We need to be putting a case to Treasury to have cloud based funded. First, they will meet with Mandy Young, the CIO and then a brief will go to Treasury. NG stated that the solution needs to be driven between DCS and GovConnect.

The Chair advised that the IPC need an agreement from DCS that these charges are not sustainable, and an update provided within the month.

Action Item: DCS to provide an update of the Corporate Service Charges and pass-through charges, what these charges are, who is responsible given that the IPC has no relationship with the service provider (ie GovConnect) and an agreement from DCS that these charged are not sustainable and a course of action outlines, within the month (NG)

Discussion was had between capital, operational and savings and engaging Treasury.

B. GovConnect Update (payroll controls)

IN's update within this paper 6 was noted.

7. External Audit – 2021/2022 Financial Statements Update

A. 2021/2022 Financial Statements Update

IN's paper was taken as read.

8. Agency Planning and Reporting

A. Monthly IPC Case File Dashboard (October 2022)

IN's paper was taken as read.

B. Quarterly Report to the Attorney General & Minister Dominello – Quarter 1 July 2022 to September 2022

This report was taken as read. ET pointed out on page 4 the program of IT work involving projects funded through minor capital that provide a basis for enhancement within the IPC and externally. Enhanced IT is one way the IPC can continue to operate efficiently. These projects require a co-ordinated approach.

MC recognised the IPC's program of work and queried how the IPC is able to sustain its work program? Our landscape has changed as the operating environment is now digital and as a small agency and regulator, we don't have the same type of infrastructure as the big agencies that are delivering this work. We need to invest in IT systems as a small agency to assist significantly. ET suggested that the answer was devising an IT strategic plan 2022 – 2027 which will lend the IPC in a position to respond to the changing landscape in IT.

C. Cyber Security

PS asked if the IPC relies on DCS for the cyber security attestations? YS advised that the IPC is responsible for the case management system attestation. All other cyber security attestations are managed by DCS.

The Chair queried the report from Matt Fedele-Sirotych and YS advised that there was definitely an overall improvement from our results over the previous year. One decrease reflected stronger rules or criteria we had to meet which involved how we manage access which is something that wasn't documented (working with DCS around accesses in EDRMS). ET noted that paragraph 15 actually comprised 11 criteria which has been revised down to 8 so most scores will look better. The rating system was clarified with the ARC noting that the scoring system is up to 5.

PS queried the tables on pages 65 & 66 and discussion was had to provide clarification.

D. Auditor-General Report on the Internal Controls & Governance – IPC Progress Report

Discussion was had around the attached paper provided by IN and SM confirmed that the Auditor General completes an annual report and paper 8D is an update with actions being taken (standing agenda item).

E. Update of WHS actions arising

IPC Work Health & Safety Plan 2021 to 2023 was noted.

F. Legislative Compliance Register

The Chair praised this paper as easily informative and understandable.

9. Internal Audit

A. Internal Audit Reports, Recommendations Register & Status Register

The ARC endorsed the closure of the Governance Health Check. IPC Records Management Recommendations and agreed actions were summarised by SM. ET advised that the dependence upon DCS where a third of the actions to be completed in October were DCS's responsibility which will need to be monitored closely. The Chair asked how we relate with DCS. YS advised that there is a representative from DCS that they meet with regularly to progress the items which are overdue, and they are confident they will be closed out as soon as possible. Discussion was had around the formatting of item 9 on pages 5/6.

The Chair asked if the IPC were surprised by the results. ET noted that there is always room for improvement, and we rely greatly on DCS.

Action: IPC (responsible officer IN) to monitor completion of records management action to address delays in completion dates

B. QAIP Update (Institute of Internal Auditors)

Ken Robertson (KR) from the Institute of Internal Auditors joined the meeting and noted that the results were very good for a small agency and provided congratulations on the outcome of the audit. There are a few minor amendments suggested for the Charter. KR spoke to declarations and assertions. The QAIP standards requires an External Quality Assessment of Internal Audit to be periodical and KR suggests this should be conducted annually which ensures updates in future years is a lot easier. KR opened for questions. The Chair commended the report and IIA & SM's work. PS & MC concurred on the great outcome.

SM spoke to Item 9Bii and the Recommendations and Status. SM asked for the endorsement of 9D & 9E. PS queried page 228: Consulting to be defined to be deleted. Both papers endorsed by the ARC.

C. Strategic Internal Audit Plan

The ARC noted the Two-Year Strategic Audit Plan: 2022– 2023.

10. Risk Management 2022-2023

A. IPC Risk Register (includes WHS) Q1 & Q2 2022-2023

SM took the paper as read and drew the attention of the ARC to the consolidation of the two quarters. Not a lot of change to the risk mitigations as they align with the two-year strategic plan and are ongoing for completion. The PMES Survey was noted as there is a potential emerging risk for the IPC arising from the results (which has been captured in the emerging risk register).

The Committee discussed the risk register including S10 (page 241) which goes to insufficient funding; these are actually a subset of a number of risks which touch on a number of items.

Discussion was had around DCS's access to IPC's EDRMS server. SM noted that this matter is part of the Records Management Audit which is being worked on and remediated.

The Chair queried whether the risk around accommodation can be removed? ET advised that it has remained an issue as to Property NSW being able to direct where departments are housed and therefore remained on the risk register.

PS queried S2 on page 236 and movement from Extreme to Moderate after applying controls and shift of that order in ratings. Are we comfortable that our controls and treatment plans are able to control the shift in ratings? Discussion was had.

The change to S7 (Moderate) was queried and does IPC have sufficient resources to help reach that change? ET advised that there is an ability to test our impact (s37 and other ways e.g. compliance committee) overall 30% increase in applications and agency timelines has been maintained and that tells us we are building capacity within agencies and we have visibility. There has been an improvement in formal decision making and less complaints about failure to provide open access information and we do have some measures in place (IA) and we can be confident that we know that.

S7 question is much harder. In terms of what is written and available more broadly as we don't know that the technology actually works. There may be a gap in the IPC staffing profile relevant to this function. SM described that this is about our ability to influence and engage with our stakeholders and we see a lot of engagement with agencies to take further actions and steps and one of the things around MNDB Scheme is a resourcing profile of what we thought it would look like 3 years ago. This has become increasingly apparent and the type of skillset that we have been funded for has shifted.

PS point was, does the IPC have the resources to engage staff with expertise in these areas to work with the agencies? Needs to be revisited informed by above.

A. IA Report – IPC Enterprise Risk Management Framework Review

SM spoke to the Enterprise Risk Management Framework Review. PS queried the IPC Risk Appetite Statement and asked about the legislation where we have no tolerance from non-compliance for example WHS? SM noted that this was not taken into consideration as the primary thinking had been through a regulatory lens function and will take WHS and Fraud & Corruption forward in this regard. PRG will provide a document to SM to assist with the Appetite and how to present it.

Action Item: SM to review the ERM Framework Review Risk Appetite Statement and provide out of session

11. Review of ARC Charter Annual Calendar

A. Annual Calendar

Accepted as read.

B. Review of business continuity and disaster recovery arrangements

Accepted as read.

C. Fraud Control Plan

Endorsed by the ARC.

D. Review and report on the performance of the ARC

Accepted as read.

Other Business

Discussion was had around the proposed times and dates provided for 2023. New schedule confirmed below:

Schedule for 2023

- Thursday, 23 March 2023 (14:30-16:30)
- Thursday, 22 June 2023 (10:00-12:00)
- Friday, 22 September 2022 (10:00-12:00)
- Thursday, 16 November 2023 (10:00-12:00)

Action Item: LM to send calendar invitations as per above

Tenure Dates

Member	Appointment	Commencement Date	End Date	Extension End Date 1	Extension End Date 2
Malcolm Clinch	Member	5 July 2015	5 July 2018	5 July 2021	5 July 2023
Marcia Doheny	Member	28 June 2019	28 June 2022		
Marcia Doheny	Chair	17 June 2022			
Peter Scarlett	Member	17 June 2022			