Australian Government
Department of Industry,
Innovation and Science

Agenda Item 4.1
Meeting of 30 August 2019

ASSURANCE AND AUDIT COMMITTEE FOR ENDORSEMENT

Title	Annual certification for preventing, detecting and dealing with fraud.
Purpose/Issue	To advise that the department has appropriate mechanisms and processes in place to prevent, detect, and effectively respond to fraud so the accountable authority can provide certification of compliance with PGPA Rule 17AG(2)(b).
Recommendation(s)	That the Committee: ***Note the mechanisms in place to prevent, detect and respond to fraud.***
Attachment(s)	**A – Certificate of Compliance** Report demonstrating compliance with legislative requirements **B – High fraud risks by division** Chart of which risk each division assessed as a high risk **C – Enterprise fraud risk profile** List of identified fraud risks and the average fraud risk ratings **D – High fraud risk treatments** Chart of the treatments proposed by each division to control high risk
Prepared by	Section 47F Fraud Control Officer
Sponsored by	Janean Richards, Chief Operating Officer

Background

This Fraud Control Report demonstrates that the department has undertaken a number of measures to deal appropriately with fraud in 2018-19. The 2018-19 Certificate of Compliance is at ***Attachment A***.

Paragraph 17AG(2)(b) of the *Public Governance, Performance and Accountability Rule 2014*, requires that the department's annual report includes certification from the Accountable Authority that:

- fraud risk assessments have been undertaken and fraud control plans have been prepared;
- that there are appropriate mechanisms for preventing, detecting, investigating or otherwise dealing with fraud;
- that alleged fraud is recorded or reported upon; and
- all reasonable measures have been taken to deal appropriately with fraud.

Fraud risk management, prevention and awareness

Risk management

1. The department has a mature fraud and corruption risk management program. Fraud risk assessments are completed for each division every two years. As part of this program, divisions with fraud risk assessed as high are monitored by the fraud team on a quarterly basis.
2. Divisional fraud risk assessments inform the development of the department's Fraud and Corruption Control Plan, Enterprise Fraud Risk Profile and further fraud control activities. Fraud risk assessments are a self-assessment and approved by Heads of Divisions, taking into account risk appetite and mitigation strategies in place. The 2018-19 fraud risk assessments revealed:
   - There were no **very high** fraud risks as assessed by divisions;
   - Section 47E(a)
   - There were 11 fraud risks common to all divisions, with one division identifying additional risks relevant to their operations.
     - Resources Division identified one more fraud risk which was fraud against the administration of departmental programmes/activities including revenue collection (e.g. royalties/licensing fee receipts).

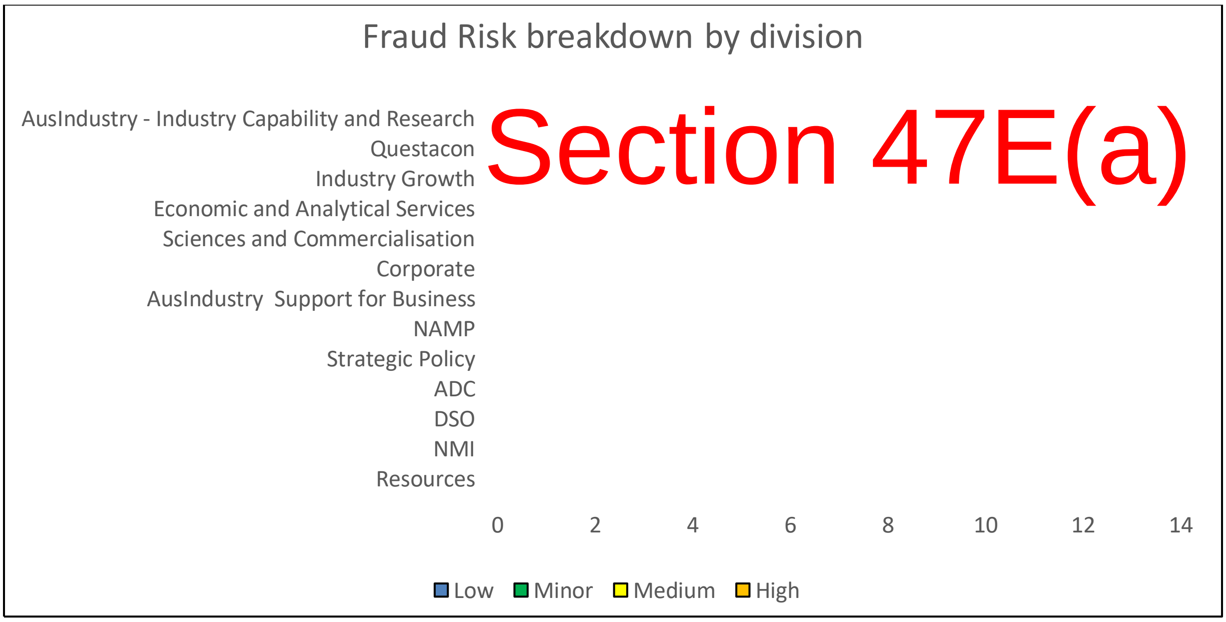
Table 1: Categories of high fraud risks identified by divisions

Internal Fraud Risks	***External Fraud Risks***

Section 47E(a)

Note: when the likelihood and consequence are averaged out in the Enterprise Fraud Risk Profile (see ***Attachment C***), Section 47E(a) .

Figure 2: All risks by division



Prevention

3. The fraud team is reviewing the divisional fraud risk assessments and fraud risk treatments (see ***Attachment D***). The review will focus on:
   a. supporting divisions to report on the implementation of fraud risk treatments for high risks to the Assurance and Audit Committee and Executive Board;
   b. analysing the risk treatments to identify common treatments and coordinating joint projects across the department to avoid duplication of effort and assign clear responsbility; and
   c. identifying new or emerging fraud risks, changes in fraud risk levels, or organisational changes impacting on fraud risk ownership.

4. The department's current ***Fraud and Corruption Control Plan 2018-20*** is published on the iCentral intranet page for all staff and contractors, as well as the Industry.gov.au internet site for external stakeholders and the general public. The Fraud and Corruption Control Plan will be updated from time to time to reflect changes in the enterprise fraud risk profile.

Awareness

5. Mandatory online fraud awareness training has been reviewed and a major effort is being made to improve completion rates. While the ANAO's Interim Report to Parliament on the 2018-19 Annual Audit of Finance Statements published that the department had a completion rate of 19 per cent at 30 June 2018. The completion rate is currently at 77 per cent (refer table 3). There are known data quality issues associated with compiling the completion rates. Work is underway with People and Planning and Data Management and Analytics Branch to reconcile data from Aurion and PageUp to provide accurate completion rates.

6. Work has commenced on developing a new face to face training program. The department will leverage the training packages of other agencies to benchmark and inform its new face to face training products, including tailored packages, to be rolled out in late 2019.

Table 3: Completion rate for mandatory online fraud awareness training at 1 July 2019

Division	Total Completed	%
Not allocated	Section 47E(a)	Section 47E(a)
Anti-Dumping Commission		
AusIndustry - Industry Capability and Research		
AusIndustry - Support for Business		
Australian Building Codes Board		
Australian Space Agency		
Corporate Group		
Department Executive		
Digital Strategy & Operations		
Economic & Analytical Services		
Finance Group		
Industry Growth		
National Measurement Institute		
NOPTA		
Northern Australia and Major Projects		
Office of Innovation and Science Australia		
Questacon[1]		
Resources		
Science Commercialisation Policy		
Strategic Policy		
Grand Total	**2,403**	**77.3**

Notes: All staff, contractors and consultants (i.e. all people who have been on-boarded, issued building passes and can access the IT system) are required to complete mandatory online training. Not completed includes booked, not started or in progress.

[1] Section 47E(a)

.

7. Two videos (an internal and external version) have been produced to educate staff and external stakeholders about the use of ‘Whispli’ which is the department’s confidential fraud reporting portal. The videos are available on the intranet and internet, and have been promoted to staff through iCentral news and the “Week at a Glance” summary of iCentral articles.

8. The Fraud Control Team joined with Finance staff to provide information sessions on changes to departmental credit card and travel policies. The presentations increased the profile of the team, generating further contacts for fraud advice and information. The team was also able to promote the serious repercussions for misuse of credit cards and staff entitlements.

Fraud detection and investigations

Detection

9. The department has clear guidelines and mechanisms for reporting suspected fraud, including the fraud hotline, Fraud Control Officer in-box, and the ‘Whispli’ confidential reporting tool. The Fraud Control Officer receives reports of alleged fraud from staff, members of the public and referrals from internal and external stakeholders.

10. The Fraud Control Officer also responds to requests for ad-hoc advice and 28 requests have been received during 2018-19. Themes of advice sought have surrounded Section 47E(a) .

11. The Fraud Intelligence Team have been reaching out to external agencies to foster data and intelligence searching capability and closer collaboration. Discussions have been held with Section 47E(a)

Using Section 47E(a) to detect fraud by grant applicants

12. The Fraud Control Team is supporting the department’s Data Strategy 2018-20 and the Digital Strategy 2017- 20 to become a data-driven organisation by developing new data analytics tools to support traditional fraud detection methodologies using active and reactive detection capabilities.

13. In 2018-19 the fraud team worked with Data Management and Analytics, and Digital Strategy and Operations (DSO) to Section 47E(a)

14. Section 47E(a)

Assessment and Investigation

15. Section 47E(a) These staff are responsible for dealing with reported incidents of fraud or suspected fraud.

16. On receipt of an allegation the referral is recorded in the case management system Section 47E(a) and allocated a ‘FIM’ reference. A case officer is allocated the assessment and is responsible for providing advice to the complainant or referral area. If there is sufficient evidence or information provided to support criminal investigation and potential prosecution, the matter is referred to the Investigations Manager who will conduct an investigation in line with Australian Government Investigation Standards and prepare a brief of evidence for the Commonwealth Director of Public Prosecutions.

Fraud allegations

17. The Department has had 35 active allegations of fraud during the 2018-19 financial year, 20 of which were new allegations received after 1 July 2018. Each allegation has been, or is in the process of being assessed. A breakdown of internal and external fraud allegations by division is provided in **figure 2** below.

Figure 2: 2018-19 Source of allegation of fraud by Division

Section 47E(a)

18. Internal allegation themes relate to Section 47E(a)

19. External allegations relate to Section 47E(a)

20. The outcomes of allegations closed after a case assessment (not accepted for investigation) have included: insufficient evidence to enable an investigation, cases that are not within the department's mandate, referrals to other agencies, fraud disproven or use of intelligence to monitor risks.

21. Section 47E(a)

.

22. Section 47E(a)

.

Attachment A – 2018-19 Certificate of Compliance

PGPA Act s26, PGPA Rule s10 Fraud Control	• A Fraud Control Plan must be implemented in line with the Commonwealth Fraud Control Framework 2017	• If a Fraud Control Plan was not implemented in line with the Commonwealth Fraud Control Framework 2017 • If instances of fraud were not reported to the Certificate of Compliance inbox when relevant	Department of Industry, Innovation and Science	Nil to report	Not applicable	All reasonable measures to prevent, detect and deal with fraud relating to the department have been taken during 2018-19. The department's fraud control and anti-corruption measures comply with the mandatory requirements of the PGPA Rule and the better practice measures as outlined in the *Commonwealth Fraud Control Framework 2017* and the *Australian Government Investigation Standards 2014*.
				Nil to report	Not applicable	In accordance with 10(a) PGPA Rule the department has conducted fraud risk assessments regularly, and when there was a substantial change in the structure, functions or activities of the department during 2018-19.
						In accordance with 10(b) PGPA Rule the department had developed and implemented *Fraud and Corruption Control Plan 2018-20* that deals with identified risks. That plan was in place during 2018-19 and was available on the department's internet page and intranet.
						In accordance with 10(c) (i) PGPA Rule the department had appropriate mechanisms for preventing fraud, and making staff aware of what constitutes fraud by developing and advertising the online fraud and corruption awareness online module, by participating in the International Fraud Awareness Week and by ongoing communications utilising the intranet throughout 2018-19.
						In accordance with 10(c) (ii) PGPA Rule, the risk of fraud and corruption was taken into account in planning and conducting activities of the department. This was achieved through the roll-out of fraud and corruption risk assessments across every division, the development of the SES Fraud Risk Management Guidance, Enterprise Fraud Risk Profile and treatment plans for each division.
						In accordance with 10(d) (f) PGPA Rule, the department had in place an appropriate mechanism for detecting incidents of fraud or suspected fraud, including a process for officials of the entity and other persons to report suspected fraud confidentially. These mechanisms included: *Passive* detection activities including the development and roll-out of new online two-way, anonymous reporting tool (whispli) and streamlining the fraud report process. *Active* detection - the department engaged an intelligence analyst to develop an active detection capability during 2018-19, Section 47E(a)
						In accordance with 10(e) PGPA Rule, the department had an appropriate mechanism for investigating or otherwise dealing with incidents of fraud or suspected fraud. The department's fraud investigations capability includes the engagement of qualified and experienced fraud investigators, maintenance of an Exhibits Facility, better practice complaint management practices, administration of a compliant Case Management System and better practice investigation standards which comply with the requirements of legislation and the *Australian Government Investigation Standards 2014*.
PGPA Act s46 Significant instances of non-compliance and the Annual Report for Commonwealth Entities	• All significant instances of non-compliance to the framework or finance laws reported to the Minister	• Have there been any significant instances of fraud identified?	**No**			
		• Have these instances been reported in the department's Annual Report?	**(N/A)**			

Appendix B - High fraud risks by division 2018-20

	Internal fraud risk type:	*Resources*	*National Measurement Institute*	*Digital Strategy & Operations*	*Anti-Dumping Commission*	*Strategic Policy*	*Northern Australia & Major Projects*	*AusIndustry - Support for Business*	*Corporate*	*Science and Commercialisation Policy*	*Economic & Analytical Services*	*Industry Growth*	*Questacon*	*AusIndustry - Industry Capability & Research*	**total**
1	Unauthorised access to, use of, and/or disclosure, modification or release of information including providing false or misleading information.														
2	Theft or misuse of departmental property, equipment or facilities including misuse or unauthorised use of Commonwealth motor vehicles (and fuel cards), computer equipment, electronic devices, awards or gifts, or improper disposal of assets.														
3	Misuse or theft of corporate credit cards, Cab charge, or other cash cards.														
4	Staff fraudulently claim entitlements (including expenses, allowances, travel or leave), misuse of travel claims, or payroll fraud etc.														
5	Fraudulent accounting practices including staff fraudulently circumventing accounts payable, accounts receivable, goods receipting, debt recovery, cash or accountable forms controls or fraudulent vendor invoicing etc.														
6	Fraudulent procurement practices, contract management or policy activities.														
7	Fraudulent recruitment practices or vetting (insider threat).														
8	Corruption including Foreign Bribery, abuse of office, accepting bribes or kickbacks, misuse or theft of Intellectual Property or trade secrets, serious failure to disclose or abuse of conflict of interest, undue influence, deliberate compromise or manipulation of investigations, or other serious or organised crime.														
	External fraud risk type:														
9	External unauthorised access, use, theft, disclosure, modification or release of departmental information including cybercrime or hacking to ICT systems.														
10	Applicants, recipients, third party providers or other external parties fraudulently claim for services, or financial assistance including submission of false information or identity, or deliberate omission of information for grant funding.														
11	Applicants, recipients, third party providers or other external parties fraudulently misuse, or misappropriate grant funding, gifts, ex-gratia payments, sponsorships or other benefits etc.														
12	Any other fraud risks against the administration of departmental programmes/activities including revenue collection (e.g. royalties/licensing fee receipts), Anti-Dumping Commission System or National Offshore Petroleum Titles Administrator etc.														
Total															

Section 47E(a)

Attachment C – Enterprise fraud risk profile (EFRP) - 2018-20

Enterprise Fraud Risk Statement		Enterprise Current Fraud Risk Ratings [1]					Enterprise Fraud Risk Owner (lead) [3]
			Current Likelihood	Current Consequence	Current fraud risk rating	Trend from 2016-18 [2]	
No.	Description	Divisions	*Rare*	*Insignificant*	*Low*		
			Unlikely	*Minimal*	*Minor*		
			Possible	*Moderate*	*Medium*		
			Likely	*Substantial*	*High*		
			Almost Certain	*Severe*	*Very High*		
Internal fraud risk type:							
1	Unauthorised access to, use of, and/or disclosure, modification or release of information including providing false or misleading information.	Section 47E(a)					Chief Information Officer (CIO), Digital Strategy & Operations (DSO) and Chief Operating Officer (COO), Corporate Division
2	Theft or misuse of departmental property, equipment or facilities including misuse or unauthorised use of Commonwealth motor vehicles (and fuel cards), computer equipment, electronic devices, awards or gifts, or improper disposal of assets.						COO, Corporate Division
3	Misuse or theft of corporate credit cards, Cabcharge, or other cash cards.						COO, Corporate Division
4	Staff fraudulently claim entitlements (including expenses, allowances, travel or leave), misuse of travel claims, or payroll fraud etc.						COO, Corporate Division
5	Fraudulent accounting practices including staff fraudulently circumventing accounts payable, accounts receivable, goods receipting, debt recovery, cash or accountable forms controls or fraudulent vendor invoicing etc.						COO, Corporate Division
6	Fraudulent procurement practices, contract management or policy activities.						COO, Corporate Division
7	Fraudulent recruitment practices or vetting (insider threat).						CIO, DSO and COO, Corporate Division
8	Corruption including Foreign Bribery, abuse of office, accepting bribes or kickbacks, misuse or theft of Intellectual Property or trade secrets, serious failure to disclose or abuse of conflict of interest, undue influence, deliberate compromise or manipulation of investigations, or other serious or organised crime.						CIO, DSO and COO, Corporate Division
External fraud risk type:							
9	External unauthorised access, use, theft, disclosure, modification or release of departmental information including cybercrime or hacking to ICT systems.						CIO, DSO and COO, Corporate Division
10	Applicants, recipients, third party providers or other external parties fraudulently claim for services, or financial assistance including submission of false information or identity, or deliberate omission of information for grant funding.						Relevant HoD Support for Business, HoD Industry Capability and Research, CIO, DSO Division
11	Applicants, recipients, third party providers or other external parties fraudulently misuse, or misappropriate grant funding, gifts, ex-gratia payments, sponsorships or other benefits etc.						Relevant HoD Support for Business, HoD Industry Capability and Research, CIO, DSO Division
12[5]	Any other fraud risks against the administration of departmental programs/activities including revenue collection (e.g. royalties/licensing fee receipts), Anti-Dumping Commission System or National Offshore Petroleum Titles Administrator etc.						Relevant HoD Support for Business, HoD Industry Capability and Research, HoD NMI, and HoD Resources Divisions

Enterprise fraud risk profile (EFRP) - 2018-20

1. The Enterprise fraud risks for ongoing monitoring and reporting against the department's Fraud Control and Corruption Plan 2018-20.
2. Trend of fraud risk from 2016-18 to 2018-20. Divisions have identified proposed treatment/s that either lower or maintain their DFRA risk rating compared to 2016-18
3. An appropriate lead assigned for monitoring the fraud risk at the enterprise level, noting there can be other fraud risk owners identified in respective DFRAs.
4. The figures reflect the number of Divisions which included this risk in their DFRA.
5. It is noted Enterprise Fraud Risk 12 includes a range of external fraud risks relating to programs administered by the department, thus the relevant HoD Support for Business, HoD Industry Capability and Research, HoD NMI, and HoD Resources Divisions are responsible for those risks.

Attachment D – High fraud risk treatments (consolidated list)

Section 47E(a)

Section 47E(a)

Section 47E(a)

Section 47E(a)

Section 47E(a)

Section 47E(a)

Section 47E(a)