s 47F

From: s 47F
Sent: Friday, 21 August 2020 5:01 PM
To: Greenwood, Emma
Cc: Fraud Control Officer
Subject: For information - Wrap up of 2018-20 Divisional Fraud Risk Assessment process – Support for Business [SEC=OFFICIAL]
Attachments: Attachment A Outcome of the independent review - Support for Business.docx

Good afternoon

For information, no action required

The Fraud Control Team (FCT) is currently preparing the 2019-20 Annual Certification of Fraud Control Measures for the Secretary's approval.

To ensure the team finalises all outstanding activities in respect of 2019-20, I'm writing to advise you of the outcomes of the Fraud Control Team's (FCT) review of the 2018-20 Divisional Fraud Risk Assessments, and provide you with an update on the status of the 2020-22 Divisional Fraud Risk Assessment Process.

Wrap up for 2018-20 Divisional Fraud Risk Assessment Process
Following the completion of Divisional Fraud Risk Assessments in April-May 2019, and collation of the Enterprise Fraud Risk Profile, the FCT presented the outcomes to Executive Board on 24 September 2019.

At the Executive Board meeting, the Secretary requested the 2018-20 Divisional Fraud Risk Assessments, which were self-assessed by divisions, be independently reviewed by the FCT to take into account known risks and to verify risk ratings.

The Fraud team reviewed all divisional fraud risk assessments and minor changes were made to some risk ratings. Changes made to your DRFA are attached for information.

Risk treatments: As part of the review, the FCT also collated common risk treatments proposed by divisions and identified some projects and activities that can be driven at a corporate level to address the risk treatments proposed by divisions. The FCT will liaise with divisions and corporate teams to reduce these common risk areas, and will continue to monitor the status of other risk treatments identified by divisions. Going forward, we are considering a divisional report back on risks rated as high, but this will be rolled into the 2020-22 approach (see below).

For information, the Secretary also requested the FCT consult other agencies on their fraud risk procedures to ensure the department's fraud risk methodology was aligned. The analysis of other agencies' risk assessment processes indicate that the department's approach is consistent.

2020-22 Divisional and Enterprise Fraud Risk Assessment Process
In line with the department's Fraud and Corruption Control Plan, the department updates divisional fraud risk assessments at least every two years, or following significant organisational changes, and collates the divisional fraud risk assessments to produce an Enterprise Fraud Risk Profile.

The FCT will soon commence the 2020-22 fraud risk assessment process. We intend to put a paper to EB in September to outline the process and will be in touch with divisions after that. We are revamping the process for 2020-22 to include tailored fraud risk training so staff are more engaged in the issues and can draw linkages to their work, and will provide new guidance and tools to support the completion of the fraud risk assessment. We will be leveraging some new resources developed by law enforcement agencies during the COVID-19 response.

In the meantime, please feel free to reach out any time you require fraud control advice or assistance, including to help inform the design of new initiatives.

Thanks, s 47F

s 47F

Manager
Audit and Fraud
Legal, Audit and Assurance Branch
Corporate and Digital Division

s 47E(d)

Department of Industry, Science, Energy and Resources | www.industry.gov.au

Supporting economic growth and job creation for all Australians

OFFICIAL

Attachment A: Outcome of the independent review of 2018-20 Divisional Fraud Risk Assessments

AusIndustry- Support for Business

Division	Risk	Self-assessed			Fraud Control Team Review			
		Likelihood	Consequence	Rating	Likelihood	Consequence	Rating	FCT Reasons

s 47E(a), s 47E(d)

Australian Government
Department of Industry, Innovation and Science

AusIndustry - Support for Business
Fraud Risk Assessment and treatment plan 2018–20

Risk Assessment

Program/Project/Activity	2018-20 Fraud Risk Assessment
Branch/Division	AusIndustry - Support for Business
Objective/Purpose *State the objective to which the risk plan relates. Describe intent, purpose and outcomes*	To assure to the Assurance and Audit Committee that the identified fraud risks faced by the Department of Industry, Innovation and Science, have a regular assessment and review of proposed risk treatment strategies
Context *List internal and external factors that influence this risk in relation to achieving objectives*	• AusIndustry has undergone a structural realignment based on the 'Mandate for Change', Mark Evans report and other portfolio strategic reviews • The government needs to meet the expectations of a modern public sector (with customers at the centre of everything we do) • Reform implementation and continuous improvement are complex and impact on workforce requirements • The department is managing service delivery across a distributed network
Date last reviewed	31 May 2019
Assessment conducted by *List all contributors*	AusIndustry – Support for Business Executive Officer AusIndustry – Support for Business Assurance Manager
Clearance by *(as per the risk action table)*	AusIndustry – Support for Business Executive Committee

Risk identification			Controls	Analysis			Owner	Evaluation	
Category Risk reference card	**Description** *Describe the risk or event (what can happen)* • *List the cause (what will cause the event to occur?)* • *Are any of the risks a shared risk?* • *Are there any constitutional risks?* ***Tip—Undertake a PESTLE or SWOT analysis to help define risks***	**Consequence** *What are the impacts of this occurring?*	**Current control(s)** *Such as existing policies; procedures; practice; governance committees; systems; technology; quality improvement plans* *Include controls for shared risks* ***Tip—is there a corresponding control for each cause of risk?***	Risk reference card **Likelihood**	**Consequence**	**Risk rating**	**Risk owner** Risk action table *Person/s responsible for managing the risk* *Include shared risk owners*	**Is risk within tolerance ?** Risk tolerance	**Accept risk?** Risk action table ***No** – Complete Treatment plan* ***Yes** – Optional Treatment plan*

s 47E(a), s 47E(d)

s 47E(a), s 47E(d)

s 47E(a), s 47E(d)

Risk Treatment Plan

Program/Project/Activity	2018-20 Fraud Risk Assessment
Branch/Division	AusIndustry - Support for Business
Date last reviewed	

Risk			Risk treatment					
Risk description	**Risk rating**	**Risk owner**	**Treatment action/s**	**Responsibility**		**Implementation**	**Monitor & Review**		
Copy from risk plan	*Copy from risk plan*	*Copy from risk plan*	*Selecting the most appropriate treatment options involves balancing the costs and efforts of implementation against the expected benefits.*	Risk action table		*Agreed timeframes for implementation of risk treatment*	Risk action table		
				Treatment owner	**Escalation**		**Frequency**	**Method**	**Status**
				Person responsible for implementing treatment	*Person for escalation/ reporting progress*		*The frequency progress is reported*	*How progress is reported*	

s 47E(a), s 47E(d)

Risk			Risk treatment						
Risk description	**Risk rating**	**Risk owner**	**Treatment action/s**	**Responsibility**		**Implementation**	**Monitor & Review**		
Copy from risk plan	*Copy from risk plan*	*Copy from risk plan*	*Selecting the most appropriate treatment options involves balancing the costs and efforts of implementation against the expected benefits.*	Risk action table		*Agreed timeframes for implementation of risk treatment*	Risk action table		
				Treatment owner	**Escalation**		**Frequency**	**Method**	**Status**
				Person responsible for implementing treatment	*Person for escalation/ reporting progress*		*The frequency progress is reported*	*How progress is reported*	

s 47E(a), s 47E(d)

Risk			Risk treatment						
Risk description	**Risk rating**	**Risk owner**	**Treatment action/s**	**Responsibility**		**Implementation**	**Monitor & Review**		
Copy from risk plan	*Copy from risk plan*	*Copy from risk plan*	*Selecting the most appropriate treatment options involves balancing the costs and efforts of implementation against the expected benefits.*	Risk action table		*Agreed timeframes for implementation of risk treatment*	Risk action table		
				Treatment owner	**Escalation**		**Frequency**	**Method**	**Status**
				Person responsible for implementing treatment	*Person for escalation/ reporting progress*		*The frequency progress is reported*	*How progress is reported*	

s 47E(a), s 47E(d)

Introduction

The Commonwealth Fraud Control Framework 2014 (the Framework) requires fraud risk assessments to be conducted at least every two years or when significant change to the organisation has occurred. Functions or operations associated with a high fraud risk, or that operate in environments with a high fraud or corruption risk, should assess risk more frequently.

The fraud risk assessment process ensures that potential exposure to fraud is identified and appropriately managed. This process informs development of the Department's Fraud Control Plan for 2016-18 including development of an Enterprise Fraud Risk Register.

This will also assist in providing assurance to the Secretary (who has overall responsibility for fraud control) that the appropriate mechanisms for preventing, detecting and dealing with fraud are in place.

Divisional Fraud Risk Assessment (DFRA) Workbook

To assist you in conducting a DFRA, this workbook provides:

- ***DFRA Worksheet*** - includes the draft outcomes based on discussions at your Division's fraud risk assessment workshop, together with additional draft content and ratings * (in blue text) for your review and updating as necessary.
- ***Definition of Fraud*** worksheet - extract of the Definition of fraud (including examples as defined in the Framework), Corruption and Foreign Bribery
- ***Risk Reference Card*** worksheet - extract of the department's risk reference card/matrix for completing your fraud risk ratings.

Some guidance to identifying and assessing the fraud risks

It is necessary to consider both internal and external fraud risks including corruption type fraud risks, as well as any new/emerging/unique fraud risks. In particular, please ensure that your DFRA:

- Identifies the fraud risks (for the functions, programmes, activities and systems etc) your Division and branches is responsible for.

- Assesses the likelihood, consequences, controls and proposed treatments to minimise fraud risks.
- Rating of fraud risks are aligned to the department's risk matrix.
- Assignment of ownership for the fraud risks and proposed treatments is appropriately identified.
- Please avoid the use of acronyms or ensure the first reference to the acronym is spelt out.
- As this is a 'Sensitive' document, distribution should be limited to those staff in your area you identify need to be involved in the fraud risk assessment process.
- The draft DFRA is returned to the Fraud.Prevention.Unit positional mailbox with your Head of Division approval/clearance by the requested due date.

* Note whilst indicative fraud risk ratings may have been included in your draft DFRA, these should be considered whether appropriate in your review and updated as necessary.

Ongoing monitoring and reporting

With fraud risk assessment being a continuous process, please ensure ongoing monitoring of your DFRA, such as:

- Monitoring fraud risks for changes (e.g. reviewing for changes in the fraud risk ratings).
- Taking action to implement the proposed treatments, including providing progress reports requested by the Fraud Prevention Unit.

- Organisational structure changes - reviewing for changes impacting on ownership of fraud risks and treatments.
- Future workshops - after your initial completed DFRA, you may wish to indicate any fraud risks which would benefit from a more comprehensive fraud risk assessment e.g. areas identified as high risks.

If you have any questions or would like to discuss the process further, please contact the Fraud Prevention Unit, (s 47F , Assistant Manager, Fraud Prevention Unit on s 47F , or s 47F , Senior Fraud Prevention Officer on s 47F

Division:	**Business Services Division (including BizLab)**
HOD Approval/Clearance:	**Chris Butler**
Date Approved:	**25 October 2016**

Risk Identification								Risk Analysis				Risk Treatment					Monitoring and Review			
Risk No.	**Division/Branch** *Source/area identifying the fraud risk*	**Fraud Risk Statement** *Identify possible sources of fraud risk - internal and external*	**Causes** *Why and how might this occur?*	**Fraud Risk Categories** *(use drop down list)* *(May need updating)*	**Fraud risk type** *(use drop down list)* **Internal (I) or External (E)**	**Consequences** *What are the impacts of this occurring?*	**Existing Controls** *What is currently done to manage this fraud risk?*	**Current fraud risk rating** *(use drop down list)* Likelihood	Consequence	Current risk rating	**Proposed Strategies/Treatments** *What additional strategies/treatments can be implemented to manage this fraud risk?*	**Residual fraud risk rating** *(use drop down list)* Likelihood	Consequence	Residual Fraud Risk Rating	**Due Date** *Target date to implement*	**Treatment Owner** *Who is responsible for implementing the proposed treatment (Role e.g. HOD, Name of Division)?*	**Fraud Risk Owner** *Who is accountable (Role e.g. HOD, Name of Division)?*	**General Comments** *Please include any general comments e.g. provide a brief reason for accepting any risks rated high or above without further mitigation strategies*
s 47E(a), s 47E(d)																				

Risk No.	Division/Branch *Source/area identifying the fraud risk*	Fraud Risk Statement *Identify possible sources of fraud risk - internal and external*	Causes *Why and how might this occur?*	Fraud Risk Categories *(Use drop down list)* *(May need updating)*	Fraud risk type *(Use drop down list)*	Internal (I) or External (E)	Consequences *What are the impacts of this occurring?*	Existing Controls *What is currently done to manage this fraud risk?*	Current fraud risk rating *(Use drop down list)*			Proposed Strategies/Treatments *What additional strategies/treatments can be implemented to manage this fraud risk?*	Residual fraud risk rating *(Use drop down list)*			Due Date *Target date to implement*	Treatment Owner *Who is responsible for implementing the proposed treatment (Role e.g. HOD, Name of Division)?*	Fraud Risk Owner *Who is accountable (Role e.g. HOD, Name of Division)?*	General Comments *Please include any general comments e.g. provide a brief reason for accepting any risks rated high or above without further mitigation strategies*
									Likelihood	Consequence	Current risk rating		Likelihood	Consequence	Residual fraud risk rating				

s 47E(a), s 47E(d)

Risk No.	Division/Branch *Source/area identifying the fraud risk*	Fraud Risk Statement *Identify possible sources of fraud risk - internal and external*	Causes *Why and how might this occur?*	Fraud Risk Categories *Use drop down list)* *May need updating!*	Fraud risk type *Use drop down list)*	Internal (I) or External (E)	Consequences *What are the impacts of this occurring?*	Existing Controls *What is currently done to manage this fraud risk?*	Current fraud risk rating *Use drop down list)*			Proposed Strategies/Treatments *What additional strategies/treatments can be implemented to manage this fraud risk?*	Residual fraud risk rating *Use drop down list)*			Due Date *Target date to implement*	Treatment Owner *Who is responsible for implementing the proposed treatment (Role e.g. HOD, Name of Division)?*	Fraud Risk Owner *Who is accountable (Role e.g. HOD, Name of Division)?*	General Comments *Please include any general comments e.g. provide a brief reason for accepting any risks rated high or above without further mitigation strategies*
									Likelihood	Consequence	Current risk rating		Likelihood	Consequence	Residual fraud risk rating				
s 47E(a), s 47E(d)																			

Risk No.	Division/Branch *Source/area identifying the fraud risk*	Fraud Risk Statement *Identify possible sources of fraud risk - internal and external*	Causes *Why and how might this occur?*	Fraud Risk Categories *Also drop down list)* *(May need updating)*	Fraud risk type *(Use drop down list)*	Internal (I) or External (E)	Consequences *What are the impacts of this occurring?*	Existing Controls *What is currently done to manage this fraud risk?*	Current fraud risk rating *(Use drop down list)*	Likelihood	Consequence	Current risk rating	Proposed Strategies/Treatments *What additional strategies/treatments can be implemented to manage this fraud risk?*	Residual fraud risk rating *(Use drop down list)*	Likelihood	Consequence	Residual fraud risk rating	Due Date *Target date to implement*	Treatment Owner *Who is responsible for implementing the proposed treatment (Role e.g. HOD, Name of Division)?*	Fraud Risk Owner *Who is accountable (Role e.g. HOD, Name of Division)?*	General Comments *Please include any general comments e.g. provide a brief reason for accepting any risks rated high or above without further mitigation strategies*
s 47E(a), s 47E(d)																					

[Draft]

Definition of Fraud

The Commonwealth Fraud Control Framework 2014 (Fraud Guidance) defines fraud against the Commonwealth as *'dishonestly obtaining a benefit, or causing a loss, by deception or other means'* . This definition is based on the fraudulent conduct offences under part 7.3 of the Criminal Code, in addition to other relevant offences under chapter 7 of the Criminal Code.

Examples of fraud against the Commonwealth may include (but is not limited to):

- theft
- accounting fraud (e.g. false invoices, misappropriation)
- misuse of Commonwealth credit cards
- unlawful use of, or unlawful obtaining of, property, equipment, material or services
- causing a loss, or avoiding and/or creating a liability
- providing false or misleading information to the Commonwealth, or failing to provide information when there is an obligation to do so
- misuse of Commonwealth assets, equipment or facilities
- cartel conduct
- making, or using false, forged or falsified documents, and/or
- wrongfully using Commonwealth information or intellectual property.

A benefit is not restricted to monetary or material benefit, and can be tangible or intangible, including the unauthorised provision of access to or disclosure of information. A benefit may also be obtained by a third party rather than, or in addition to, the perpetrator of the fraud.

Fraud against the Commonwealth can take many forms and may target:

- revenue (e.g. income tax, GST fraud, customs duties)
- property (e.g. cash, computers, other portable and attractive items, stationery)
- information and intelligence (e.g. personal information or classified material)
- program funding and grants
- entitlements (e.g. expenses, leave travel, travel allowances, attendance records)
- facilities (e.g. unauthorised use of vehicles, information technology and telecommunication systems), and
- money or property held in trust or confiscated.

Fraud can be committed by staff or contractors (internal fraud) or by persons external to the Department (external fraud) such as clients, service providers or other members of the public. It may also be committed jointly between an employee and outside party.

Definition of Corruption

AS/NZ 8001:2008 – Fraud and Corruption Control, defines corruption as: *"Dishonest activity in which a director, executive , manager, employee or contractor of an entity acts contrary to the interest of the entity and abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself for another person or entity"* .

Complex fraud, which may also constitute corrupt conduct, can include instances where an employee of group of employees are targeted and succumb to exploitation by external parties, or initiate the misconduct.

The Department must be alert to the risk of complex fraud involving collusion between agency employees and external parties.

Foreign Bribery
The Australian Government Policy on foreign bribery states:

Australia has a zero tolerance approach to foreign bribery and corruption. Australia works actively with foreign governments to stamp out bribery, and strongly discourages companies from making facilitation payments.

The Australian Government supports ethical business practices, and the prosecution of those who engage in illegal practices. This helps to improve Australia's investment opportunities overseas and is an important aspect of Australia's global reputation.

Foreign bribery undermines the reputation of all Australian businesses and impacts negatively on business and government relations.

Risk Reference Card (excerpt from the department's Risk Management Framework 2015-16)

GENERAL RISK CATEGORIES	CONSEQUENCE				
	INSIGNIFICANT	MINIMAL	MODERATE	SUBSTANTIAL	SEVERE
Capability and Capacity	Discrete skills deficiency within work teams	Loss of key personnel. Poor allocation/ management of resources within branches/ sections.	Gaps in skills, knowledge and experience to deliver objectives. Poor allocation/ management of resources within divisions	Skills, knowledge and experience are not developed or maintained to deliver key objectives. Deficient prioritisation of resources across the department	Skills, knowledge and experience are unavailable to deliver key objectives. The department is not agile to adapt to changing government priorities
Service Delivery	Temporary reduction in performance with no impact to business.	Interruptions causing temporary reduction in performance and inconvenience to business.	Interruptions to key functions leading to reduced performance and moderate impact on business accessing government assistance/ information	Breakdown of key functions leading to substantial impact on business accessing government assistance/information	Critical business failure leading to severe impact on business accessing government assistance/ information.
Business Outcomes	Policy advice and/or programme delivery substantially met intended Government priorities with some slight variations No adverse impact on target market to benefit from department's policy and programme initiatives	Policy advice and/or programme delivery varied from intended Government priorities Majority of target market benefit from department's policy and programme initiatives	Policy advice and/or programme delivery partially meet Government priorities Target market partially benefit from department's policy and programme initiatives with limited unintended negative impacts	Policy advice and/or programme delivery off track to meet Government priorities Minority of target market benefit from department's policy and programme initiatives with some unintended negative impacts	Policy advice and/or programme delivery fail to meet Government priorities Target market fail to benefit from department's policy and programme initiatives with unintended negative impacts
Reputation[1]	Customer complaint/ unsubstantiated rumours Minimal change in stakeholder confidence No media coverage Few audit recommendations which focus on improvement opportunities	Key stakeholders are concerned Scrutiny in local /specialist/social media Audit recommendations that can be addressed by management actions Temporary impact on public confidence	Minister is concerned Key stakeholders lose confidence in the department Criticism in local/specialist/social media Challenging audit recommendations that can be addressed with appropriate action plans Short term (less than 1 months) impact on public confidence	Minister loses confidence in the department Specific and sustained criticism at Senate Estimates hearings Key stakeholders outspoken against the department Criticism in national media Sustained criticism in social media or expansion into other media streams Adverse audit findings Medium term (less than 6 months) impact on public confidence	Prime Minister loses confidence in the department Key stakeholders actively coordinate criticism of the department Criticism in international media Parliamentary or judicial inquiry Detrimental audit report Lasting impact on public confidence
Administered Finance	Variation of administered funds <2% or $2.5 million without sound justification	Variation of administered funds >2% or $2.5 million without sound justification	Variation of administered funds >3% or $5 million without sound justification	Variation of administered funds >4% or $7.5 million without sound justification	Variation of administered funds >5% or $10 million without sound justification
Compliance (ex-security)	Technical breach of an internal policy or guideline	Failure to comply with internal policy or AAI Trivial, technical breach of Commonwealth Regulations	A single breach of Commonwealth Acts or Regulations or failure to comply with Government Policy	Multiple breaches of Commonwealth Acts or Regulations	Significant and protracted breach of major elements of law

SPECIALIST RISK CATEGORIES[2]	CONSEQUENCE				
	INSIGNIFICANT	MINIMAL	MODERATE	SUBSTANTIAL	SEVERE
Security	A security breach that could be expected to cause limited damage to National interest, organisations or individuals	A security breach that could be expected to cause damage to the National interest, organisations or individuals	A security breach that could be expected to cause significant damage to the National interest, organisations or individuals	A security breach that could be expected to cause serious damage to the National interest, organisations or individuals	A security breach that could be expected to cause grave damage to the National interest
Fraud and Corruption	A suspected fraud with negligible impact on individuals, systems and programmes. Insignificant or no financial cost. Loss of confidence contained to one minor stakeholder group.	A suspected fraud with minor impact on individuals, systems and programmes. Minimal or no financial cost. Loss of confidence by multiple minor stakeholder groups.	A suspected fraud or corrupt conduct with moderate impact to individuals, systems and programmes. May include moderate financial cost. Deteriorating confidence of one or more key stakeholder groups.	A suspected fraud or corrupt conduct that may have a major impact on individuals, systems and programmes. May include substantial financial cost. Significant loss in confidence by one or more key stakeholders.	A suspected fraud or corrupt conduct that could gravely threaten individuals, continued operation of systems and effectiveness of programmes. May include severe financial cost. Total loss of confidence by multiple stakeholders.
Work Health & Safety[3]	Work environment causes injuries or incidents that do not require medical attention	One-off or near miss Work Health and Safety incident occurs Work environment causes minor injury, first aid treatment required Multiple Work Health and Safety near miss incidents	Multiple Work Health and Safety near miss incidents Serious injury causing hospitalisation or multiple medical treatments cases	Preventable injury to staff Life threatening or multiple serious injuries causing hospitalisation	Preventable death of a staff member or persons Death or multiple life threatening injuries

LIKELIHOOD	PROBABILITY	LIKELIHOOD RATING	CONSEQUENCE RATINGS				
			INSIGNIFICANT	MINIMAL	MODERATE	SUBSTANTIAL	SEVERE
↑	The event is expected to occur in most circumstances as there is a history of recurrence.	Almost Certain	Minor	Medium	High	Very High	Very High
↑	The event is expected to occur with strong possibility as there is a history of frequent occurrence.	Likely	Minor	Medium	High	High	Very High
↑	The event might occur as there is a history of casual occurrence.	Possible	Low	Minor	Medium	High	Very High
	There is a slight possibility that the event might occur at some time.	Unlikely	Low	Minor	Minor	Medium	High
	The event is not likely to occur, but may occur in exceptional circumstances.	Rare	Low	Low	Minor	Medium	High

1. Reputation risk is a strategic risk that can not be considered in isolation. This is a risk that is driven by a wide range of other risks that should be actively managed to reduce reputational consequence.
2. For risks relating to Security, Fraud and WH&S, specialist risk frameworks exist and should be referred to where appropriate.
3. 'Injury' refers to both physical and psychological injuries.