Agenda Item 2.5

NATIONAL DISABILITY INSURANCE AGENCY BOARD
BOARD MEETING 14/2014 OF 19 NOVEMBER 2014

UPDATED RISK MANAGEMENT STRATEGY

Recommendation(s) – that the Board:

1. **Note** that the Risk Management Framework (Framework) approved by the Board at its September meeting includes the Agency's written risk management strategy (Strategy) at Chapter 4 (**Attachment A**).

2. **Agree** that the Board submit the entire Framework to the COAG Disability Reform Council (Ministerial Council) seeking approval of the Strategy, to comply with the requirement in the National *Disability Insurance Scheme-Risk Management Rules 2013* (Risk Management Rules) that the Agency's risk management strategy, and any material amendments to it, must be submitted to, and approved by, the Ministerial Council.

Key Issues and Sensitivities

1. The Risk Management Rules require the Board to have a risk management framework that includes a written risk management strategy. The framework does not have to be in writing.

2. The Risk Management Rules further require that the strategy, and any amendments to it, must be approved by the Ministerial Council, and the Board must submit the strategy or amendments to the Ministerial Council as soon as reasonably practicable after the strategy or amendments have been approved by the Board.

3. At its September meeting the Board approved the Framework, which includes the Agency's Strategy at Chapter 4 (see Attachment A).

4. Given the Strategy is inextricably linked with the Framework approved by the Board, we recommend that the Board submit the entire Framework to the Ministerial Council, seeking approval of the Strategy only, as required by the Risk Management Rules.

5. The alternative would be to submit only the Strategy at Chapter 4 of the Framework to the Ministerial Council. However:

    a. this would require the drafting of substantial additional contextual material to support the Strategy – for example, because the Strategy cross-refers to other parts of the Framework, and

    b. this would lead to the development of an additional stand-alone risk management document, rather than an integrated framework as approved by the Board.

Key Legal Issues / Risks

6. The Agency's Corporate Counsel has advised that submitting the Framework to the Ministerial Council would meet the Board's obligation under the Risk Management Rules to submit the Strategy for approval.

7. In addition, following table shows how the Strategy, as articulated in the Framework approved by the Board, meets the minimum requirements specified in section 8(1) of the Risk Management Rules:

The risk management strategy must: (see Risk Management Rules, section 8(1))	**Cross-reference to Agency Risk Management Framework (including Risk Management Strategy) (see Chapter 4)**
(a) outline the risk governance relationship between the Board, committees of the Board and the senior management of the Agency	pages 22—29
(b) describe the processes for the Agency to identify and assess risks	pages 30—34
(c) describe the process for the Agency to establish mitigation and control mechanisms for individual risks	pages 35—37
(d) describe the process for monitoring and reporting issues in relation to risk (including the communication and escalation of such issues)	pages 38—40
(e) describe how the Agency is to: (i) ensure that relevant staff are aware of issues relating to risk; and (ii) instil an appropriate culture in relation to risk; and (iii) ensure that the risk management strategy is accessible to the Agency's staff	page 40
(f) identify persons and positions in the Agency with roles and responsibilities in relation to risk, or groups of such persons and positions, and set out those roles and responsibilities	pages 41—44
(g) describe the review process [ie, a review process to ensure that the risk management framework is effective in identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating, material risks (see section 5(4)(d))]	page 44

8. The Framework (and Strategy) will be reviewed by the Board on an annual basis and Ministerial Council approval of the Strategy will be required if material changes are made to the Strategy.

Prepared by: s22	Approved by: s22
Team: Director , Risk and Assurance	A/g General Manager
Phone: s22	Phone: s22

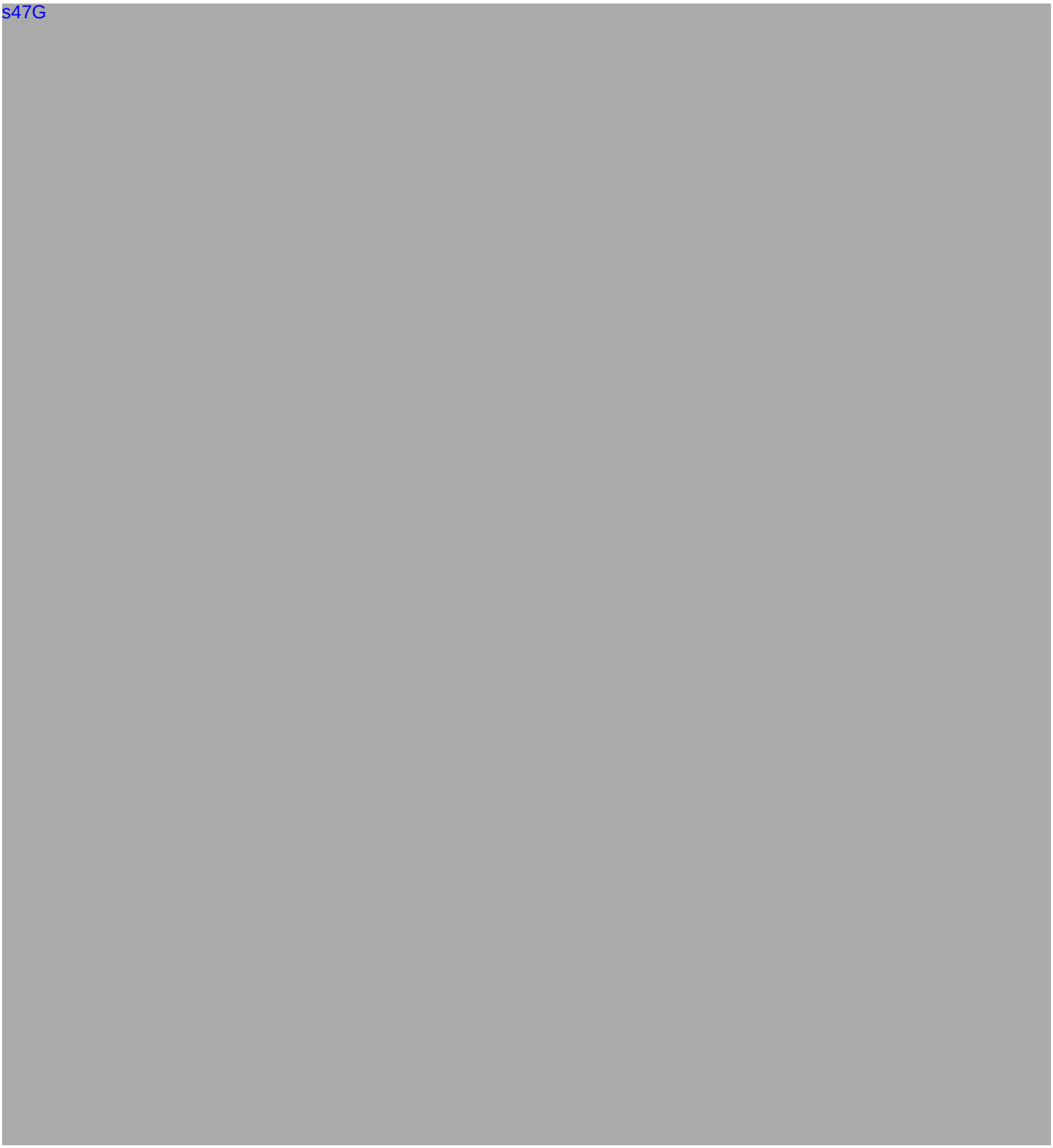
Attachments:

Attachment A NDIA Risk Management Framework

From: Comcover <comcover@comcover.com.au>
Sent: Thursday, 8 January 2015 12:35 PM
To: Comcover
Subject: Comcover Update - January 2015

s47G

s47G



From: s22
Sent: Friday, 6 March 2015 4:18 PM
To: 'comcover@comcover.com.au'
Cc: s22
Subject: Feedback in relation to the 2015 Comcover Risk Management Survey [SEC=UNOFFICIAL]

Good afternoon,

s47C

s22

Director
Risk and Assurance Team
Legal, Parliamentary and Risk Branch
National Disability Insurance Agency

T s22 **E** s22 @ndis.gov.au

From: s22
Sent: Friday, 6 March 2015 3:32 PM
To: s22
Cc: s22
Subject: FOR ACTION: Comcover risk management benchmarking survey 2015 [SEC=UNCLASSIFIED]
Attachments: SCANNED COPY_SIGNED_Comcover Risk Management Benchmarking Survey 2015_06 MAR 15.PDF

s22

s47C

s22

A/g General Manager and Chief Risk Officer
Governance Division
National Disability Insurance Agency

T s22 **M** s22 **E** s22 @ndis.gov.au

Australian Government
Comcover

Comcover Risk Management Benchmarking Survey 2015

s47E(d) - certain operations of agencies

Comcover Benchmarking Survey: 27 January - 6 March 2015

Stephen Broadfoot
National Disability Insurance Agency

Terms and Conditions

Terms and Conditions

I, on behalf of my entity, have read and agree to the terms and conditions outlined above: *

☑ -

- **Terms and Conditions for Survey Participation**

Access to Comcover's Benchmarking Survey is provided subject to the following conditions. Use and participation in this Survey constitutes acceptance of these conditions in full.

This survey is presented by Comcover for the purpose of obtaining information regarding the Risk Management practices of Fund Member entities for benchmarking their risk management capability and maturity.

The person/s completing the survey should consult with others in their organisation to ensure the accuracy of their entity's responses in particular when identifying the target maturity states for each element of the survey.
Participants have six weeks to complete the survey and it will not be possible to grant an extension after the survey closes. All responses must be submitted online via the survey tool. Participants cannot update or amend their answers to the survey after the closing date.

Participants should be aware that there are inherent risks transmitting information across the Internet. Information submitted unencrypted via email or web forms may be at risk of being intercepted, read or modified.

In order to check the integrity of the survey results, Deloitte Touche Tohmatsu (Deloitte) will conduct a series of random validation reviews of the responses of a selection of entities once the surveys are completed and submitted. In participating in the programme, you acknowledge that your entity's survey responses may be examined and agree to allow this to occur, and to assist where possible, provided you are given a minimum of 24 hours' notice of such an intention by Deloitte staff.

You also acknowledge that if, based on the validation reviews,, one or more responses to questions in the survey should be modified, you will accept the revised answers and the revised benchmark score. In such an instance, you will be consulted prior to finalising the decision to modify one or more of your entity's responses.

Comcover will have access to the responses of all participating entities. . It will take appropriate measures to keep all information confidential and secure. The survey is carried out and benchmarking analysis will be prepared for Comcover at their request and in accordance with the contract with Deloitte. You acknowledge that the benchmarking analysis and any benchmarking information to which you may be provided access relates to the work which is being undertaken by Deloitte under the direction of Comcover for the purpose stated above. Any benchmarking information to which you may be provided access may not be sufficient or appropriate for any other purpose. Any questions regarding the scope of the work performed or regarding any of the benchmark information should be addressed to Comcover, for the attention of the Director, Risk Management.

You agree that you will not make any claim or demand or bring any proceedings against Comcover or Deloitte in connection with the benchmarking information or any

extract there from to which you are provided access.

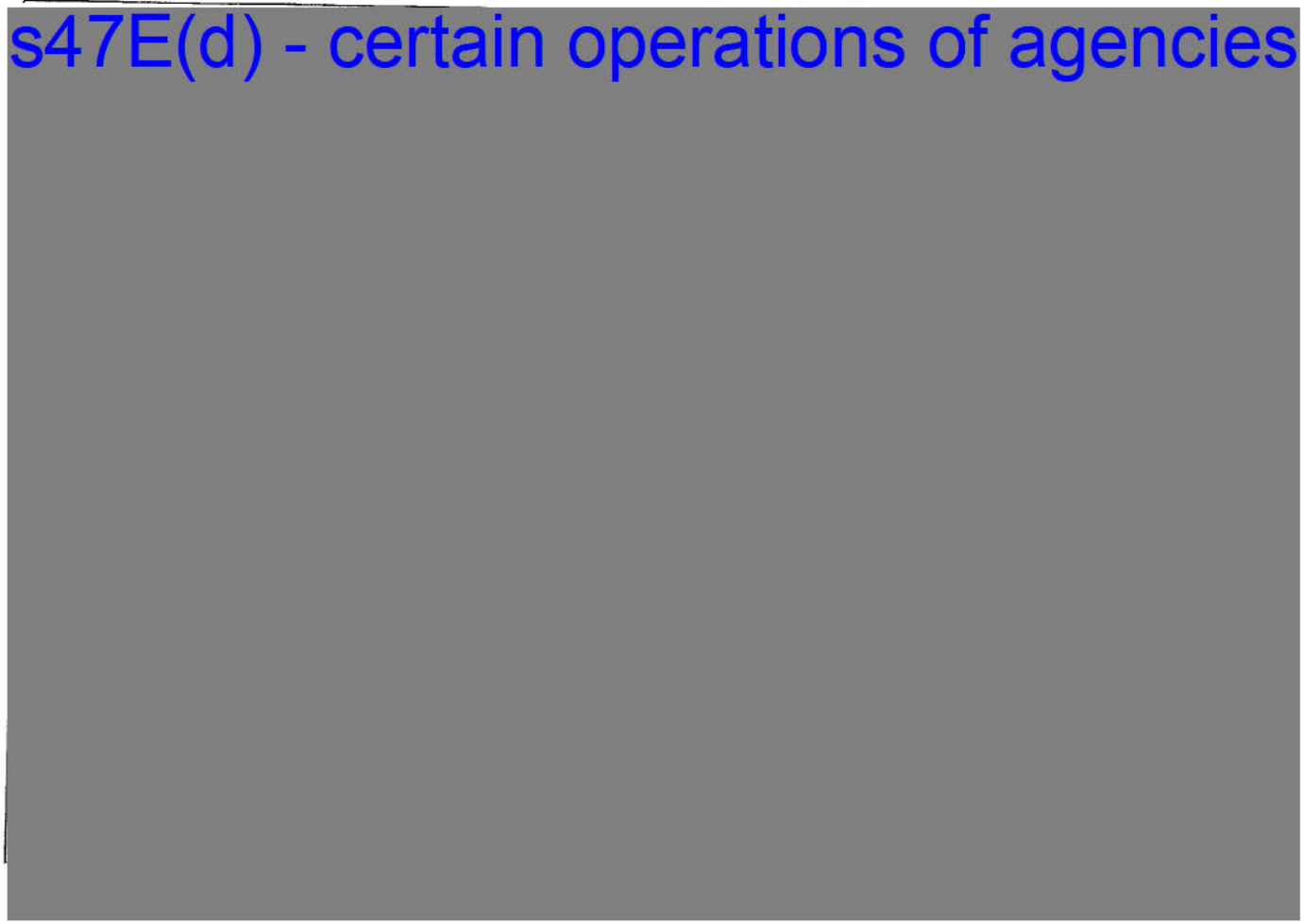
Comcover retains all intellectual property rights in the survey. Any unauthorised use or duplication of the survey without prior permission from Comcover or Deloitte is prohibited.

I, on behalf of my entity, have read and agree to the terms and conditions outlined above:

Establishing a risk management policy

s47E(d) - certain operations of agencies

Establishing a risk management policy



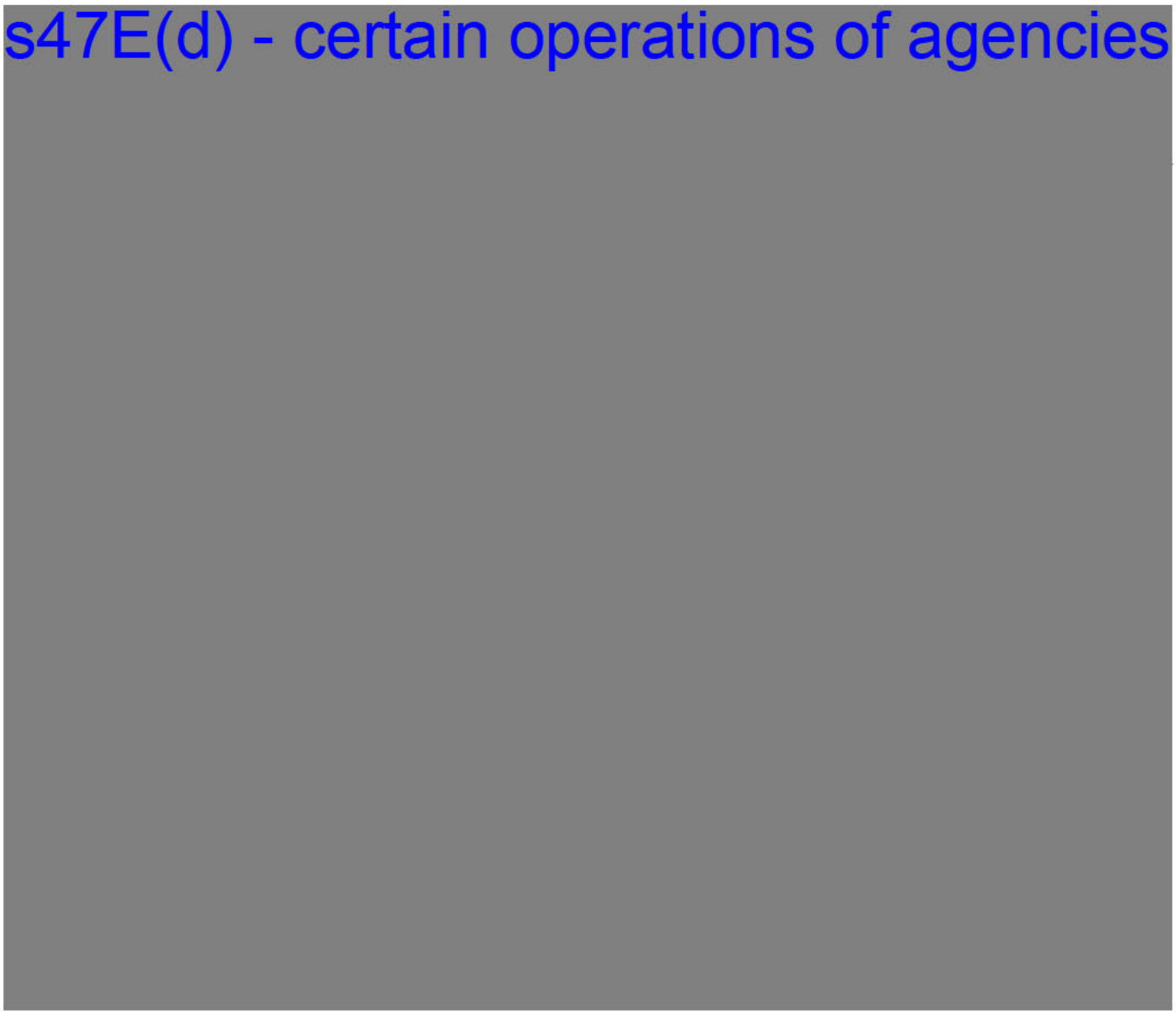
Establishing a risk management policy

s47E(d) - certain operations of agencies

Establishing a risk management policy

s47E(d) - certain operations of agencies

Establishing a risk management framework

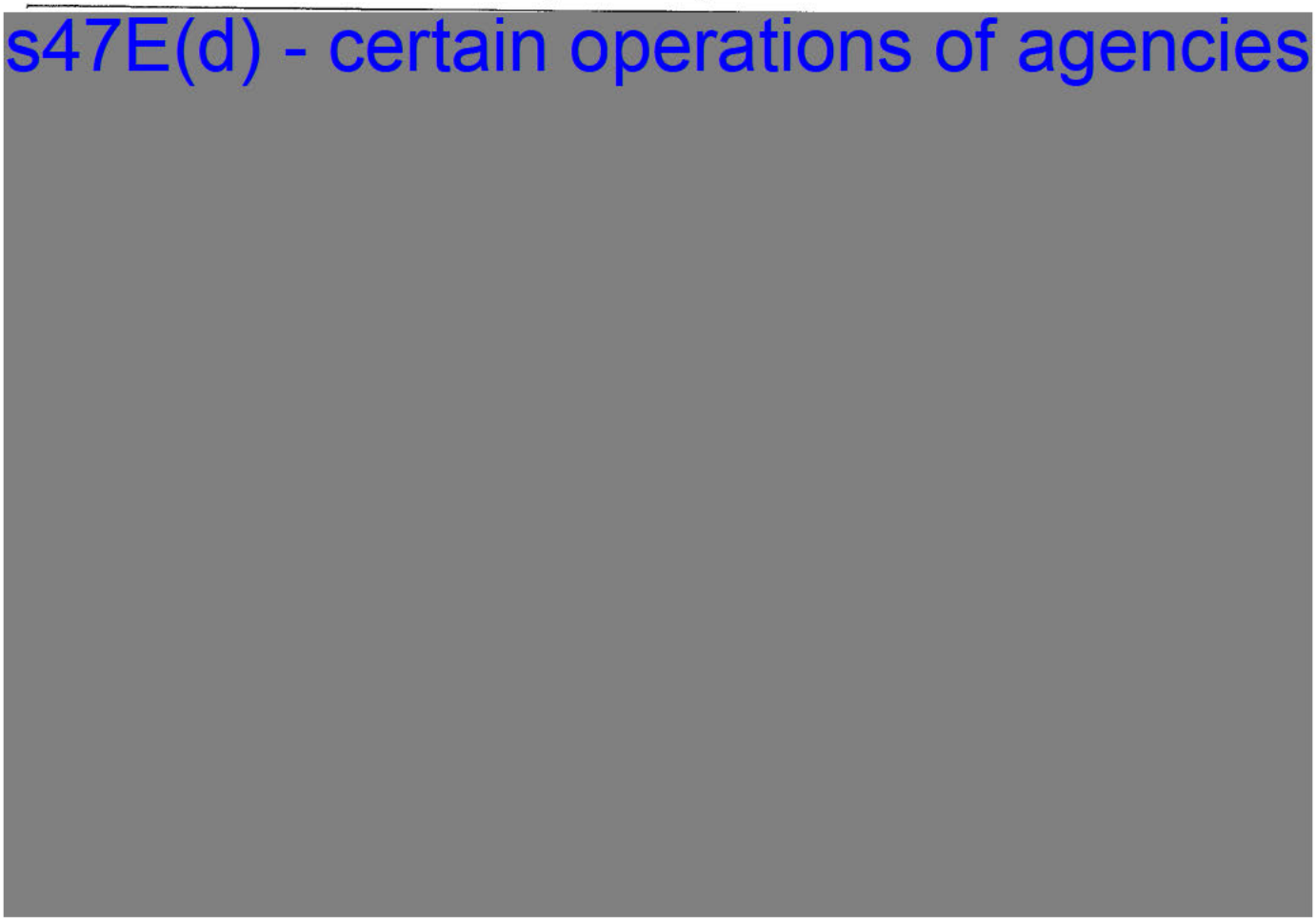


Establishing a risk management framework

Establishing a risk management framework

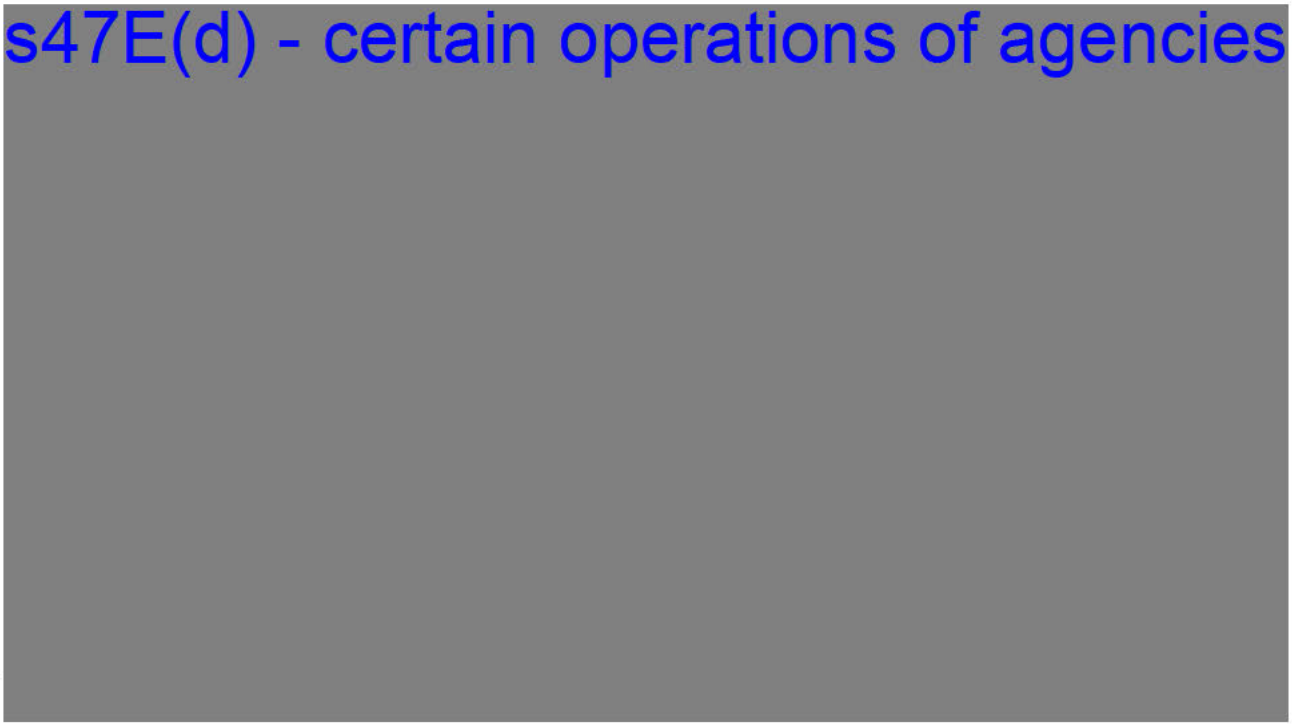
s47E(d) - certain operations of agencies

Establishing a risk management framework



Establishing a risk management framework

Notes section – please use this text box to make any notes relevant to this question. These notes will not impact scoring:



Establishing a risk management framework

s47E(d) - certain operations of agencies

Establishing a risk management framework

s47E(d) - certain operations of agencies

Establishing a risk management framework

s47E(d) - certain operations of agencies

Establishing a risk management framework

s47E(d) - certain operations of agencies

Establishing a risk management framework

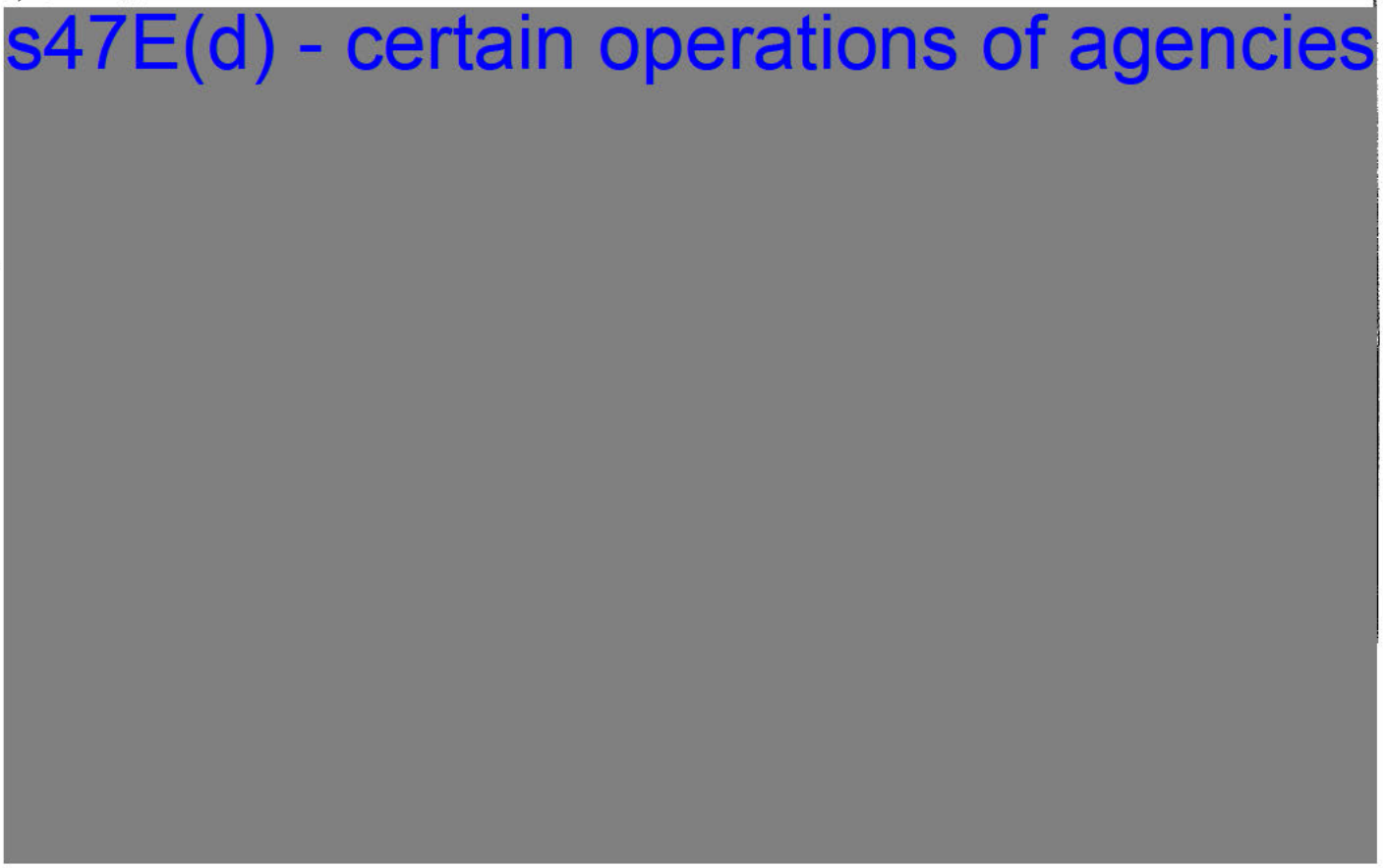
s47E(d) - certain operations of agencies

Establishing a risk management framework

s47E(d) - certain operations of agencies

Establishing a risk management framework

s47E(d) - certain operations of agencies

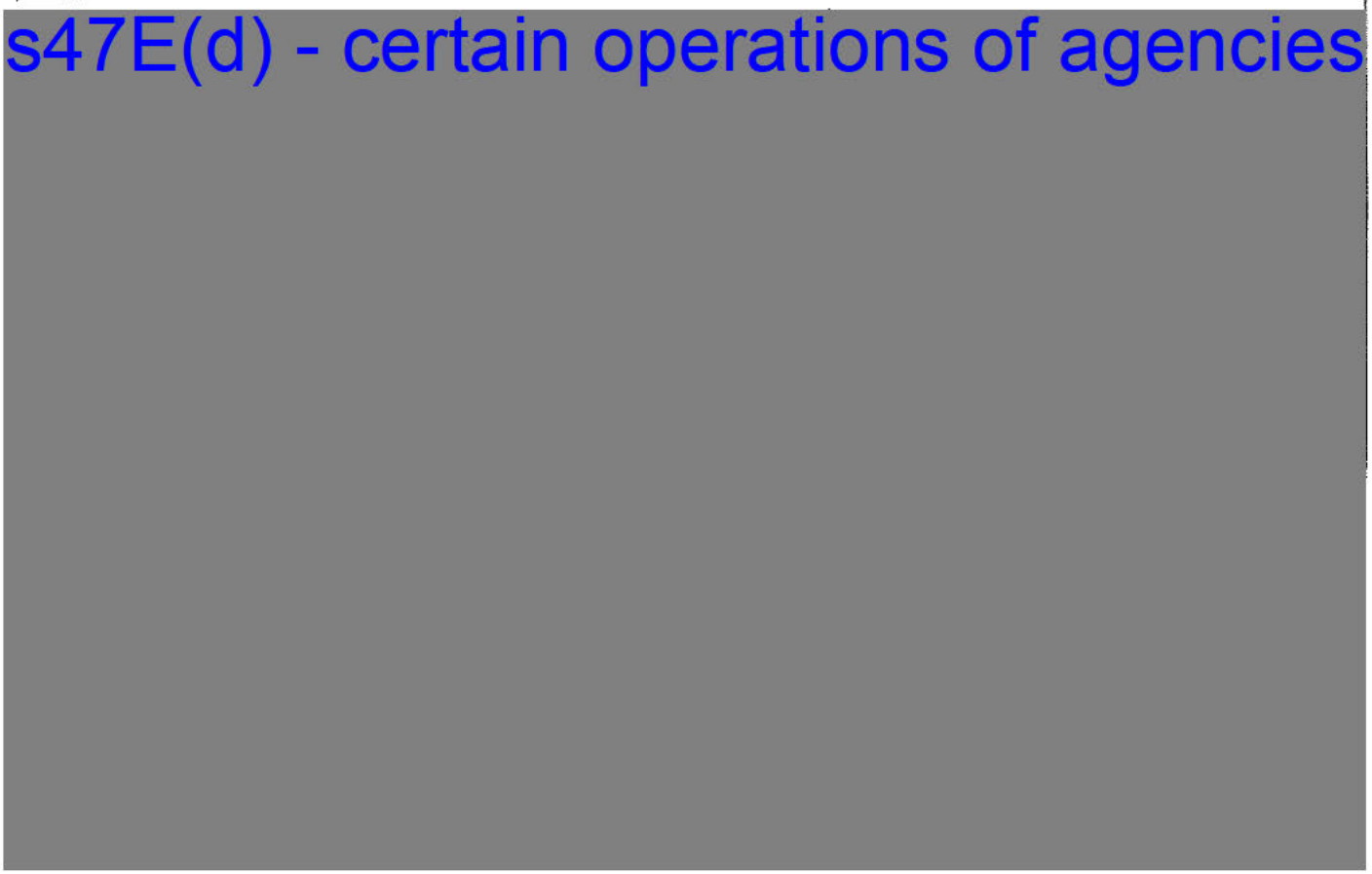


Establishing a risk management framework

s47E(d) - certain operations of agencies

Establishing a risk management framework

s47E(d) - certain operations of agencies

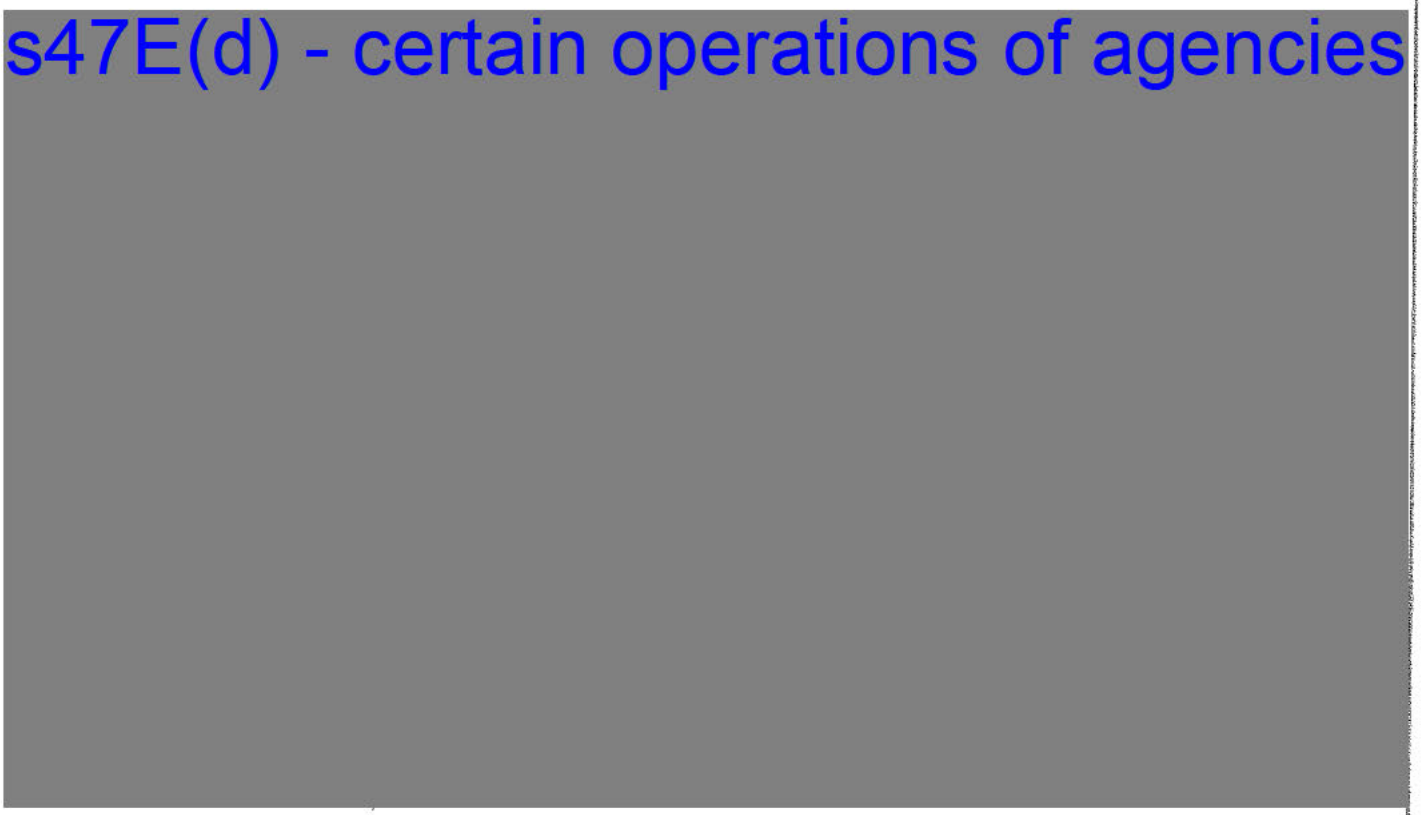


Defining responsibility for managing risk

Defining responsibility for managing risk

s47E(d) - certain operations of agencies

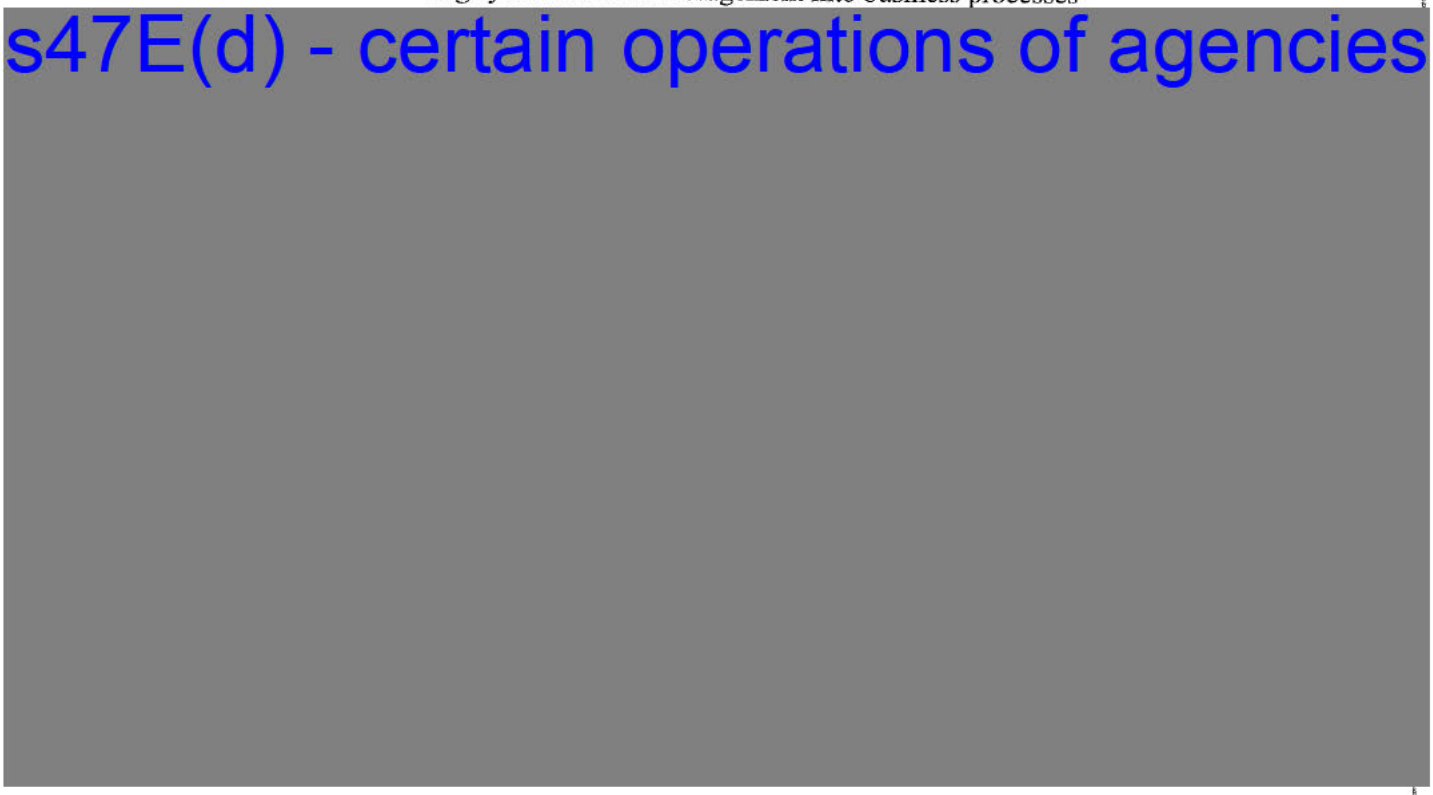
Embedding systematic risk management into business processes



Embedding systematic risk management into business processes

Embedding systematic risk management into business processes

s47E(d) - certain operations of agencies



Developing a positive risk culture

s47E(d) - certain operations of agencies

Developing a positive risk culture

Developing a positive risk culture

s47E(d) - certain operations of agencies

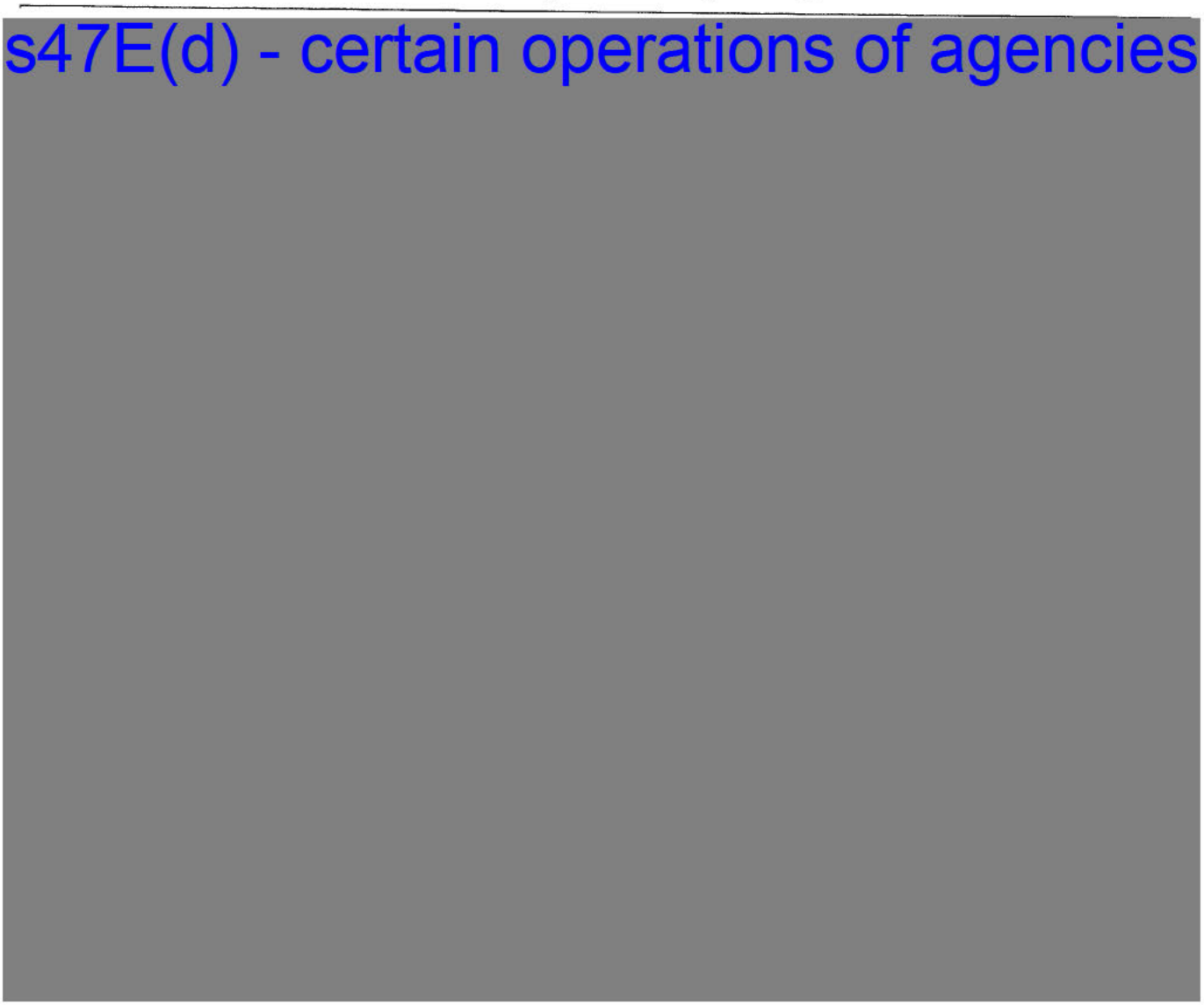
Developing a positive risk culture

s47E(d) - certain operations of agencies

Communicating and consulting about risk

s47E(d) - certain operations of agencies

Communicating and consulting about risk



Understanding and managing shared risk

s47E(d) - certain operations of agencies

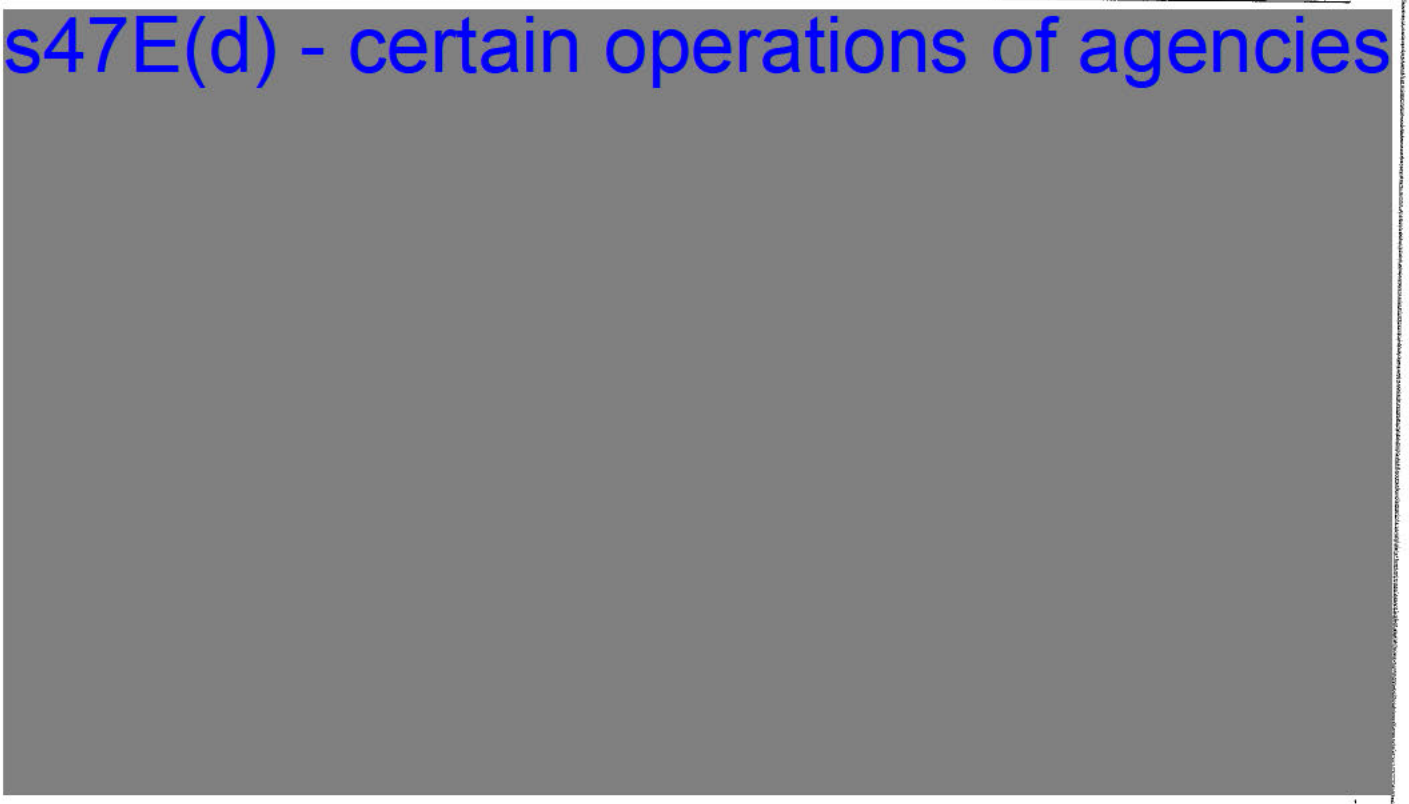
Understanding and managing shared risk

s47E(d) - certain operations of agencies

Understanding and managing shared risk

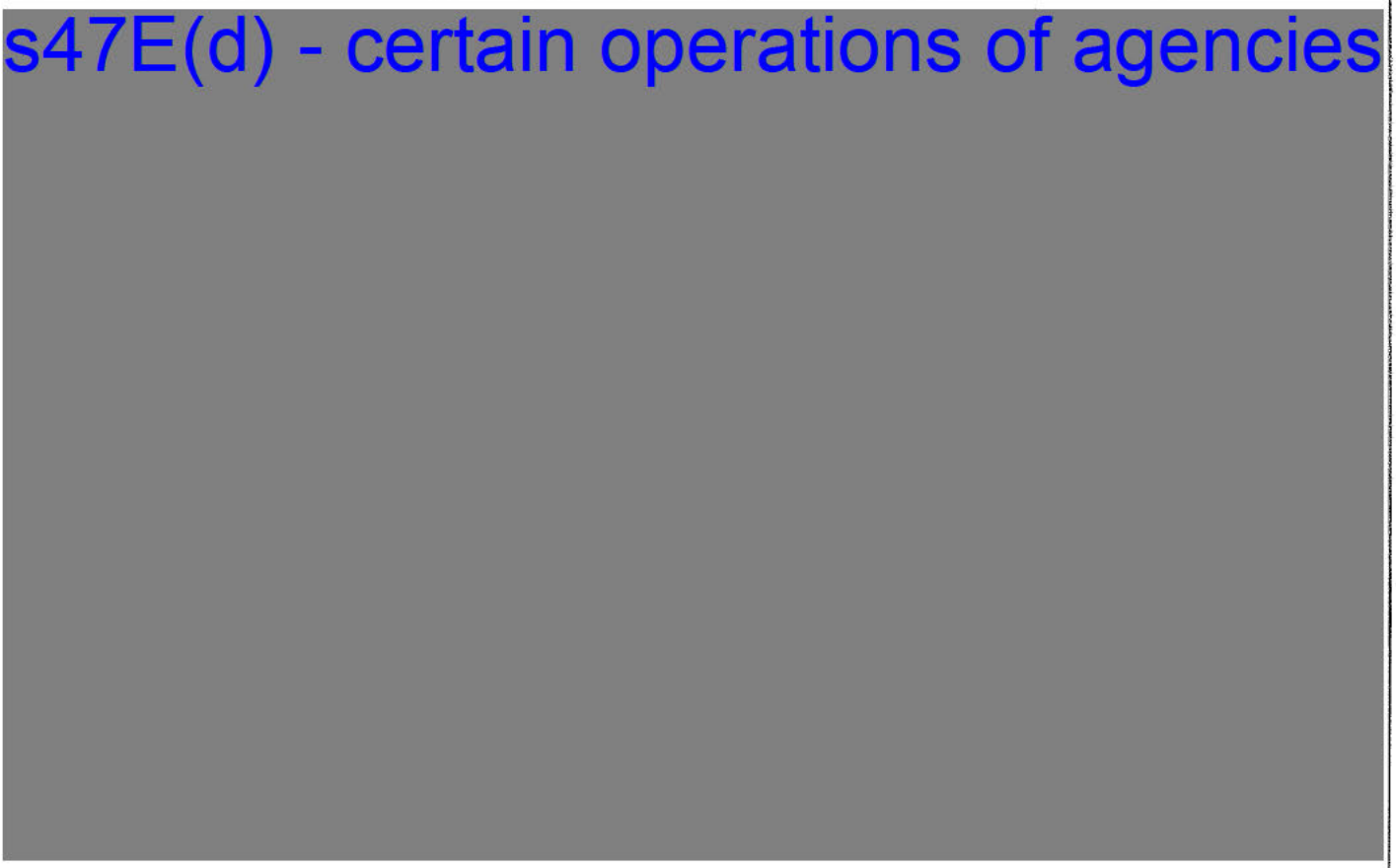
s47E(d) - certain operations of agencies

Maintaining risk management capability



Maintaining risk management capability

s47E(d) - certain operations of agencies



Maintaining risk management capability

Maintaining risk management capability

s47E(d) - certain operations of agencies

Maintaining risk management capability

Maintaining risk management capability

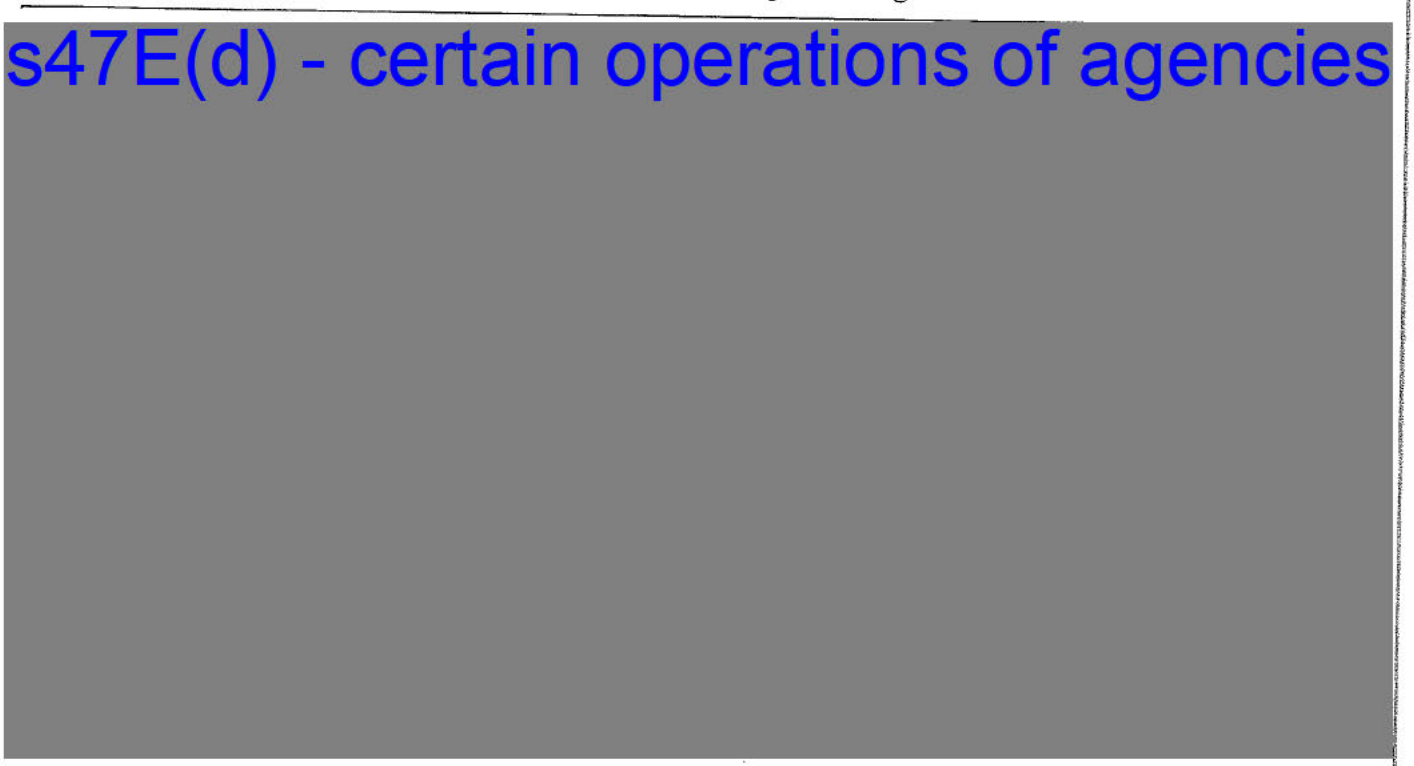
s47E(d) - certain operations of agencies

Reviewing and continuously improving the management of risk

Reviewing and continuously improving the management of risk

s47E(d) - certain operations of agencies

Reviewing and continuously improving the management of risk



Reviewing and continuously improving the management of risk

Determining Target State Maturity

Overall Target State Maturity

s47E(d) - certain operations of agencies

Determining Target State Maturity

Element Target State Maturity

s47E(d) - certain operations of agencies


s47E(d) - certain operations of agencies

Determining Target State Maturity

Segmentation and Disclosure

Communities of Practice

s47E(d) - certain operations of agencies

Segmentation and Disclosure

Disclosure

s47E(d) - certain operations of agencies

Audit, Risk & Finance Committee Charter

The Board has established an Audit, Risk and Finance Committee in compliance with section 45 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and rule 17 of the *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule).

Under rule 17 of the PGPA Rule, the Board must, by written charter, determine the functions of the committee.

1. Purpose

The Committee is a sub-committee of the Board of the National Disability Insurance Agency (Agency), and is established to assist the Board discharge its responsibilities under the *National Disability Insurance Scheme Act 2013* and the PGPA Act including by reviewing the appropriateness of the Board's financial reporting, performance reporting, risk oversight and management and internal controls, for the Agency.

2. Authority

The Board authorises the Committee, within its responsibilities, to:

a) Obtain any information it requires from any official or external contractor to the Agency (subject to any legal obligation to protect information);

b) Discuss any matters with the external auditor (ANAO), or other external parties (subject to confidentiality considerations);

c) Request the attendance of any official, including members of the Board, at Committee meetings; and

d) Obtain legal or other professional advice at Agency expense, as considered necessary to meet its responsibilities.

3. Membership

a) The Audit, Risk & Finance Committee comprises 5 Members, appointed on resolution of the Board.

b) The Board will appoint a Non-Executive Director as the Chair of the Committee and a Non-Executive Director as the Deputy Chair. The Chair and Deputy Chair must be Directors of the Board.

c) Where the Chair of the Committee is unable to attend a meeting, the Deputy Chair will preside over that meeting.

d) The Chair of the Board is entitled to attend Committee meetings, but will not be a Member of the Committee.

e) Board Directors, Chief Financial Officer, Chief Risk Officer, Scheme Actuary, Chief Information Officer, Internal Auditor and other management representatives or external advisors may attend meetings as advisers or observers, on the invitation of the Chair, but will not be Members of the Committee.

f) A representative of the ANAO will be invited to attend meetings as an observer.

g) The Members, taken collectively, will have a broad range of skills and experience relevant to the operations of the Agency and the disability sector with at least one Member of the Committee having significant accounting or related financial management experience with an understanding of accounting and auditing standards in a public sector context.

h) Members will be appointed for an initial period not exceeding 3 years. Members may be re-appointed after a formal review of their performance, for a further period not exceeding 3 years (i.e. 2 term limit).

4. Functions

The Committee is not responsible for executive management functions of the Agency and as such has no executive powers or delegations.

The Committee will engage with management in a constructive and professional manner in discharging its responsibilities and formulating its advice to the Board.

Financial Reporting

a) Assess the interim and annual financial statements and provide advice to the Board; (including recommending their signing). In particular, the committee will:
   - Assess the Agency's compliance with accounting standards, including an assessment of the appropriateness of accounting policies and disclosures;
   - Assess areas of significant judgement and financial statement balances that require estimation;
   - Assess any significant changes to accounting policies and practices, (by May of each year); and
   - Assess whether appropriate management action has been taken in response to any issues raised by the ANAO, including findings, financial statement adjustments, revised disclosures or other recommendations;

b) Provide guidance to the Agency on the types and frequency of financial information to be provided to the Board;

c) Provide guidance to the Agency on the reporting of metrics that reflect measures of operational and network efficiency;

d) Monitor the standard and relevance of financial information provided to the Board;

e) Assess the processes in place designed to ensure that financial information included in the Agency Annual Report is consistent with the signed financial statements;

f) Satisfy itself that the financial statements and notes thereto are supported by appropriate management sign-off and that the systems of internal controls and risk management are adequate;

g) Provide advice to the Board regarding the issue of the Agency annual Certificate of Compliance, or equivalent report; and

h) Discuss with the ANAO the Auditor's judgments about the quality of Agency accounting policies and processes for the preparation of the Financial Statements.

Performance Reporting

a) Satisfy itself that the Agency has a framework for managing performance and reporting it to the Board and externally that is appropriately linked to organisation objectives and outcomes;

b) Review the performance reporting framework for the selection of key performance indicators and other performance measures and metrics;

c) Advise the Board of actions that could be taken on significant matters of concern or significant opportunities for improvement that are mentioned in internal or external audit reviews and report;

d) Investigate any issues relating to Agency performance that the Committee considers warrant review or investigation, or that are referred to the Committee by the Board or other Committees of the Board; and

e) Assess the proposed reporting of Agency performance to ensure that the information is consistent with reported financial information.

Risk Oversight and Management

a) Assess whether the Agency has in place systems, policies and procedures to promote compliance with the Risk Management Rules and relevant sections of the Rules for the Scheme Actuary 2013 and provide advice to the Board regarding the sign-off of the Risk Management Declaration for annual provision to the Ministerial Council.

b) Assess whether the Agency has in place a current and sound enterprise Risk Management Framework and associated procedures for effective identification and management of Agency strategic, business, operational, project and financial risks, including fraud and corruption; and review and recommend approval of the Risk Management Framework to the Board;

c) Monitor the Agency's approach to managing the risk of fraud and corruption and review reports on fraud from the Agency that outline any significant or systemic allegations of fraud, the status of any on-going investigations and any changes to identified fraud and corruption risk across the Agency;

d) Determine whether the Agency has appropriately considered legal and compliance risks as part of its Enterprise Risk Management Plan;

e) In close consultation with the ICT Committee, consider the adequacy of the Agency's ICT risk profile and in particular, key risks associated with the ICT Programme;

f) Determine whether a sound and effective approach has been followed in establishing the Agency business continuity planning arrangements, including whether business continuity and disaster recovery plans are periodically updated and tested; and

g) Assess whether management has taken steps to embed a culture which is committed to ethical conduct and lawful behaviour.

Internal Control Environment

Internal Control Framework

a) Assess whether the Agency approach to maintaining an effective internal control environment is sound and effective;

b) Assess whether the Agency has in place comprehensive and relevant policies and procedures designed to maintain an effective internal control framework, such as policies, procedures and delegations, including over external parties such as contractors and advisers;

c) Determine whether the Agency has appropriate operating and monitoring processes in place to assess, whether key policies, procedures, laws and regulations are complied with and that policies and procedures are kept up to date;

d) In close consultation with the ICT Committee, consider the adequacy of the Agency's information technology security arrangements; and

e) Assess the adequacy of Agency compliance with relevant legislative and legal obligations, with particular reference to compulsory compliance declarations.

Internal Audit

a) Assess, update and approve the Internal Audit charter;

b) Assess the proposed internal audit coverage, ensure the coverage is aligned to Agency key risks, and assess the adequacy of internal audit resources to carry out its responsibilities;

c) Assess all audit reports and provide advice to the Board on significant issues identified in these reports and recommend action on issues raised, including

identification and dissemination of good practice;

d) Monitor Agency coordination of audit programmes conducted by internal audit and other review functions;

e) Where internal audit recommendations are accepted, monitor their implementation in terms of timeliness and outcomes;

f) Periodically assess the performance of internal audit programmes and providers; and

g) Discuss privately with the internal audit service provider at least once per year the findings of the provider and its performance in carrying out its functions.

Engagement with the ANAO

The committee will engage directly with the ANAO, as the entity's external auditor, in relation to accounting policies and practices, the preparation and content of the financial statements and the notes thereto and performance auditing. In particular, the Committee will:

a) Provide input and feedback on planned ANAO financial statement and performance audit coverage and provide feedback to ANAO on the extent and standard of services provided;

b) Monitor Agency responses to all ANAO financial statement management letters, findings and performance audit reports, including the timely and effective implementation of audit recommendations; and

c) Discuss privately with the ANAO at least once per year the findings of the ANAO and its performance in carrying out its functions

Reporting

The Committee will update the Board after each meeting on its activities and make recommendations to the Board, as appropriate.

The Chair of the Committee will report to the Board at the next Board meeting following a meeting of the Committee on any matters that the Chair considers should be brought to the attention of the Board.

The Committee will at least annually confirm to the Board that all functions/responsibilities outlined in this charter have been carried out, and comply with any other reporting requirements specified by the Board from time to time.

The Committee will provide guidance to the Board on the adequacy of Agency compliance with relevant legislative and legal obligations, with particular reference to compulsory compliance declarations (e.g. the Financial Statements and the Risk Management Declarations).

5. Administrative Arrangements

Meetings

The Committee will meet at least 4 times per year. One or more special meetings may be held to review Agency annual Financial Statements or to meet other responsibilities of the Committee.

All Members are expected to attend each meeting, in person or via tele-or-video conference on agreement with the Chair.

The Chair is required to call a meeting if asked to do so by the Board, and decide if a meeting is required if requested by any Committee Member, or by the internal auditor or the ANAO.

Planning

The Committee will develop a forward meeting schedule that includes the dates, location, and proposed agenda items for each meeting for the forthcoming year, and that covers all the responsibilities outlined in this charter, aligned to Board requirements

Quorum

A quorum will consist of a majority of Committee Members. The quorum must be in attendance at all times during the meeting.

Secretariat

Secretariat arrangements will be the same as for the Board. The Secretariat will ensure the agenda for each meeting is approved by the Chair in advance, that the agenda and supporting papers are circulated in advance of meetings where practicable to do so and at least 5 working days before a meeting; and ensure the Minutes of each meeting are prepared and maintained. Minutes must be reviewed by the Chair and circulated within 10 working days of each meeting to each Member and Observer, as appropriate.

Conflicts of interest

Members will provide written conflict of interest declarations annually to the Board declaring any material personal interests they may have in relation to their responsibilities. External members should consider past employment, consultancy arrangements and related party issues in making these declarations and the Board, in consultation with the Chair, should be satisfied that there are sufficient processes in place to manage any real or perceived conflict.

At the beginning of each meeting, Members are required to declare any material personal interests that may apply to specific matters on the meeting agenda. Where required by the Chair, the member will be excused from the meeting or from Committee consideration of the relevant agenda item(s).

The Chair is also responsible for deciding if they should excuse themselves from the meeting or from Committee consideration of the relevant agenda item(s).

Details of material personal interests declared by the Chair and other Members, and actions taken, will be appropriately recorded in the minutes.

Induction

New Members will receive relevant information and briefings on their appointment to assist them to meet their Committee responsibilities.

Performance Assessment Arrangements

The Chair will initiate a self-assessment of the performance of the Committee at least annually. The review will involve input from the Board, each Member, senior management, internal audit, the ANAO, and any other relevant stakeholders as determined by the Committee.

Review of Committee Charter

At least once a year the Committee will review this Charter for consultation with the Board.

Any changes to the Charter must be approved by the Board.

Approved

[Signature]

[Chair of the accountable authority] or Board
Date

Fraud and Risk Management

ACT Site Office

Helen McKenna (Chief Risk Officer and Branch Manager Business Assurance)

June 2014

Session Outline

- What is Risk/Risk Management?
- Why is it important?
- The Agency's approach to Risk Management
- What is your role?
- Fraud in the Commonwealth
- The Agency's approach to Fraud Control
- What is your role?

What is Risk?

National disabilityinsurance Agency

"*Risk is the effect of uncertainty on objectives*"

AS/NZS ISO31000:2009

Risk Management

National disabilityinsurance Agency

Risk Management is the process of identifying, analysing and evaluating risks with a view to ensuring the effective management of potential opportunities while reducing or avoiding adverse effects.

Why is it important?

National disabilityinsurance Agency

- To minimise the negative impact of risks upon achievement of objectives; and
- To maximise the Agency's ability to realise potential opportunities

Risk management is a proactive attempt to identify potential risks and incidents before they happen in order to develop prevention and response strategies.

- Increase the likelihood of the Agency achieving strategic and business objectives;
- Encourage a high standard of accountability at all levels of the organisation;
- Support more effective decision making through better understanding of risk exposures;
- Create an environment that enables the Agency to deliver timely services and meet performance objectives in an efficient and cost effective manner;
- Safeguard the Agency's assets – human, property and reputation; and
- Meet compliance and governance requirements.