CSIRO
csiro.au
foi@csiro.au
ABN 41 687 119 230

This document was created in response to a Freedom of Information request made to CSIRO.

FOI Number: FOI2021/17

Date: 12 March 2021

Request: Fraud-risk assessment for purposes of s10(a) of the Rule, and
Fraud/compliance audit implemented for purposes of s10(b/d) of the Rule.

Document(s): 1-6

For more information, please refer to CSIRO's FOI disclosure log at www.csiro.au/FOILog

Memorandum to the CSIRO Board Audit and Risk Committee

Meeting No: 129	29 August 2016	Agenda Item: 8.1
Subject:	2015/2016 Security and Fraud Control Report	Document 1
Author:	Security & Fraud Control / Cyber Security	
Sponsor:	s 22	
Date:	17 August 2016	
Action for BARC:	Decision ☐ Discussion ☐ Information ☒	

1. Executive Summary

s 22

CSIRO continues to adhere to its responsibilities under the Public Governance, Performance and Accountability Act 2013 (PGPA Act) in relation to effective fraud control and the implementation of mandatory requirements contained within the Protective Security Policy Framework. CSIRO Risk and Audit are currently undertaking the 2016 PSPF compliance audit, the results of which will be presented to the BARC by October 2016.

s 22

s 22

[redacted]

s 22

[redacted]

3.2 Fraud Control

s 22

[redacted]

s 22

[redacted]

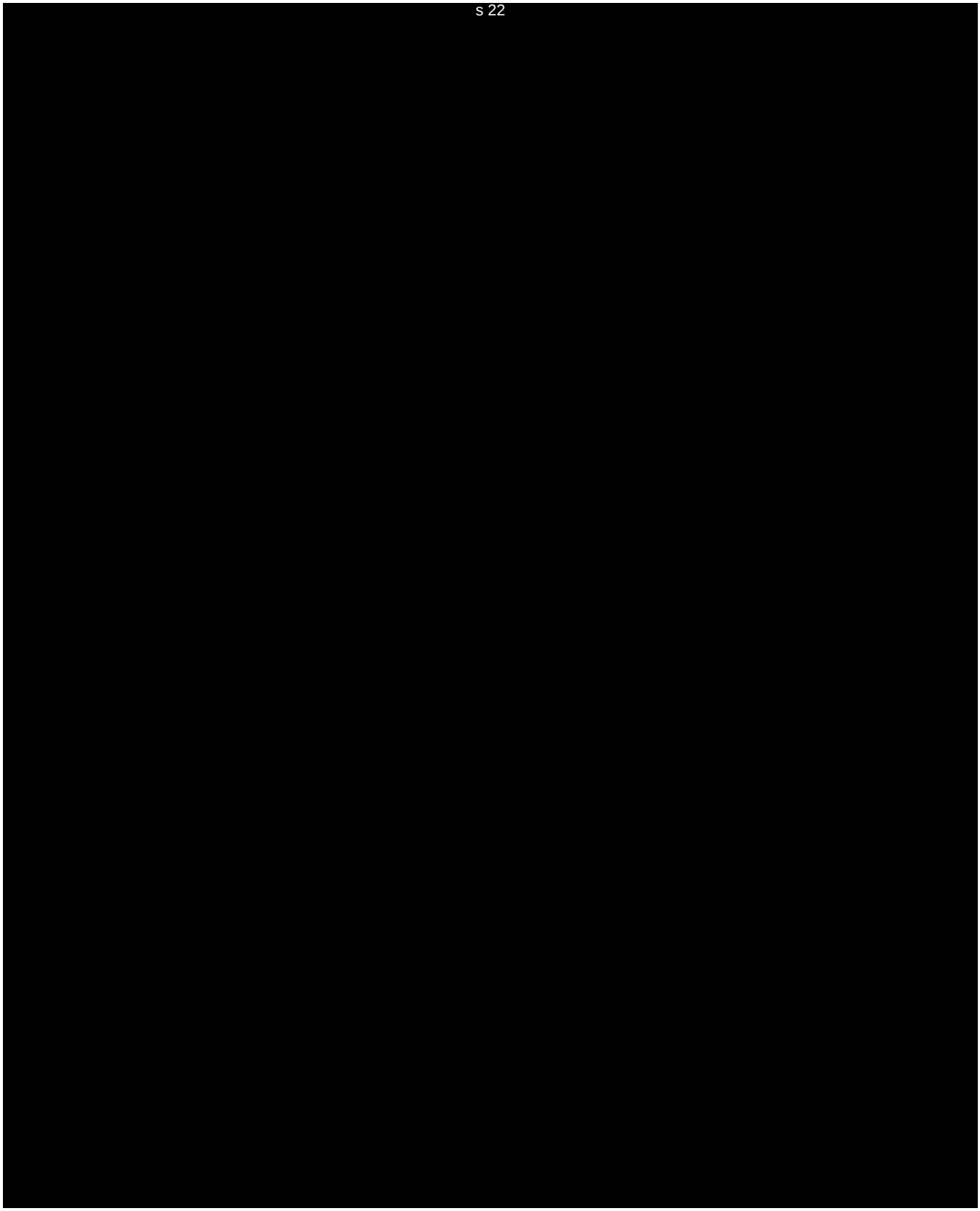
- Undertaking the CSIRO Fraud Risk Assessment (FRA) and Fraud Control Plan (FCP). Both the FRA and FCP are important elements of CSIRO's Fraud and Corruption control framework which are reviewed biennially at a minimum, or as required. The FRA was a joint collaboration between Governance (Risk) and S&FC

s 22

In line with CSIRO's annual reporting obligations under the Commonwealth Fraud Control Framework 2014, fraud incident data was collated and submitted to the Australian Institute of Criminology (AIC) in September 2015. CSIRO has complied with the PGPA Rule and Commonwealth Fraud Control Framework in FY15/16.

s 22

s 22



Memorandum to the CSIRO Board Audit and Risk Committee

Meeting No: 129	29 August 2016	Agenda Item: 8.2
Subject:	2016 Fraud Risk Assessment (FRA) and 2016 Fraud and Corruption Control Plan ('The Plan')	
Author:	s 22	Document 2
Sponsor:		
Date:	19 August 2016	
Action for BARC:	Decision ☒ Discussion ☐	Information ☐

1. Executive Summary

CSIRO seeks Board Audit and Risk Committee (BARC) endorsement of two CSIRO fraud and corruption control frameworks; the 2016 Fraud Risk Assessment (FRA) and the 2016 Fraud and Corruption Control Plan ('The Plan').

These frameworks are updated biennially consistent with the Public Governance, Performance and Accountability (PGPA) Rule and Commonwealth Fraud Control Framework 2014.

2. Background

As a Corporate Commonwealth entity (CCE), CSIRO must comply with both the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). The *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule) underpins the PGPA Act and provides the legislative basis for the Commonwealth's fraud control arrangements.

CSIRO is also bound to comply with the Commonwealth Fraud Control Framework 2014's 'Fraud Rule' which directs CSIRO to undertake regular fraud risk assessments and develop fraud control plans in line with its fraud responsibilities to prevent, detect and deal with fraud relating to our entity. The Protective Security Policy Framework (PSPF) to which CSIRO voluntarily applies ahead of the anticipated Government Policy Order (GPO), also requires CSIRO to implement the PGPA Rule.

Whilst the PGPA Rule requires these fraud frameworks to be undertaken regularly, the Commonwealth Fraud Control Framework stipulates these should be conducted at least biennially, or '*when there is a substantial change in the structure, functions or activities of the entity*'. In line with these requirements, the key considerations and impetus for updating these fraud frameworks include;

1. The 2014 FRA and 2014 Fraud Control Plan are now outdated, and
2. The organisation is undergoing a strategy realisation and investment decision outcome process in support of CSIRO's 2020 Strategy.

Type	Title	Purpose
Framework	2016 Fraud Risk Assessment (FRA)	To undertake a comprehensive organisational fraud risk evaluation, and in doing so, assess the causes, impacts and existing controls; both preventative and mitigating, for the fraud risks identified. Regular FRAs are a legislative requirement but are also essential in reviewing current and emerging risks to our business. This process supports the BARC's fraud accountabilities as an 'accountable authority' under the PGPA Act.
Framework	2016 Fraud and Corruption Control Plan ('The Plan')	The Plan works in conjunction with the FRA. It identifies organisational fraud and corruption risks, assigns risk owners, and highlights strategies for addressing these risks. This document and review process supports the BARC's role as an 'accountable authority' under the PGPA Act.

3. Summary

2016 Fraud Risk Assessment (FRA)

The 2016 FRA has identified fifteen potential fraud risks which, at any time, can manifest as a result of dishonest conduct by either internal, or external perpetrators.

CSIRO's scientific and industrial research integrity is paramount, and as such, the fraud related risks that carry the most significant inherent consequences relate directly to the conduct of our scientific research integrity. They include:

- Scientific Fraud/Research Misconduct – s 22
- Unauthorised release of classified/sensitive information (s 22
- Unauthorised practices in overseas jurisdictions s 22
- Potential for an insider threat s 22
- Unauthorised access to CSIRO's ICT, Data and Sites s 22

Other fraud risks classified as critical relate to:

- Modes of theft – credit cards, procurement, assets, cash and cash equivalents s 22
- Misrepresentation of qualification/identity s 22
- Unauthorised disclosure or theft of intellectual property s 22
- Fraudulent activity in CRC's, Joint Ventures ('JVs'), spin-off companies, or other collaborative activities (s 22
- Falsification of statutory documentation or funding submissions s 22

The 2016 FRA is provided at **Attachment 1.**

2016 Fraud and Corruption Control Plan

The Plan assigns ownership for the organisational risks identified and works in conjunction with the Fraud Risk Assessment. The plan:

- Highlights CSIRO's legislative requirements to fraud and corruption control,
- Provides the framework and strategies for the prevention, detection, investigation, reporting and response activities for addressing fraud risks and combating fraud,
- Details support mechanisms and avenues available to assist those reporting suspected, or actual, fraud and corruption matters,

- Compliments S&FC's ongoing fraud education and awareness activities, and
- Supports fraud and risk Governance, including the Fraud Risk Assessment and Fraud Control Procedure.

The 2016 Fraud and Corruption Control Plan is provided at **Attachment 2.**

s 22

[redacted]

Attachments:

Attachment 1	2016 Fraud Risk Assessment
Attachment 2	2016 Fraud and Corruption Control Plan

www.csiro.au

Fraud Risk Assessment 2016

Table of Contents

Introduction

Scope and Context

Governance (Risk) and B&IS (Security & Fraud) have undertaken the Fraud Risk Assessment 2016 in the context of CSIRO's internal and external environment, and the impact of these variables on our organisation's wider exposures to fraud. Factors which were deemed important and included in the 2016 FRA analysis, included; CSIRO Strategy 2020 and associated change management activities (and their impact to staff), past instances of fraud, security breaches, and external fraud surveys, all of which, highlight the growing risks to our organisation from fraud, bribery and corruption. CSIRO, like any large Corporate Commonwealth entity (CCE), is not immune to fraud.

Background

The Fraud Rule is the legislative framework under which CSIRO's 2016 Fraud Risk Assessment (FRA) is being undertaken. It is a mandatory fraud requirement for all Commonwealth entities and comprises a part of the Commonwealth Fraud Control Framework 2014 (which underpins the *Public Governance, Performance and Accountability Act 2013* (PGPA Act)). The PGPA Act took effect from 1 July 2014, and requires Commonwealth entities (corporate and non-corporate alike) to apply financial, operational, accountability and governance standards to the management and utilisation of public resources. From a risk perspective, section 16 of the PGPA Act assigns duties for Commonwealth entities to establish and maintain systems relating to risk and control, such as having:

> *'…an appropriate system of risk oversight and management for the entity; and…an appropriate system of internal control for the entity.'*

From a fraud perspective, section 10 of the Public Governance, Performance and Accountability Rule 2014 (Fraud/PGPA Rule) stipulates the organisation's obligations in preventing, detecting and dealing with fraud. In particular, CSIRO is tasked with:

> *'…conducting fraud risk assessments regularly and when there is a substantial change in the structure, functions or activities of the entity…' and*
>
> *'developing and implementing a fraud control plan that deals with identified risks as soon as practicable after conducting a risk assessment…'*

There is a direct linkage between CSIRO's Fraud Risk Assessment and the organisation's Fraud Control Plan (FCP), and as such, the FCP has been updated in line with the FRA in order to maintain a strong fraud framework. It is important to note that 'regularly' is defined by the Commonwealth Fraud Control Framework 2014 ('Framework') as being at least once every two years, with consideration to be given to an entity's function and operation; if these are associated with high fraud risks, or the entity operates in high fraud or corruption risk areas, assessments should be undertaken at more frequent intervals. The 2016 FRA was undertaken as the last FRA was conducted in 2014 and, as an organisational realignment is currently underway, is now outdated. CSIRO is voluntarily applying the Protective Security Policy Framework and governance requirement thirteen (GOV-13) requires agencies to comply with the Fraud/PGPA Rule, and the Commonwealth Fraud Control Policy which is deemed best practice for fraud control.

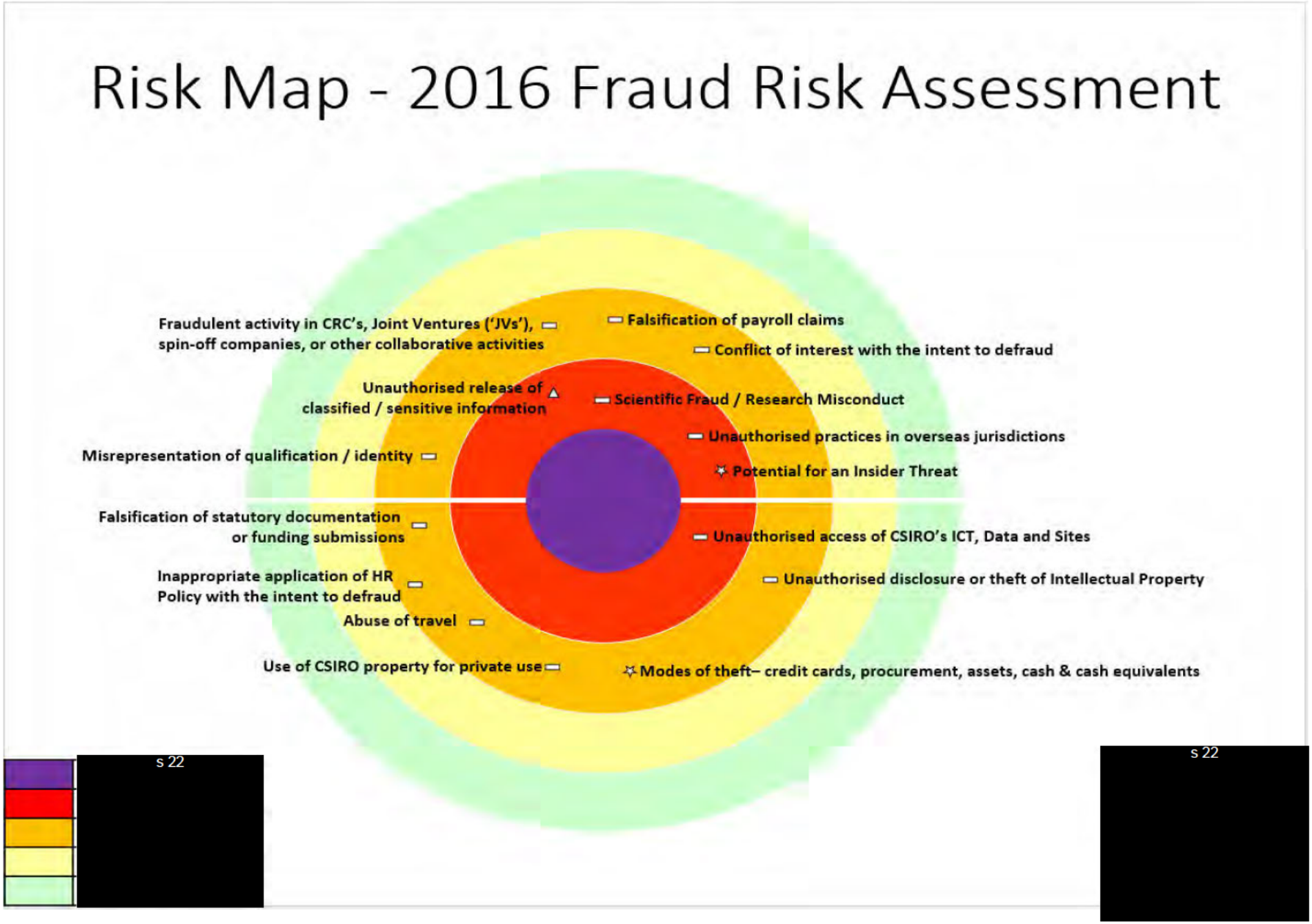
s 22

[redacted]

s 22

[redacted]

Risk Map


Risk Map - 2016 Fraud Risk Assessment
Fraudulent activity in CRC's, Joint Ventures ('JVs'), spin-off companies, or other collaborative activities
Falsification of payroll claims
Conflict of interest with the intent to defraud
Unauthorised release of classified / sensitive information
Scientific Fraud / Research Misconduct
Unauthorised practices in overseas jurisdictions
Misrepresentation of qualification / identity
Potential for an Insider Threat
Falsification of statutory documentation or funding submissions
Unauthorised access of CSIRO's ICT, Data and Sites
Inappropriate application of HR Policy with the intent to defraud
Unauthorised disclosure or theft of Intellectual Property
Abuse of travel
Use of CSIRO property for private use
Modes of theft– credit cards, procurement, assets, cash & cash equivalents
s 22
s 22

Risk Table

Risk No	Risk Title	s 22
1	Scientific Fraud / Research Misconduct	
2	Unauthorised release of classified / sensitive information	
3	Unauthorised practices in overseas jurisdictions	
4	Potential for an Insider Threat	
5	Unauthorised access of CSIRO's ICT, Data and Sites	
6	Modes of theft – credit cards, procurement, assets, cash & cash equivalents	
7	Misrepresentation of qualification / identity	
8	Unauthorised disclosure or theft of Intellectual Property	
9	Fraudulent activity in CRC's, Joint Ventures ('JVs'), spin-off companies, or other collaborative activities	
10	Falsification of statutory documentation or funding submissions	

Risk No	Risk Title	s 22
11	Inappropriate application of HR Policy with the intent to defraud	
12	Conflict of interest with the intent to defraud	
13	Abuse of Travel	
14	Use of CSIRO property for private use	
15	Falsification of payroll claims	

s 22

s 22

RISK NUMBER: 1

Scientific Fraud / Research Misconduct

s 22

s 22

s 22

2. IMPACTS	
1	Reputational damage to CSIRO in our capacity.
2	Potential future funding implications.
3	Existing partnerships, collaborations and/or ventures being affected.
4	Legal ramifications as a result of scientific fraud.
5	Breach of the Commonwealth Fraud Control Framework 2014 tenet to have an effective fraud control framework in place.
6	Publication retraction/s due to scientific falsification.
7	Increased scrutiny of CSIRO's processes and operational management.
8	Irreparable damage to CSIRO as "Australia's national science agency".
9	Negative impact to CSIRO's credibility leading to a decline in Science Quality and Health.
10	

s 22

s 22

RISK NUMBER: 2

Unauthorised release of classified / sensitive information

s 22

s 22

2. IMPACTS	
1	Potential loss of commercially valuable Intellectual Property (IP).
2	Irreparable damage to CSIRO's reputation.
3	Theft of commercial data could have serious financial implications for the organisation.
4	Breach of third party IP and information security obligations (i.e. classified documents) resulting in legal recourse being pursued.
5	Breach of the National Privacy Principles (NPP) in relation to the storage (principle 4) and protection of sensitive information (principle 10).
6	Breach of: - Protective Security Policy Framework (PSPF) - *Crimes Act* - PGPA Act - *Criminal Code Act 1995,* which may result in legal recourse.
7	Industry partners and collaborators experiencing a loss of trust in CSIRO.
8	
9	

s 22

s 22

s 22

RISK NUMBER: 3

Unauthorised practices in overseas jurisdictions

s 22

s 22

s 22

[redacted]

s 22

[redacted]

RISK NUMBER: 4

Potential for an Insider Threat

s 22

[redacted]

s 22

[redacted]

2. IMPACTS	
1	Damage to CSIRO's brand and reputation.
2	Potential to undermine CSIRO's operations, management and strategic aspirations.
3	Potential loss of visibility around commercial assets (i.e. IP) and future commercial value of emerging IP with staff taking IP with them when they leave.
4	Failure to adequately respond to staff feedback resulting in staff pursuing external avenues in an attempt to "be heard", such as unauthorised disclosures to the media.
5	Security breaches, theft of intellectual property, and financial losses.
6	Increased likelihood and consequence of fraud risks; - Risk 5 (Unauthorised access of CSIRO ICT, Data and Sites), - Risk 8 (Unauthorised disclosure or theft of Intellectual Property), - Risk 15 (Falsification of payroll claims), - Risk 2 (Unauthorised release of classified / sensitive information), - Risk 6 (Modes of theft – credit cards, procurement, assets, cash and cash equivalents), and - Risk 12 (Conflict of interest with the intent to defraud).
7	Perceived "unpleasant" culture and/or environment as a result of fraudulent conduct impacting upon CSIRO's ability to attract, and retain, talented staff.
8	Inappropriate storage and/or data protection policies resulting in data losses, and staff departures resulting in data sets being lost or stolen.
9	Failure to identify and properly manage potentially malicious conduct leading to an unethical organisational culture.
10	

[redacted]

s 22

[redacted]

s 22

RISK NUMBER: 5

Unauthorised access of CSIRO's ICT, Data and Sites

s 22

s 22

	2. IMPACTS
1	Loss of sensitive information with consequential loss of intellectual property (IP) and potential for commercialisation.
2	Irreparable damage to CSIRO's reputation.
3	Damage, theft or loss of CSIRO resources; property, plant or equipment.
4	Loss of data; breach of principle 4 of the National Privacy Principles (NPP).
5	Loss of capability to deliver impact science objectives.
6	Breaching the tenets of the PSPF and ISM.
7	Potential for data compromise – data being changed and its resulting impact (i.e. false data, results).
8	Degradation of our system performance, including personal use of CSIRO ICT.
9	
10	

[redacted]

s 22

[redacted]

s 22

[redacted]

RISK NUMBER: 6

Modes of theft – credit cards, procurement, assets, cash & cash equivalents

s 22

[redacted]

s 22

[redacted]

2. IMPACTS	
1	Damages the reputation of CSIRO.
2	Value for money not obtained - breach of the Commonwealth Procurement Rules (CPRs).
3	Waste and/or abuse of public resources – breach of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) with potential fines enforced.
4	Inappropriate approvals obtained - breach of internal CSIRO controls (i.e. Delegations and Authorities Manual).
5	Redirection of resources (i.e. time and money) to investigate, prosecute and recover misappropriated funds.
6	Involvement of enforcement agencies (i.e. AFP and CDPP) for serious and/or complex misconduct.
7	Significant financial losses for the organisation.
8	Change to operations and/or processes - the implementation of new or additional internal controls to prevent future occurrences.
9	Breach of the Commonwealth Fraud Control Framework 2014 - Government expectations in relation to effective fraud control for agencies and their officials.
10	Parliamentary scrutiny in CSIRO's operations and management.

[redacted]

s 22 [redacted]

s 22 [redacted]

RISK NUMBER: 7

Misrepresentation of qualification / identity

s 22 [redacted]

s 22 [redacted]

2. IMPACTS	
1	Unqualified applicants selected for positions resulting in both a financial and resource (i.e. time) loss to the organisation - contravening the principles of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).
2	Breach of the Protective Security Policy Framework (PSPF) if information or security principles are violated.
3	The appointment of a dishonest employee could have serious financial and information security implications.
4	CSIRO could face reputational, civil and criminal repercussions from the appointment of an unqualified, and/or unexperienced employee.
5	Project deliverable delays.
6	Additional recruitment or re-training costs.
7	Potential for unauthorised release of classified/sensitive information (link to risk 2).
8	Significant reputational harm for the organisation.
9	Potential media scrutiny.
10	

s 22 [redacted]

s 22 [redacted]

s 22

[redacted]

s 22

RISK NUMBER: 8

Unauthorised disclosure or theft of Intellectual Property

s 22

[redacted]

s 22

	2. IMPACTS
1	CSIRO's valuable intellectual property (IP) being lost affecting CSIRO's ability to commercialise concepts and deliver impact back to industry partners, Government, and/or the wider Australian community.
2	Damage to CSIRO's reputation.
3	Poor client relationships as a result of unauthorised disclosures/IP theft.
4	Potential legal liability for breach of contract.
5	Reduced client confidence in CSIRO and our ability to "deliver impact".
6	Inability to deliver strategic goals in a particular science area.
7	A reluctance to engage with other external collaborators in the future due to previous breaches of trust arising from corporate espionage.
8	
9	
10	

s 22

[redacted]

s 22

[redacted]

s 22

RISK NUMBER: 9

Fraudulent activity in CRC'S, Joint Ventures ('JVs'), spin-off companies, or other collaborative activities

s 22

[redacted]

s 22

[redacted]

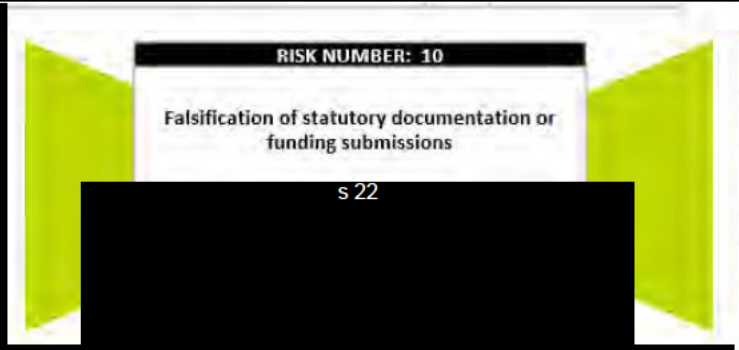
2. IMPACTS	
1	Financial consequences resulting from policy breaches (i.e. domestic and international bribery and corruption contraventions).
2	Intellectual Property (IP) loss to the organisation, some of which, the worth is incalculable.
3	Damage to CSIRO's reputation and status as 'Australia's Innovation Catalyst'.
4	Damage to collaborative partnerships, Government, and/or industry.
5	Incalculable damage to the Cooperative Research Centre (CRC) Programme resulting in reduced confidence in CSIRO from our Minister.
6	CSIRO's ability to achieve its strategic aspirations being significantly impeded.
7	
8	
9	
10	

[redacted]

s 22

[redacted]

s 22



	2. IMPACTS
1	Financial consequences – third parties or industry bodies resorting to administrative remedies for recompense.
2	Financial implications - loss of future funding as a result of falsification, fabrication, or unethical conduct.
3	The Australian Government, or other funding bodies, reducing support for CSIRO on an account of internal mismanagement.
4	Significant and irreparable reputational damage.
5	Damage to long-held partnerships and relationships.
6	Dishonestly gaining a benefit or an advantage - breach of the Commonwealth Fraud Control Framework 2014.
7	
8	
9	
10	

s 22

[redacted]

s 22

[redacted]

s 22

[redacted]

RISK NUMBER: 11

Inappropriate application of HR Policy with the intent to defraud

s 22

[redacted]

1	Incressed risk of fraudulent activities as a result of collusion or protection.
2	Significant reputational damage to CSIRO.
3	Dishonest practices becoming increasingly difficult to detect within CSIRO.
4	In-perpetuity benefits (financial or otherwise) resulting from inappropriate appointment and/or promotion.
5	Unsuitable promotions and role appointments adversely affecting efficiency and productivity within the organisation.
6	In breach of the tenets of the Protective Security Policy Framework (PSPF) in relation to agencies carrying out their responsibilities to combat fraud.
7	Perception of inconsistent application of rewards criteria can lead to staff leaving the organisation.
8	Leadership pipelines not correctly reflecting CSIRO capability which can impact on our ability to deliver on our commitments, fulfil our organisational strategy aspirations, and demonstrate real impact.
9	Unfair dismissals and/or disputes over entitlements resulting in external party involvement; Fair Work commission, Unions, and the Public Sector Commission.
10	Scrutiny from the media and Government.

[redacted]

s 22

[redacted]

s 22

RISK NUMBER: 12

Conflict of interest with the intent to defraud

s 22

[redacted]

	2. IMPACTS
1	Undermined public and political confidence in the organisation's integrity.
2	Engaging the wrong suppliers and/or contractors.
3	Not achieving true value for money – breach of the Commonwealth Procurement Rules (CPRs).
4	Regulatory penalties for breach of fiduciary and conflict of interest obligations under the PGPA Act.
5	Significant financial losses as a result of imposed penalties/fines (i.e. breach of anti-bribery and corruption laws).
6	Reduction in future funding support from key Government and industry players.
7	Financial losses (some of which may be incalculable) as a result of the dishonest conduct.
8	Dishonest staff within the organisation posing great risks to its reputational, economic, and social viability.
9	Appointing unsuitable applicants as a result of conflicting interests, adversely affecting efficiency and productivity within the organisation (link to risk 11).
10	A perceived 'toxic culture' – affecting our ability to attract and retain talented staff.

[redacted]

s 22

[redacted]

s 22

RISK NUMBER: 13

Abuse of Travel

s 22

[redacted]

2. IMPACTS	
1	Deficit program budgets as a result of inflated or unnecessary travel.
2	Parliamentary scrutiny in CSIRO's operations and management.
3	Reputational damage to the organisation.
4	Waste and/or abuse of public resources – breach of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).
5	Failure to achieve value for money; breach of the Commonwealth Procurement Rules (CPRs).
6	Not adhering to the Whole of Australian Government (WoAG) travel arrangements – subject to Department of Finance enforcement.
7	Damage to future collaborative partnerships.
8	Breach of the Commonwealth Fraud Control Framework 2014 - Government expectations in relation to effective fraud control for agencies and their officials.
9	

[redacted]

s 22

[redacted]

s 22

RISK NUMBER: 14

Use of CSIRO property for private use

s 22

[redacted]

2. IMPACTS	
1	Injury or harm from utilising CSIRO resources offsite (to staff member or third party).
2	Financial loss to the organisation.
3	Reputational damage from inappropriate use of CSIRO resources.
4	Reputational damage resulting from a staff member, or third party, sustaining an injury whilst utilising CSIRO resources offsite for non-work purposes.
5	Gaining a personal benefit by deceit.
6	Potential for physical harm and environmental damage resulting from inappropriate use and disposal of chemical, biological and radiological assets.
7	
8	
9	
10	

[redacted]

s 22

s 22

s 22

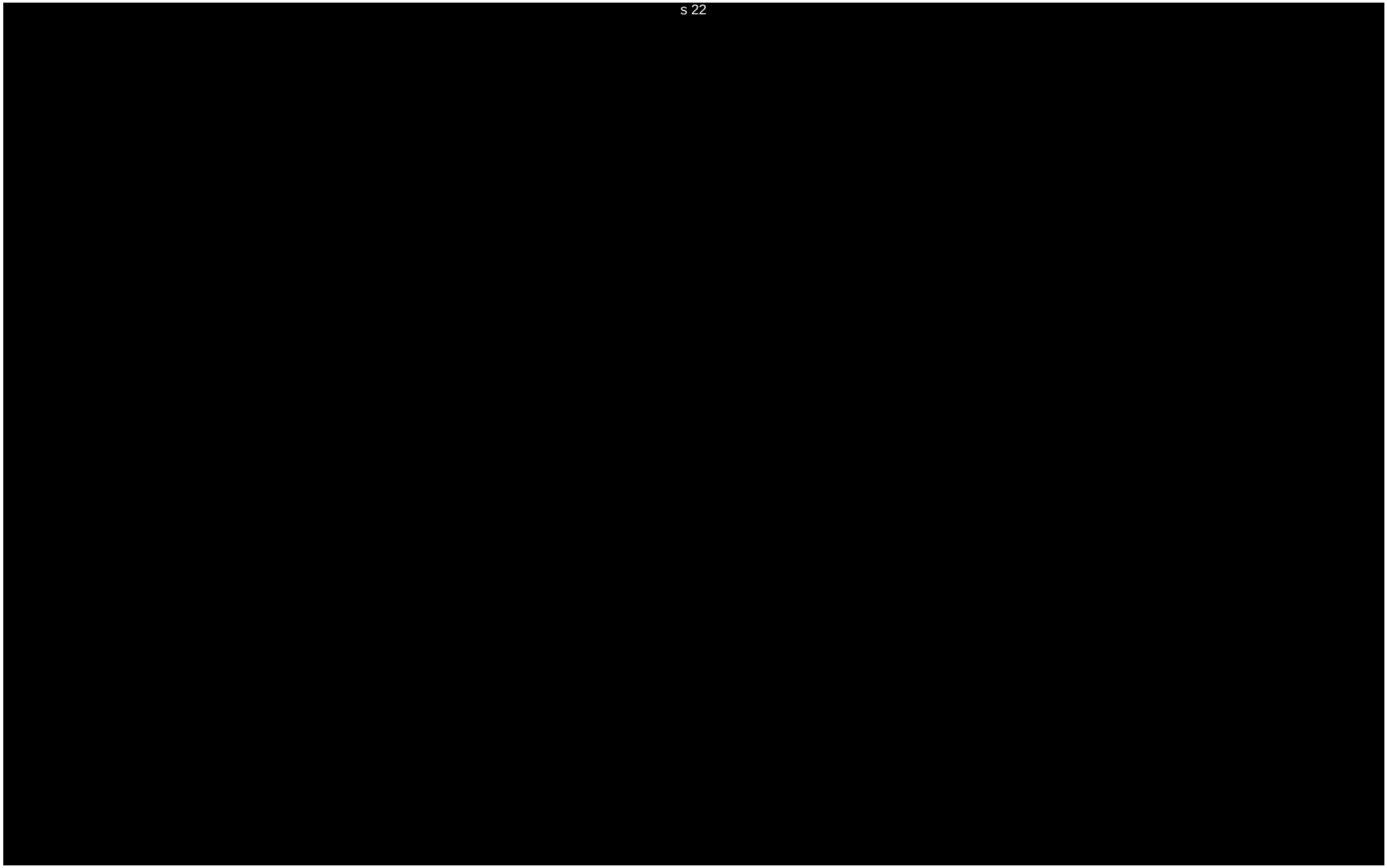
RISK NUMBER: 15

Falsification of payroll claims

s 22

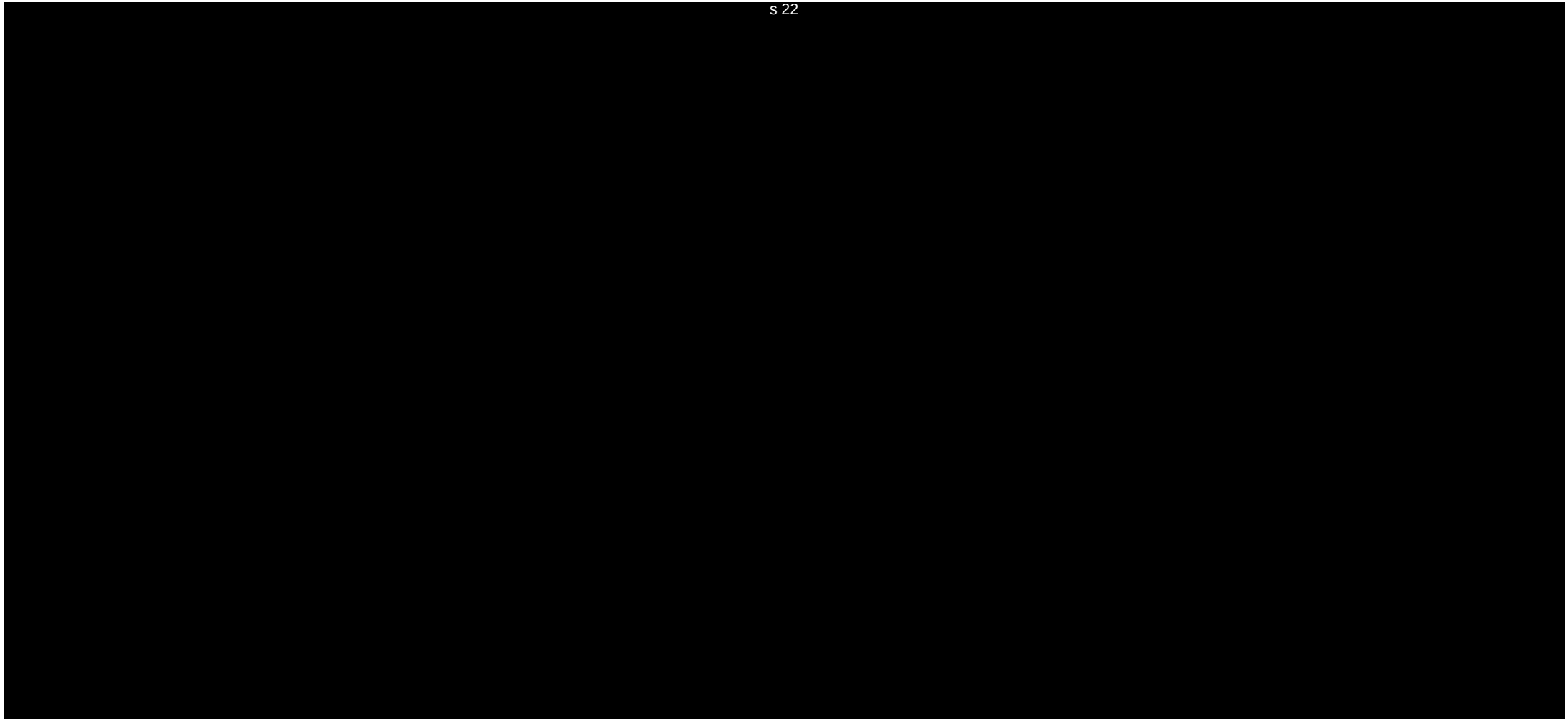
s 22

s 22



s 22

s 22



Appendix B - 2016 Fraud and Corruption Control Plan ('The Plan')

The organisational Fraud and Corruption Control Plan ('The Plan') formerly known as the Fraud Control Plan was reviewed and updated in conjunction with the 2016 Fraud Risk Assessment (FRA). The Plan continues to be maintained by the CSIRO Agency Security Advisor (ASA)/Fraud Control Manager, and will be submitted to the Board Audit and Risk Committee (BARC) along with the FRA. At present, the Plan and FRA are undertaken on a biennial basis in line with the Commonwealth Fraud Control Framework's Fraud Rule.

The Plan declares CSIRO's commitment to fraud and corruption prevention, detection, investigation, response and recovery, highlights the organisation's fraud responsibilities, supports the Security & Fraud Control team's fraud awareness and education agenda, and discusses the fraud risks and strategies in place to prevent and mitigate their effects, aided by the inclusion of the FRA results.

The Plan details:

1. **CSIRO's Fraud Control Framework** (Code of Conduct, 2015-2016 Fraud Control Strategy, Security & Fraud Two Year Plan, 2016 FRA, Fraud and Corruption Control Plan and Fraud Control Procedure)
2. **CSIRO Governance** (legislative framework and assurance roles and responsibilities)
3. **CSIRO's Operational Context** (operations, structure and staff demographics)
4. **Fraud and Corruption Prevention Strategies** (CSIRO Procedure, Pre-employment screening practices, cessation procedures, fraud awareness training and agenda, and other internal controls)
5. **Fraud and Corruption Detection** (Code of Conduct responsibilities, avenues to report fraud allegations, Public Interest Disclosure Scheme (P.I.D.), fraud projects, leave deeming, early warning indicators, the roles of internal and external audit and fraud control officers, and financial management and compliance programs)
6. **Fraud and Corruption Response** (investigation procedures, escalation to law enforcement agencies, disciplinary procedures, funds recovery process and post-incident review process)
7. **Fraud Control Reporting Requirements** (internal and external reporting requirements) and
8. **2016 Fraud Risk Assessment (FRA) Results*** (including likelihood, consequence and management action table).

It is a fluid document, subject to review and evaluation in order to remain consistent with Government policy, and remain an effective part of CSIRO's existing assurance and accountability framework.

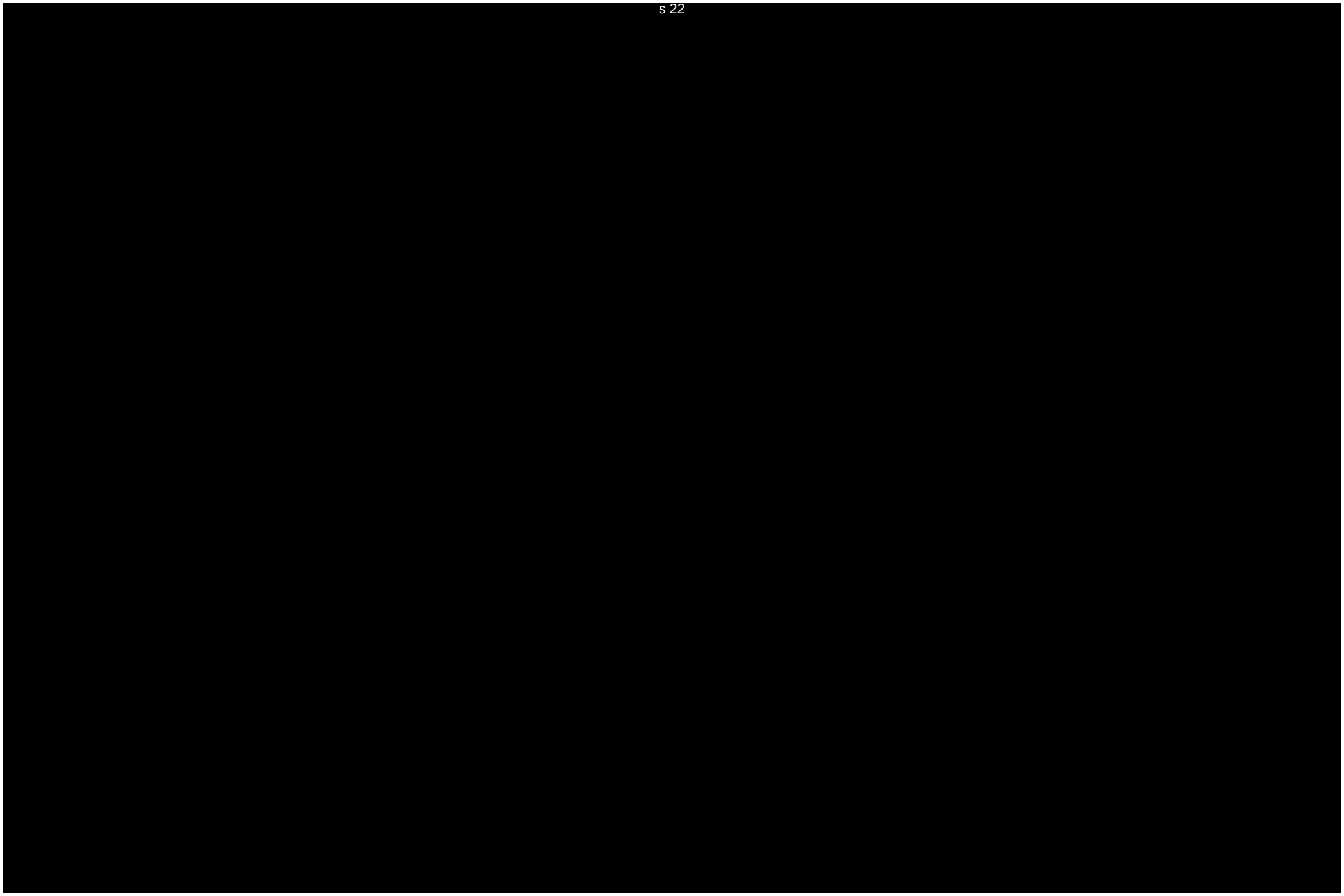
The Australian Standards Fraud and Corruption Control (AS 8001 – 2008), *Public Governance, Performance and Accountability Act 2013* (PGPA Act), Commonwealth Fraud Control Framework 2014 ('Framework'), Australian National Audit Office's (ANAO) 'Fraud Control in Australian Government Entities' and CSIRO policy, were all consulted in the development of the 2016 Fraud and Corruption Control Plan.

* Sensitive/privileged information omitted.

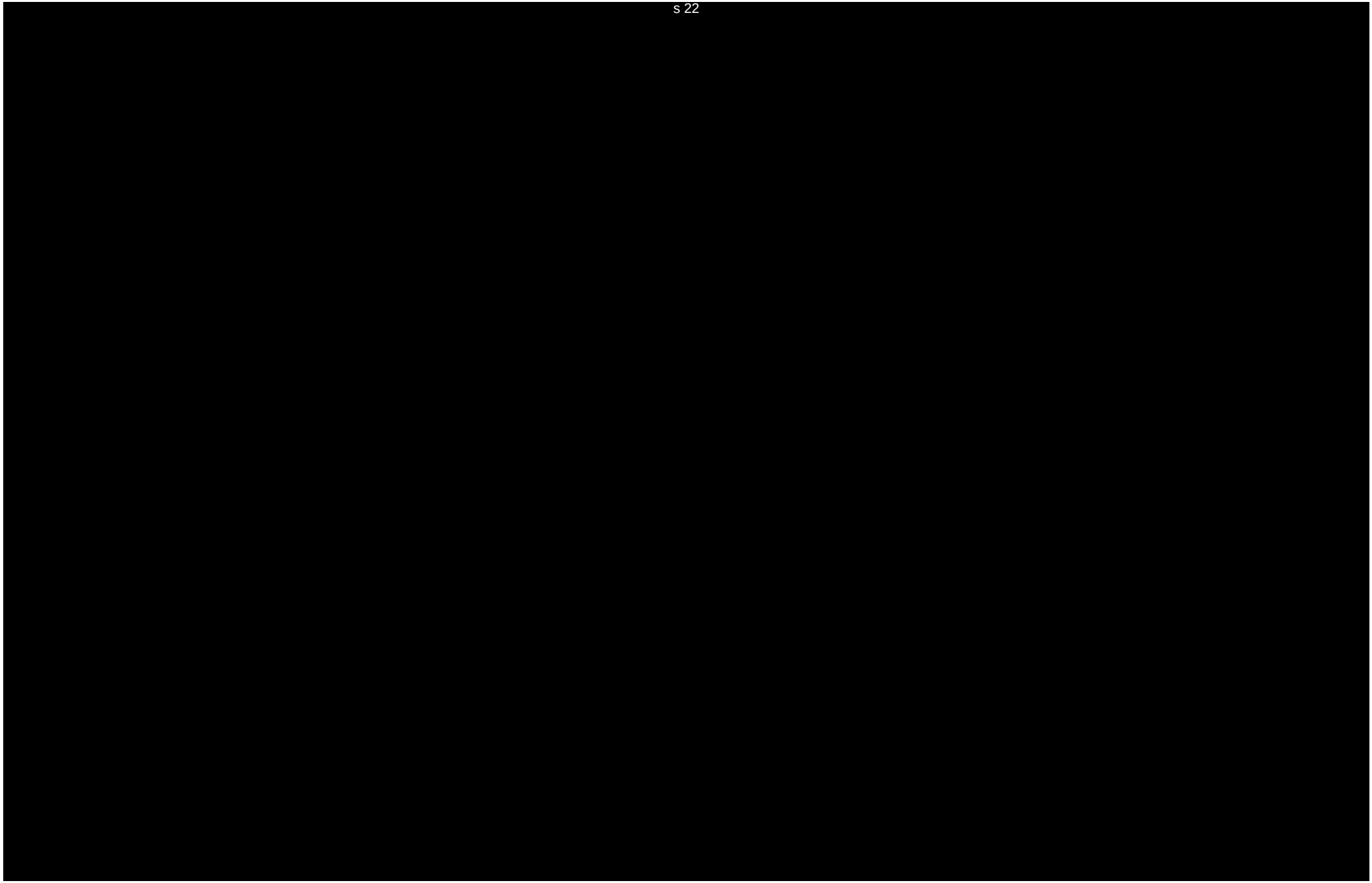
Appendix C - 2016 Fraud Risk Assessment Participant List

Name	Job Title
s 22	

s 22



s 22



CSIRO BUSINESS & INFRASTRUCTURE SERVICES
www.csiro.au

2016
Fraud and Corruption Control Plan

('The Plan')

Table of Contents

* Sensitive/Privileged information omitted. Detail available in the 2016 Fraud Risk Assessment.


s 22

2 INTRODUCTION

2.1 Foreword by the Chief Finance Officer

CSIRO'S COMMITMENT TO FRAUD AND CORRUPTION CONTROL

The Commonwealth Scientific and Industrial Research Organisation (herein referred to as CSIRO), has a **zero tolerance** fraud and corruption policy. The Commonwealth Fraud Control Framework 2014, to which CSIRO adheres as a Corporate Commonwealth entity, defines fraud as '*dishonestly obtaining a benefit, or causing a loss, by deception or other means*'. Corrupt conduct can be defined as the misuse of power for personal benefit and may, or may not, comprise elements of fraud.

Fraud and corruption are very serious matters and have far reaching consequences. As Australia's national science agency, the most damaging effect for CSIRO is that it reduces funding available for science. CSIRO is committed to the prevention, detection, reporting, and investigation of dishonest conduct affecting our organisation. We will also take all reasonable measures to recover financial losses to CSIRO caused by illegal activity.

Fraud against CSIRO is fraud against the Commonwealth, and can be prosecuted under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), *Crimes Act 1914*, and *Criminal Code Act 1995*. Corrupt conduct and Fraud are both breaches of CSIRO's Code of Conduct and may result in a termination of employment or other disciplinary action.

CSIRO will investigate all reported incidents of alleged fraud, and corrupt conduct comprising fraud, and any disclosures made under CSIRO's Public Interest Disclosure (PID) Scheme will be protected in line with this policy.

All staff members and CSIRO affiliates have a responsibility to understand what constitutes fraud and corrupt conduct, and a duty to report suspected fraud and corrupt conduct to their Line or Senior Management, or to CSIRO's Fraud Control Manager. In accordance with CSIRO's Code of Conduct, all staff members and CSIRO affiliates are expected to act ethically and with integrity in the course of their duties.

I encourage all staff members and CSIRO affiliates to familiarise themselves with the Fraud Control intranet page, to understand how we all play a part in maintaining CSIRO's ethical culture.

Sincerely,

s 22

Date:

Chief Finance Officer

2.2 Executive Summary

The Fraud and Corruption Control Plan ('The Plan') forms a crucial part of CSIRO's Fraud and Corruption Control Governance. The Plan's intent is to document all fraud and corruption control strategies (prevention, detection and response) and assign ownership for these activities. The Plan is developed by the Security & Fraud Control (S&FC) team, and is maintained by CSIRO's Agency Security Advisor and Fraud Control Manager.

In line with the Public Governance, Performance and Accountability Act 2013 (PGPA Act) and underpinning Commonwealth Fraud Control Framework 2014 ('Framework'), the Plan is required to be undertaken at least every two years*, and as soon as practicable after conducting the organisation's Fraud Risk Assessment (FRA). Both the FRA and Plan are submitted to the Board Audit and Risk Committee (BARC) for endorsement.

The purpose of the Plan is to:

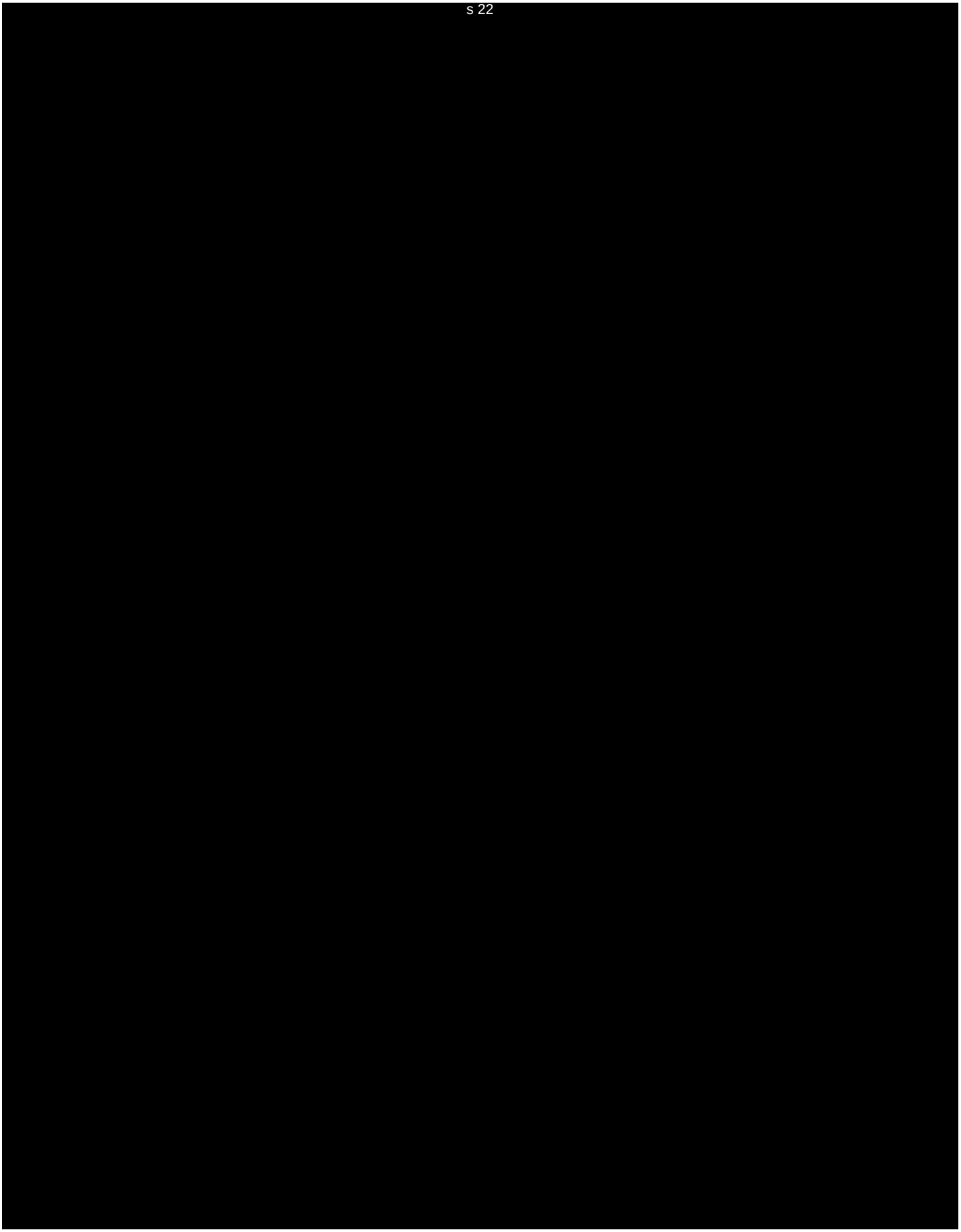
- Identify existing organisational fraud and corruption risks, and highlight strategies for addressing these risks,
- Declare CSIRO's commitment to fraud and corruption control,
- Provide a framework for the organisation's fraud prevention, detection, investigation, reporting and response activities,
- Detail support mechanisms and avenues available to assist those reporting suspected, or actual, fraud and corruption matters,
- Highlight CSIRO's legislative requirements to fraud and corruption control (including external escalation and reporting obligations),
- Support its regular review which is mandated at least on a biennial basis,
- Complement S&FC's ongoing fraud education and awareness activities, and
- Support fraud and risk Governance, such as the organisation's Fraud Risk Assessment.

The following guidance has been consulted in the development of this Fraud and Corruption Control Plan:

- Australian Standards Fraud and Corruption Control (AS 8001 – 2008)
- PGPA Act
- Framework
- Australian National Audit Office's (ANAO) 'Fraud Control in Australian Government Entities' and
- CSIRO policy.

* Or as a result of a substantial change to the organisation

s 22



s 22

[redacted]

3.4 2016 Fraud Risk Assessment (FRA)

The 2016 FRA has been jointly undertaken by B&IS (Security & Fraud) and Governance (Risk) to identify and evaluate potential organisational fraud and corruption risks. The FRA is a comprehensive process in which key organisational stakeholders are consulted, external fraud and corruption findings are reviewed, CSIRO policy is assessed, and findings are submitted to the BARC for endorsement. Inherent risk ratings (IRRs) are allocated for all identified organisational fraud risks in the form of 'risk bow-ties' (considering the likelihood and consequence of the fraud risks occurring), and after existing preventative and mitigating controls have been applied and assessed, all risks are then assigned residual risk ratings (RRRs). Fifteen organisational fraud risks have been identified through the 2016 FRA (including the amalgamation of a few existing risks). Both the FRA and Plan are consistent with the AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines, and the Australian Standard AS 8001-2008 Fraud and Corruption Control. The top five fraud risks (based on IRRs) have been highlighted below, with further detail provided in section 10.

1. **Risk 1:** **Scientific Fraud / Research Misconduct** [redacted]

[redacted]

[redacted] **Risk 2:** **Unauthorised release of classified/sensitive information** [redacted]

[redacted]

[redacted]

3. **Risk 3:** **Unauthorised practices in overseas jurisdictions** [redacted]

[redacted]

4. **Risk 4:** **Potential for an Insider Threat** [redacted]

[redacted]

[redacted]

5. **Risk 5:** **Unauthorised access of CSIRO's ICT, Data and Sites (** [redacted]

[redacted]

[redacted]

4 GOVERNANCE

4.1 Legislative Framework

The *Commonwealth Authorities and Companies Act 1997* (CAC Act) was replaced as the primary financial legislation for the Commonwealth on 1 July, 2014. CSIRO, a Corporate Commonwealth entity (CCE) under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), must adhere to the Fraud Rule, which is a tenet of the Commonwealth Fraud Control Framework 2014 ('Framework'). The Framework requires CSIRO to complete regular Fraud Risk Assessments and Fraud Control Plans.

CSIRO is an Australian Government Corporate entity, constituted and operating under the *Science and Industry Research Act 1949* (SIR Act). Section 22 of the PGPA Act allows the Finance Minister to issue government policy orders* to CSIRO in relation to Australian Government policy.

* A government policy order is a legislative instrument under the *Legislative Instruments Act 2003* (section 42 'disallowance' does not apply).

CSIRO's Governance structure is as follows:

- CSIRO Board – all Board members (other than Chief Executive) are appointed by the Governor-General
- Chief Executive Officer – appointed by the Board
- Executive Team – comprising a Deputy Chief Executive, Science Group Executives and the Chief Finance Officer. This team is supported by the Science, Strategy, Investment and Impact Committee, Major Transactions Committee, and other Governance and Management Committees.
- CSIRO Leadership Team – comprising Business Unit Directors and Enterprise group General Managers.
- Delegated authorities – Authorised Delegates (i.e. Line and Senior Management, Project Leaders, and Delegations by Policy Area and Authority Ranking).

4.2 Assurance and Accountability Roles and Responsibilities

CSIRO BOARD	**The CSIRO Board have:** o Legislative obligations under the PGPA Act as CSIRO's accountable authority o A responsibility for endorsing all internal audit activity o A responsibility to the Australian Government for CSIRO policy, direction, development, performance and assurance – as per the Board Charter o Core fraud control and corruption accountabilities.
CHIEF EXECUTIVE OFFICER (CEO)	**Accountable for:** o CSIRO's fraud control program, activities, governance, and legislative obligations o Acting in consultation with the Board in determining and implementing CSIRO policy, direction, and assurance framework.
EXECUTIVE TEAM	**Accountable for:** o Demonstrating CSIRO's fraud control and corruption commitment o Ensuring a coordinated fraud control and corruption approach is adopted o Overseeing and endorsing appropriate fraud control and corruption strategies o Taking ownership of the Fraud Control Plan and Fraud Risk Assessment o Ensuring that current (and new) organisational strategies and programs are appropriately fraud risk assessed, and that adequate fraud controls are incorporated where necessary.
BOARD AUDIT & RISK COMMITTEE (BARC)	**Accountable for:** o Assisting the Board in matters pertaining to financial and risk management, internal control, and legislative compliance o Annually reviewing the Internal Audit Charter o Having oversight on the implementation of the organisation's Fraud Control Plan and ensuring that regular Fraud Risk Assessments are undertaken.

EXECUTIVE MANAGER, AUDIT	**Manages the Internal Audit team, who:** o Have a core responsibility to ensure the adequacy and reliability of internal controls o Assists in assessing the organisation's performance in achieving its objectives o Undertake key assurance and advisory functions within the organisation, i.e. compliance with legislative and organisational policy requirements **Accountable to:** o The CSIRO Board for the management of the Internal Audit team.
EXECUTIVE MANAGER, RISK	**Responsible for:** o Undertaking risk assessments of organisational processes, strategies and initiatives, and in the identification and management of the key risks identified o Assisting in the coordination of the organisational Fraud Risk Assessment, and in obtaining BARC endorsement o Working in consultation with the CSIRO Board and Executive Team to develop the Risk Plan, Profile, Framework and Risk Management Process.
AGENCY SECURITY ADVISOR & FRAUD CONTROL MANAGER	**Responsible for:** o Assisting in the coordination of the organisational Fraud Risk Assessment o Responsible for the development, review, application and promotion of CSIRO's fraud control and corruption framework, in line with mandated fraud legislation, policy and Government directives o Being a central point of contact for all fraud related matters o Coordinating fraud investigations (including preliminary fraud investigations) into suspected fraud matters o Reporting to the CEO on fraud control in their capacity as a fraud control delegate within the organisation.
CSIRO FRAUD CONTROL OFFICER	**Assists the Fraud Control Manager by:** o Ensuring that CSIRO adheres to mandatory fraud requirements; prevention, detection, response, reporting, investigation and recovery o Developing, reviewing, applying and promoting CSIRO's fraud control framework in line with fraud legislation, policy and Government directives **Responsible for:** o Ensuring that CSIRO's Fraud Risk Assessment and Fraud Control Plan are periodically undertaken o Maintaining a strong fraud control awareness agenda within CSIRO o The formation of strategic fraud control activities o External fraud control requirements, i.e. Australian Institute of Criminology (AIC) annual fraud survey o Staying abreast of current and emerging fraud trends and identifying linkages (i.e. fraud and corruption synergies, for example) o Assisting in suspected fraud and corruption investigations.
LINE MANAGEMENT AND SUPERVISORS	**Responsible for:** o Demonstrating a commitment to CSIRO's fraud control and corruption efforts o Promoting a culture of ethical behaviour o Managing fraud and corruption risks within responsibility areas o The proper use of delegated authorities, and position o Promptly escalating fraud matters to the Fraud Control Manager o Being vigilant to potential fraud warning signs ('red flags').

STAFF MEMBERS AND CSIRO AFFILIATES	**Required to:** ○ Adhere to the CSIRO Code of Conduct and PGPA Act which requires staff to act ethically, and with integrity, in their official capacity ○ Report all Code of Conduct breaches ○ Be familiar with organisational fraud policy ○ Participate in all awareness and educational campaigns (i.e. Fraud eLearning courses) ○ Disclose any real, or potential, conflicts of interest ○ Embody strong moral aptitude ○ Assist the Fraud Control team with any informal or formal enquiries ○ Report any suspected fraud to either line or senior management, the Fraud Control Manager or an Authorised Internal Recipient (under PID Scheme).

s 22

s 22

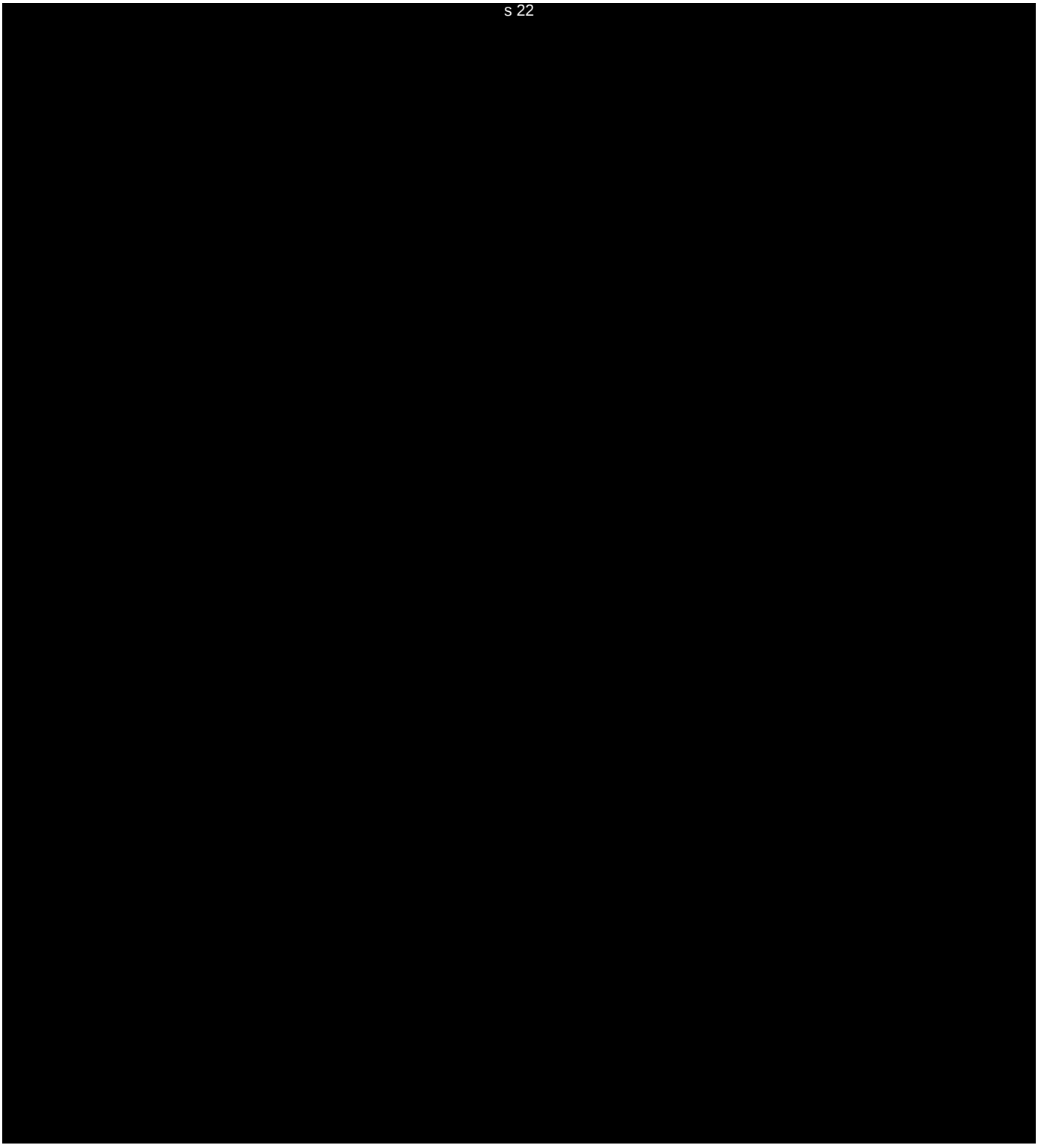
s 22

s 22

s 22

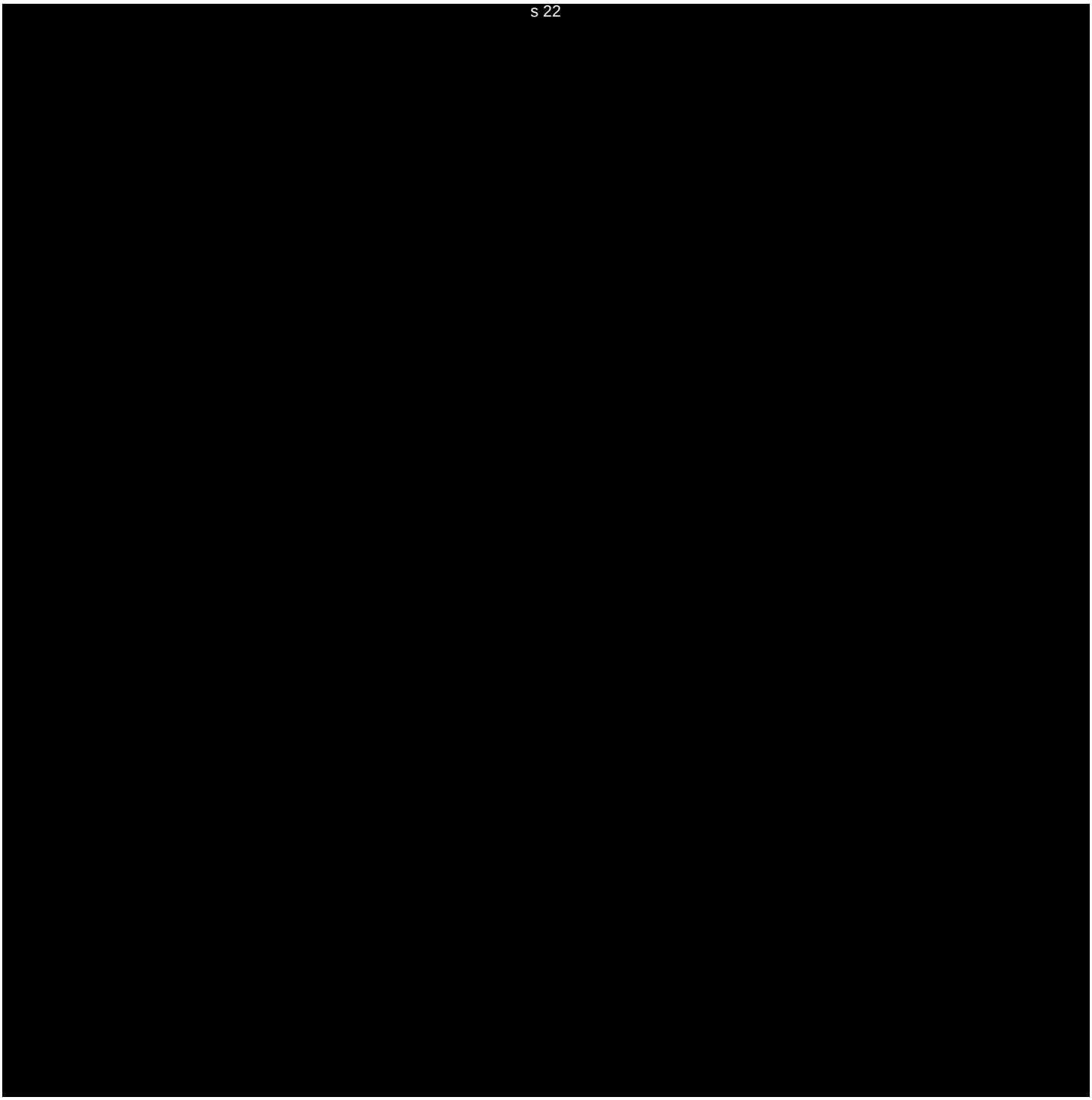
s 22

s 22


s 22

s 22

s 22


s 22

10 2016 FRAUD RISK ASSESSMENT (FRA) RESULTS* Sensitive/privileged information omitted.

Fraud Risk Number	Fraud Risk Title	Fraud Risk Description
1	Scientific Fraud / Research Misconduct	s 22
2	Unauthorised release of classified / sensitive information	
3	Unauthorised practices in overseas jurisdictions	
4	Potential for an Insider Threat	

s 22

Fraud Risk Number	Fraud Risk Title	s 22	s 22
5	Unauthorised access of CSIRO ICT, Data and Sites		
6	Modes of theft – credit cards, procurement, assets, cash and cash equivalents		

Fraud Risk Number	Fraud Risk Title	s 22	s 22
7	Misrepresentation of qualification / identity		
8	Unauthorised disclosure or theft of Intellectual Property		
9	Fraudulent activity in CRCs, Joint Ventures ('JVs'), spin-off companies, or other collaborative activities		
10	Falsification of statutory documentation or funding submissions		

Fraud Risk Number	Fraud Risk Title	s 22	s 22
11	Inappropriate application of HR Policy with the intent to defraud		
12	Conflict of interest with the intent to defraud		
13	Abuse of Travel		
14	Use of CSIRO property for private use		
15	Falsification of payroll claims		

10.1 Likelihood Table

LEVEL		LIKELIHOOD DESCRIPTION	LIKELIHOOD FACTOR
5	ALMOST CERTAIN	> 90% chance of the risk occurring or The risk event is expected to occur at least once within the next year or The issue has occurred within the last year	5
4	LIKELY	60-90% chance of the risk occurring or The risk event is expected to occur at least once within the next 2 years or The issue has occurred within the last 2 years	4
3	POSSIBLE	40-60% chance of the risk occurring or The risk event is expected to occur at least once within the next 3 years or The issue has occurred within the last 3 years	3
2	UNLIKELY	10-40% chance of the risk occurring or The risk event is expected to occur at least once within the next 4 years or The issue has occurred within the last 4 years	2
1	RARE	<10% chance of the risk occurring or The risk event is expected to occur at least once within the next 5 years or The issue has occurred within the last 5 years	1

s 22

[redacted]

10.3 Enterprise Risk Scoring Matrix and Management Action Table

Memorandum to the CSIRO Board Audit and Risk Committee

Meeting No: 137 | 24 August 2018 | Agenda Item: 8.2

Subject: 2017/2018 Security and Fraud Report

Document 3

Author: s 22 [redacted]

Sponsor:

Date: 18 July 2018

Action for BARC: Decision ☐ Discussion ☐ Information ☒

1. Executive Summary

As required by the Commonwealth Fraud Control Framework ('**Framework**'), CSIRO complies with the Fraud Rule. s 22 [redacted]

During 2017-2018, Security & Fraud:

- completed the 2018 CSIRO Fraud Risk Assessment (with CSIRO Risk) and 2018 Fraud and Corruption Control Plan in accordance with the Fraud Rule;

s 22 [redacted]

2. Background

s 22 [redacted]

s 22

[redacted]

s 22

[redacted]

Fraud - Operational Activities

s 22

- Undertaking the 2018 Fraud Risk Assessment (FRA) and completing the 2018 Fraud and Corruption Control Plan ('The Plan').

s 22

Memorandum to the CSIRO Board Audit & Risk Committee (Board in Confidence)

BARC Meeting No: 137	24 August 2018	Agenda Item: 8.3
Subject:	2018 Fraud Risk Assessment (FRA) and 2018 Fraud and Corruption Control Plan ('The Plan')	
Author:	s 22	Document 4
Sponsor:		
Date:	15 August 2018	
Action for BARC:	Decision ☒ Discussion ☐ Information ☐	

s 22

2. Background

The Fraud Rule is one element of the Commonwealth Fraud Control Framework and it is binding on CSIRO as a corporate Commonwealth entity. The Fraud Rule requires that the accountable authority of a Commonwealth entity must conduct fraud risk assessments regularly and when there is a substantial change in the structure, functions or activities of the entity. CSIRO last conducted a Fraud Risk Assessment in 2016. The Fraud Guidance within the Commonwealth Fraud Framework, while not binding on CSIRO, recommends that entities conduct fraud risk assessments at least every 2 years. Having regard to the Fraud Guidance and, given the significant alleged fraud that occurred in 2017, it was timely that the FRA was conducted and that CSIRO's Fraud and Corruption Control Plan was updated.

The Plan documents current organisational fraud risks and assigns control ownership for these risks.

3. Current Situation

2018 Fraud Risk Assessment

Since the 2016 FRA was conducted there has been a slight increase in the number of reports of alleged fraud and/or misconduct. Given the fraud risks identified in the FRA the Security &Fraud team has assessed there is an increased likelihood of fraud risk events for CSIRO if certain fraud risks are left untreated.

The 2018 FRA identifies **15 potential fraud risks** which could manifest as a result of dishonest conduct by either internal or external perpetrators. The risk ratings are informed by the *Fraud statistics 1 July 2016 – 30 June 2018, below,* and an assessment of risk factors and mitigations agreed to with relevant risk owners.

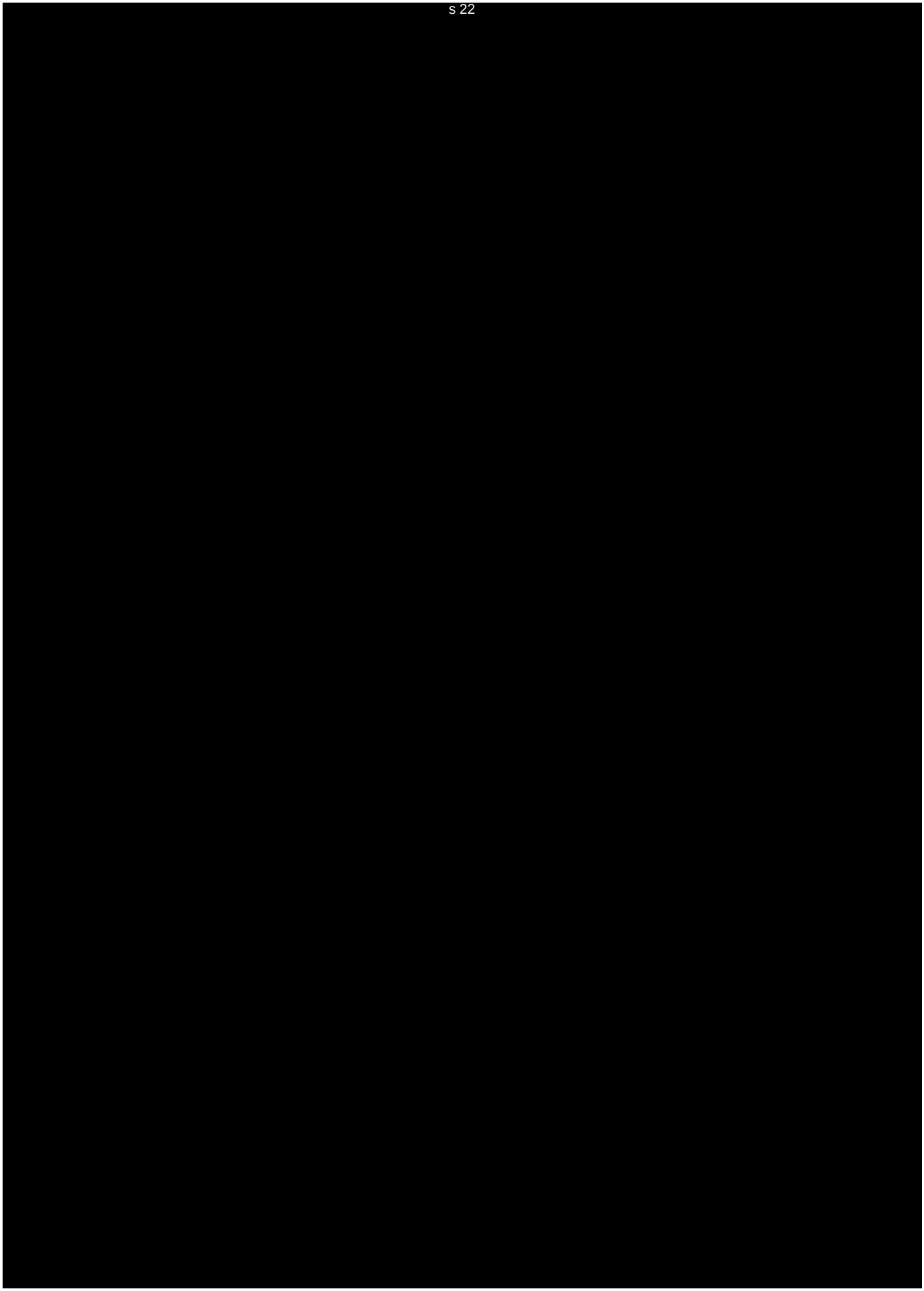
The 2018 FRA identified the following 15 fraud risks for CSIRO:

Risk No	Risk Title
1	Data & Sites
2	Scientific Misconduct and Research Fraud
3	Unauthorised practices in overseas jurisdictions
4	Modes of theft utilising CSIRO corporate credit cards (CCCs)
5	Modes of theft utilising Accounts Payable & Procurement
6	Fraudulent activities in JVs, UJVs, CRCs, Partnerships, spin-off companies, CSIRO formed and/or controlled companies/partnerships/trusts, companies for which CSIRO holds shares, and/or similar arrangements
7	Unauthorised or untimely disclosure or theft of Intellectual Property (IP)
8	Abuse of Travel
9	Improper, unreasonable or excessive use of CSIRO resources
10	Theft or inappropriate use and/or disposal of assets
11	Conflicts of interest with the intent to defraud
12	Falsification of payroll
13	Qualification and/or identity misrepresentation
14	Falsification of funding submissions or deliberately circumventing funding approval processes
15	Inappropriate application of HR Policy with the intent to defraud

s 22 [redacted]

s 22 [redacted]

s 22



s 22

[redacted]

2018 Fraud and Corruption Control Plan

The Plan assigns ownership for the organisational fraud risks identified in the FRA. The Plan:

- Identifies organisational fraud and corruption risks,
- Documents controls for these risks,
- Provides staff guidance around fraud and their responsibilities,
- Details reporting mechanisms for alleged fraud and corruption, and
- Reflects the recommendations made in the FRA which aim to strengthen existing controls to reduce the occurrence and impact of CSIRO's fraud risks.

This Plan should not be considered in isolation and it recognises that there are additional fraud controls in place within the organisation which are managed by the respective risk control owners who are the first line of defence (e.g. HR, Finance Support, Governance, IM&T).

s 22

[redacted]

s 22

[redacted]

Attachment 1 CSIRO's Fraud Risks, Future Mitigation and Additional Recommendations

Attachment 2 2018 Fraud & Corruption Control Plan

Attachment 1 - CSIRO's Fraud Risks, Future Mitigations and FRA Recommendations

RISK TITLE & OVERVIEW	s 22
Risk 1: Data & Sites – s 22	[redacted]
Risk 2: Scientific Misconduct and Research Fraud – s 22	[redacted]
Risk 3: Unauthorised practices in overseas jurisdictions – s 22	[redacted]
Risk 4: Modes of theft utilising CSIRO corporate credit cards s 22	[redacted]

RISK TITLE & OVERVIEW	s 22
Risk 5: Modes of theft utilising Accounts Payable & Procurement – s 22	
Risk 6: Fraudulent activities in joint ventures (JVs), unincorporated joint ventures (UJVs), Cooperative Research Centres (CRCs), Partnerships, Spin-off Companies, CSIRO formed and/or controlled companies/partnerships/trusts, companies for which CSIRO holds shares, and/or similar arrangements.	
Risk 7: Unauthorised or untimely disclosure or theft of Intellectual Property (IP) – s 22	
Risk 8: Abuse of Travel – s 22	
Risk 9: Improper, unreasonable or excessive use of CSIRO resources – s 22	
Risk 10: Theft or inappropriate use and/or disposal of assets – s 22 s 22	

RISK TITLE & OVERVIEW	s 22
Risk 11: Conflicts of interest with the intent to defraud – s 22	
Risk 12: Falsification of payroll - s 22 .	
Risk 13: Qualification and/or identity misrepresentation s 22	
Risk 14: Falsification of funding submissions or deliberately circumventing funding approval processes - s 22	
Risk 15: Inappropriate application of HR Policy with the intent to defraud - s 22	

Overarching Recommendations

1. Implement an Integrity Office or Integrity Oversight Committee comprising key stakeholders, to ensure consistency in matter handling for alleged misconduct and fraud within CSIRO. Currently, there are disparate processes within Business Units and Functions, and implementing an Integrity Office will ensure that;
    a. Alleged misconduct and fraud is treated consistently, in line with CSIRO and Australian Government policy.
    b. Relevant CSIRO stakeholders (e.g. Security & Fraud, HR, WR&P, Legal) have absolute oversight of misconduct or fraud risk events requiring action,
    c. There is an increased visibility of the overall incidences and consequences associated with misconduct and fraud.
    d. The organisation has comprehensive and accurate data to determine the effect misconduct and fraud poses to CSIRO.
2. Due to the increasing trend of reported fraud and misconduct within CSIRO, CSIRO should consider increasing fraud control resourcing. According to the AIC's 'Commonwealth fraud investigations 2015-16' report, *'Entities with fewer than 1,000 employees commonly had fewer than five employees working in fraud control, while large entities with over 1,000 employees had between six and 10 fraud control staff, on average'.*
3. Continue to increase visibility of CSIRO's PID Scheme and the Security & Fraud Control Team.
4. Implement a single investigative procedure to ensure investigative process consistency and discharged in line with legal requirements.
5. Board and Management (at all levels) should implement mechanisms to strengthen an anti-fraud culture in CSIRO which;
    a. Encourages the reporting of fraud and misconduct
    b. Enables an environment where staff and affiliates feel comfortable and safe to report fraud and misconduct
    c. Increases awareness and training to enable staff and affiliates to recognise different fraud and misconduct types
    d. Introduces consistent and more robust consequence management, e.g. 'deterrent effect'
    e. Demonstrates that the organisation is serious about tackling fraud and misconduct.
6. Liaise with Internal Audit to inform CSIRO's Annual Internal Audit Plan to ensure high fraud risk areas, e.g. credit cards, service claims, travel, and assets, are periodically audited and controls reviewed for effectiveness.

www.csiro.au

2018 CSIRO Fraud Risk Assessment

Document 5

CSIRO Board Audit & Risk Committee (Board in Confidence)

Authors: Governance - Security & Fraud Control (S&FC) and Risk

Sponsor: Chief Operating Officer (COO)

Table of Contents

Introduction

Scope

CSIRO's Fraud Risk Assessment (FRA) provides an articulation of CSIRO's critical fraud risks. As with the previous FRA conducted in 2016, the development of the 2018 FRA involved a comprehensive identification, assessment and evaluation of key fraud risk areas, key risk factors and mitigation strategies in the context of CSIRO's internal and external environments. Fraud is a threat that affects every Commonwealth entity, in all areas of business. Fraud and related misconduct against CSIRO impacts directly on Australians; it reduces the availability of funds and impacts the delivery of our Strategy and undermines our reputation. The FRA is a critical input into CSIRO's Fraud and Corruption Control Plan and Framework, with the aim of strengthening existing controls by providing recommendations to reduce CSIRO's fraud risks. The FRA is also mandated by the PGPA/Fraud Rule.

Context and Background

The Fraud Rule of the Framework which is binding to Corporate Commonwealth entities requires fraud risk assessments to be conducted *'regularly and when there is a substantial change in the structure, functions or activities of the entity'.* The Fraud Guidance (fraud control better practice) defines 'regularly' as at least every two years, with consideration to be given to an entity's function and operation; if activities are associated with high fraud risks, or the entity operates in high fraud or corruption risk areas, assessments should be undertaken at more frequent intervals. Given the internal matters reported and investigated within CSIRO during this period, it is timely for the FRA and Fraud and Corruption Control Plan to be undertaken at this time.

The 2018 FRA was developed in a consultative and considered manner, with a review of CSIRO's internal and external environments to ensure the FRA assessed the environments in which we operate, impact, and are impacted by.

- Internal environmental scan;
    - Risk discussions with key internal stakeholders from ESS Functions and Business Units, and review of relevant documentation
    - Reviewing and assessing alleged frauds escalated through the Public Interest Disclosure (PID) Scheme, Security & Fraud Control Function and other mechanisms
    - Relevant Policies, Procedures and Controls
    - CSIRO Strategy
    - Organisational Risk Profiles: 2016 and 2017
    - Internal Audit Reports and recommendations (e.g. 2016 Research Conduct Audit)
- External environmental scan – reviewed external fraud, bribery and corruption reports included;
    - ACFE's 'Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse'
    - EY's 2017 Asia-Pacific Fraud Survey: *'Economic uncertainty, Unethical conduct: How should over-burdened compliance functions respond?*
    - Deloitte's 'Bribery and Corruption Survey 2017 Australia and New Zealand'
    - Grant Thornton's 'Fraud in focus – March 2017' report
    - World Economic Forum's report: 'The Global Risks Report 2018'
    - Eurasia Group's 'Top Risks 2018' report
    - Kroll's 'Global Fraud & Risk Report: Building Resilience in a Volatile World'

Please refer to Appendix B 'External Fraud, Anti-bribery & Corruption Findings' for survey results and key themes relevant to the FRA's findings.

Fraud Risk in the Organisational Risk Context

It is acknowledged that fraud risk should not be considered in isolation and has important synergies across the Organisational risk management environment. Organisational vulnerabilities such as poor IT network controls, people checking or building security controls create vectors by which fraud risk events can manifest, therefore fraud risk management strategies are considered integral and complementary withint the context of broader risk management planning (ie Enterprise Security Program), and vice versa.

Limitations

Details relating to the alleged fraud incident involving a senior CSIRO Executive member which was made known to CSIRO in July 2017 have not been considered within this Fraud Risk Assessment with the exception of key incident themes, as full details surrounding this incident were not made available to the FRA team during this process. Statistics provided in the 'findings' section do not include matters managed in-house by Business Units (BU), Human Resources (HR)/Workplace Relations and Policy (WR&P), IM&T/Cyber Security and Security which do not get report to S&FC. These BUs and Functions have their own reporting mechanisms, processes and confidentiality requirements which means not all matters are escalated through to the Fraud Control Team.

Key Changes from 2016 Fraud Risk Assessment

Closed risks:

- **Potential for an insider threat**

This is no longer a standalone risk, the essence of this risk has been included as a "causes" into the other 2018 FRA risks.

New risks:

- **Data & Sites**

Unauthorised release of classified/sensitive information' merged with *'unauthorised access of CSIRO's ICT, Data and Sites' to form 'Data & Sites'*.

The 2016 FRA risk *"Modes of theft – credit cards, procurement, assets, cash & cash equivalents',* was separated into the following three risk to ensure appropriate evaluation:.

- **Modes of theft utilising CSIRO corporate credit cards**
- **Modes of theft utilising Accounts Payable & Procurement**
- **Theft or inappropriate use and/or disposal of assets**

s 22

[redacted]

The overarching recommendations based on this year's FRA include:

1. Consideration of an Integrity Office or Integrity Oversight Committee comprising key stakeholders, to ensure consistency in matter handling for alleged misconduct and fraud within CSIRO. Currently, there are disparate processes within Business Units and Functions, and implementing an Integrity Office will ensure that;
    a. Alleged misconduct and fraud is treated consistently, in line with CSIRO and Australian Government policy.
    b. Relevant CSIRO stakeholders (e.g. Security & Fraud, HR, WR&P, Legal) have absolute oversight of misconduct or fraud risk events requiring action,
    c. There is an increased visibility of the overall incidences and consequences associated with misconduct and fraud.
    d. The organisation has comprehensive and accurate data to determine the effect misconduct and fraud poses to CSIRO.
2. Due to the increasing trend of reported fraud and misconduct within CSIRO, and to strengthen the FY 18/19-FY19/20 strategy and workplan by supporting more fraud prevention efforts and allow more timely response capabilities, CSIRO should consider increasing fraud control resourcing. According to the AIC's 'Commonwealth fraud investigations 2015-16' report, *'Entities with fewer than 1,000 employees commonly had fewer than five employees working in fraud control, while large entities with over 1,000 employees had between six and 10 fraud control staff, on average'.*
3. Continue to increase visibility of CSIRO's PID Scheme and the Security & Fraud Control Team.
4. Implement a single investigative procedure to ensure investigative process consistency and discharged in line with legal requirements.
5. Board and Management (at all levels) should implement mechanisms to strengthen an anti-fraud culture in CSIRO which;

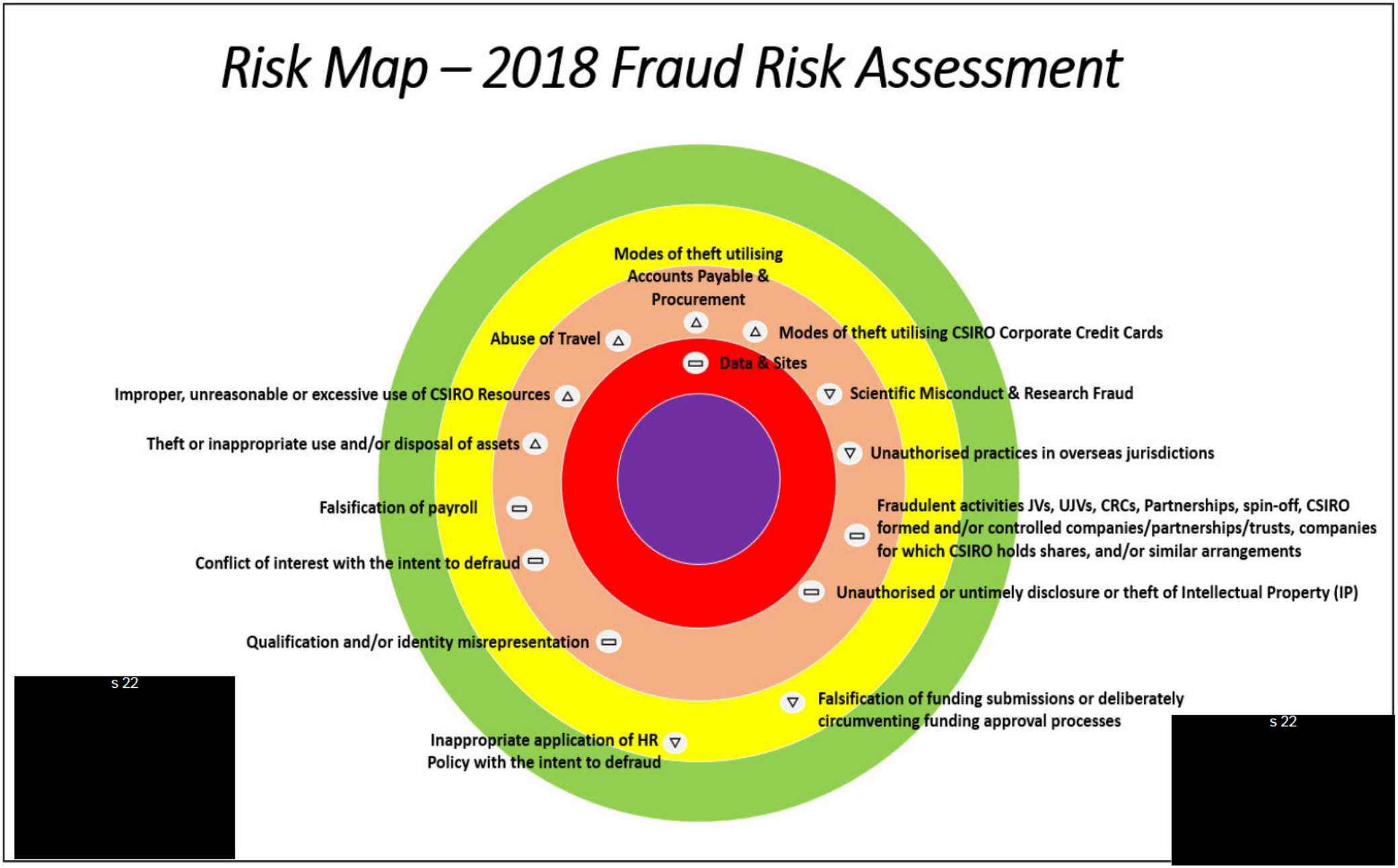
a. Encourages the reporting of fraud and misconduct
b. Enables an environment where staff and affiliates feel comfortable and safe to report fraud and misconduct
c. Increases awareness and training to enable staff and affiliates to recognise different fraud and misconduct types
d. Introduces consistent and more robust consequence management, e.g. 'deterrent effect'
e. Demonstrates that the organisation is serious about tackling fraud and misconduct.

6. Mechanism used to inform CSIRO's Annual Internal Audit Plan to ensure high fraud risk areas, e.g. credit cards, service claims, travel, and assets, are periodically audited and controls are considered for review.
7. Support the implementation of 'additional FRA recommendations' as highlighted in Appendix A.

CSIRO's Top 10 Fraud Risks	s 22
1. Data and Sites	
2. Scientific Misconduct and Research Fraud	
3. Unauthorised practices in overseas jurisdictions	
4. Modes of theft utilising CSIRO corporate credit cards	
5. Modes of theft utilising Accounts Payable & Procurement	
6. Fraudulent activities in JVs, UJVs, CRCs, Partnerships, Spin-off Companies, CSIRO formed and/or controlled companies/partnerships/trusts,	

	companies for which CSIRO holds shares, and/or similar arrangements.	s 22
7.	Unauthorised or untimely disclosure or theft of Intellectual Property (IP)	
8.	Abuse of Travel	
9.	Improper, unreasonable or excessive use of CSIRO resources	
10.	Theft or inappropriate use and/or disposal of assets	

Risk Map


Risk Map – 2018 Fraud Risk Assessment
Modes of theft utilising Accounts Payable & Procurement
Modes of theft utilising CSIRO Corporate Credit Cards
Abuse of Travel
Data & Sites
Improper, unreasonable or excessive use of CSIRO Resources
Scientific Misconduct & Research Fraud
Theft or inappropriate use and/or disposal of assets
Unauthorised practices in overseas jurisdictions
Falsification of payroll
Fraudulent activities JVs, UJVs, CRCs, Partnerships, spin-off, CSIRO formed and/or controlled companies/partnerships/trusts, companies for which CSIRO holds shares, and/or similar arrangements
Conflict of interest with the intent to defraud
Unauthorised or untimely disclosure or theft of Intellectual Property (IP)
Qualification and/or identity misrepresentation
s 22
Falsification of funding submissions or deliberately circumventing funding approval processes
Inappropriate application of HR Policy with the intent to defraud
s 22

Risk Table & Risk Register (Bow-Ties)

Risk No	Risk Title
1	Data & Sites
2	Scientific Misconduct and Research Fraud
3	Unauthorised practices in overseas jurisdictions
4	Modes of theft utilising CSIRO corporate credit cards (CCCs)
5	Modes of theft utilising Accounts Payable & Procurement
6	Fraudulent activities in joint ventures (JVs), unincorporated joint ventures (UJVs), Cooperative Research Centres (CRCs), Partnerships, spin-off companies, CSIRO formed and/or controlled companies/partnerships/trusts, companies for which CSIRO holds shares, and/or similar arrangements
7	Unauthorised or untimely disclosure or theft of Intellectual Property (IP)
8	Abuse of Travel

s 22 [redacted]

Risk No	Risk Title	s 22
9	Improper, unreasonable or excessive use of CSIRO resources	
10	Theft or inappropriate use and/or disposal of assets	
11	Conflicts of interest with the intent to defraud	
12	Falsification of payroll	
13	Qualification and/or identity misrepresentation	
14	Falsification of funding submissions or deliberately circumventing funding approval processes	
15	Inappropriate application of HR Policy with the intent to defraud	

RISK #	RISK TITLE
1	Data & Sites

s 22

[redacted]

RISK #	RISK TITLE
2	Scientific Misconduct and Research Fraud

s 22

s 22

RISK #	RISK TITLE
3	Unauthorised practices in overseas jurisdictions

s 22

s 22

RISK #	RISK TITLE
4	Modes of theft utilising CSIRO corporate credit cards (CCCs)

s 22

s 22

RISK #	RISK TITLE
5	Modes of theft utilising Accounts Payable & Procurement

s 22

[redacted]

RISK #	RISK TITLE
6	Fraudulent activities in joint ventures (JVs), unincorporated joint ventures (UJVs), Cooperative Research Centres (CRCs), Partnerships, spin-off companies, CSIRO formed and/or controlled companies/partnerships/trusts, companies for which CSIRO holds shares, and/or similar arrangements

s 22

s 22

s 22

RISK #	RISK TITLE
7	Unauthorised or untimely disclosure or theft of Intellectual Property (IP)

[redacted]

RISK #	RISK TITLE
8	Abuse of Travel

s 22

[redacted]

RISK #	RISK TITLE
9	Improper, unreasonable or excessive use of CSIRO resources

s 22

[redacted]

RISK #	RISK TITLE
10	Theft or inappropriate use and/or disposal of assets

s 22

[redacted]

RISK #	RISK TITLE
11	Conflicts of interest with the intent to defraud

s 22

[redacted]

s 22

RISK #	RISK TITLE
12	Falsification of payroll

[redacted]

s 22

RISK #	RISK TITLE
13	Qualification and/or identity misrepresentation

[redacted]

s 22

RISK #	RISK TITLE
14	Falsification of funding submissions or deliberately circumventing funding approval processes

RISK #	RISK TITLE
15	Inappropriate application of HR Policy with the intent to defraud

s 22

s 22

Appendix A – Detailed Recommendations

The overarching recommendations based on this year's FRA include:

1. Implement an Integrity Office or Integrity Oversight Committee comprising key stakeholders, to ensure consistency in matter handling for alleged misconduct and fraud within CSIRO. Currently, there are disparate processes within Business Units and Functions, and implementing an Integrity Office will ensure that;
    a. Alleged misconduct and fraud is treated consistently, in line with CSIRO and Australian Government policy.
    b. Relevant CSIRO stakeholders (e.g. Security & Fraud, HR, WR&P, Legal) have absolute oversight of misconduct or fraud risk events requiring action,
    c. There is an increased visibility of the overall incidences and consequences associated with misconduct and fraud.
    d. The organisation has comprehensive and accurate data to determine the effect misconduct and fraud poses to CSIRO.
2. Due to the increasing trend of reported fraud and misconduct within CSIRO, CSIRO should consider increasing fraud control resourcing. According to the AIC's 'Commonwealth fraud investigations 2015-16' report, *'Entities with fewer than 1,000 employees commonly had fewer than five employees working in fraud control, while large entities with over 1,000 employees had between six and 10 fraud control staff, on average'.*
3. Continue to increase visibility of CSIRO's PID Scheme and the Security & Fraud Control Team.
4. Implement a single investigative procedure to ensure investigative process consistency and discharged in line with legal requirements.
5. Board and Management (at all levels) should implement mechanisms to strengthen an anti-fraud culture in CSIRO which;
    a. Encourages the reporting of fraud and misconduct
    b. Enables an environment where staff and affiliates feel comfortable and safe to report fraud and misconduct
    c. Increases awareness and training to enable staff and affiliates to recognise different fraud and misconduct types
    d. Introduces consistent and more robust consequence management, e.g. 'deterrent effect'
    e. Demonstrates that the organisation is serious about tackling fraud and misconduct.
6. Liaise with Internal Audit to inform CSIRO's Annual Internal Audit Plan to ensure high fraud risk areas, e.g. credit cards, service claims, travel, and assets, are periodically audited and controls reviewed for effectiveness.

RISK TITLE & OVERVIEW	s 22
Risk 1: Data & Sites – s 22 [redacted]	s 22 [redacted]
Risk 2: Scientific Misconduct and Research Fraud s 22 [redacted]	

RISK TITLE & OVERVIEW	s 22
Risk 3: Unauthorised practices in overseas jurisdictions s 22	
Risk 4: Modes of theft utilising CSIRO corporate credit cards – s 22 s 22	
Risk 5: Modes of theft utilising Accounts Payable & Procurement – s 22 s 22	

RISK TITLE & OVERVIEW	s 22
s 22	
Risk 6: Fraudulent activities in joint ventures (JVs), unincorporated joint ventures (UJVs), Cooperative Research Centres (CRCs), Partnerships, Spin-off Companies, CSIRO formed and/or controlled companies/partnerships/trusts, companies for which CSIRO holds shares, and/or similar arrangements.	
Risk 7: Unauthorised or untimely disclosure or theft of Intellectual Property (IP) – s 22	
Risk 8: Abuse of Travel – s 22 s 22	
Risk 9: Improper, unreasonable or excessive use of CSIRO resources – s 22	
Risk 10: Theft or inappropriate use and/or disposal of assets – s 22	
Risk 11: Conflicts of interest with the intent to defraud – s 22	

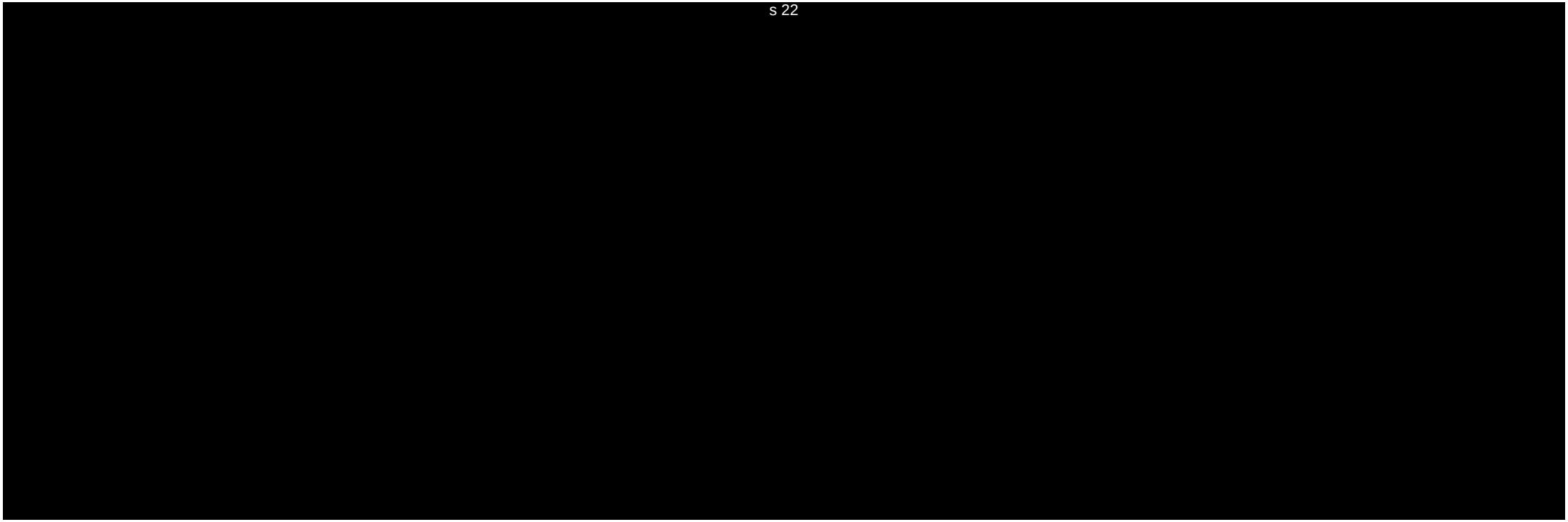
RISK TITLE & OVERVIEW
Risk 12: Falsification of payroll - s 22
Risk 13: Qualification and/or identity misrepresentation - s 22
Risk 14: Falsification of funding submissions or deliberately circumventing funding approval processes - s 22
Risk 15: Inappropriate application of HR Policy with the intent to defraud - s 22

s 22

s 22

s 22

s 22



Appendix C - 2018 Fraud and Corruption Control Plan ('The Plan')

The Fraud and Corruption Control Plan ('The Plan') documents current organisational fraud risks and assigns control ownership for these risks. The Plan is developed and maintained by CSIRO's Senior Fraud Control Advisor. The Fraud Risk Assessment (FRA) and Plan comprise a part of CSIRO's Fraud and Corruption Control Framework.

The Plan is updated in line with the FRA as required by the Commonwealth Fraud Control Framework 2017 ('Framework') which underpins the PGPA Act. It remains a crucial part of CSIRO's Fraud and Corruption Control Framework and complements the 2018 FRA. The FRA and Plan are both submitted for Board Audit & Risk Committee (BARC) endorsement. The intent of the Plan is to:

- Identify organisational fraud and corruption risks and document controls for these risks
- Provide recommendations based on FRA findings to strengthen existing controls
- Assist staff to know what fraud is, and what their responsibilities are, and
- Detail reporting mechanisms for alleged fraud and corruption.

The Australian Standards Fraud and Corruption Control (AS 8001 – 2008), PGPA Act, Framework, and CSIRO policy were incorporated into the Plan's development. Other legislation related to fraud and corruption control for CSIRO include: the Australian Government Information Security Manual (ISM), Australian Government Investigations Standards (AGIS), Commonwealth Procurement Rules (CPRs), *Crimes Act 1914, Criminal Code Act 1995, Freedom of Information Act 1982, PID Act, Privacy Act 1988* (and Australian Privacy Principles), *Proceeds of Crime Act 2002* and PSPF.

The 2018 Plan comprises the following:

1. **CSIRO's Commitment to Fraud Risk Management and Control**
2. **CSIRO's Fraud and Corruption Control Framework**
3. **Regulatory Framework & Governance**
4. **Fraud and Corruption Prevention & Detection Strategies (including FRA recommendations to strengthen existing risk controls)**
5. **Fraud and Corruption Response & Reporting**

Importantly, other parts of CSIRO's Fraud and Corruption Control Framework include the CSIRO Code of Conduct, CSIRO Fraud and Corruption Control Strategy 18-20, FRA, Fraud Control Procedure, strong tone from the top, adequate team resourcing, ethical culture, strong anti-fraud culture, fraud education and awareness program, and consistent consequence management for policy breaches.

Appendix D - 2018 Fraud Risk Assessment Participant List

Name	Job Title
s 22	

Attachment 2

Document 6

2018

FRAUD AND CORRUPTION CONTROL PLAN

('THE PLAN')

BARC SUMMARY

The Fraud and Corruption Control Plan ('The Plan') documents current organisational fraud risks and assigns control ownership for these risks. This Plan should not be considered in isolation and it recognises that there are additional fraud controls in place within the organisation which are managed by the respective risk control owners (e.g. HR, Finance Support, Governance, IM&T). In line with the Commonwealth Fraud Control Framework, the Plan's main emphasis is on preventative strategies.

The Plan is developed and maintained by CSIRO's Senior Fraud Control Advisor. The Fraud Risk Assessment (FRA) and Plan comprise a part of CSIRO's Fraud and Corruption Control Framework, and the FRA informs this document.

The Plan is updated in line with the FRA as required by the Commonwealth Fraud Control Framework 2017 ('Framework') which underpins the PGPA Act. The FRA and Plan are both submitted for Board Audit & Risk Committee (BARC) endorsement. The intent of the Plan is to:

- Identify organisational fraud and corruption risks and document controls for these risks
- Provide a set of overarching recommendations based on the FRA's findings (**refer to page 10**)
- Provide recommendations based on FRA findings to strengthen existing controls (**refer to Appendix A**),
- Assist staff to know what fraud is, and what their responsibilities are, and
- Detail reporting mechanisms for alleged fraud and corruption.

The overarching recommendations (**page 10**) relate to several FRA fraud risks and the additional recommendations (**Appendix A**) are areas in which existing controls could be further strengthened, with the acknowledgement that existing preventative and mitigating controls do exist. This document includes recommendations, both overarching and relating to specific fraud risks, as the Plan is focussed on preventing fraud and one way of achieving this is through strengthening the controls that are currently in place.

The Australian Standards Fraud and Corruption Control (AS 8001 – 2008), PGPA Act, Framework, CSIRO policy and Australian Government legislation.

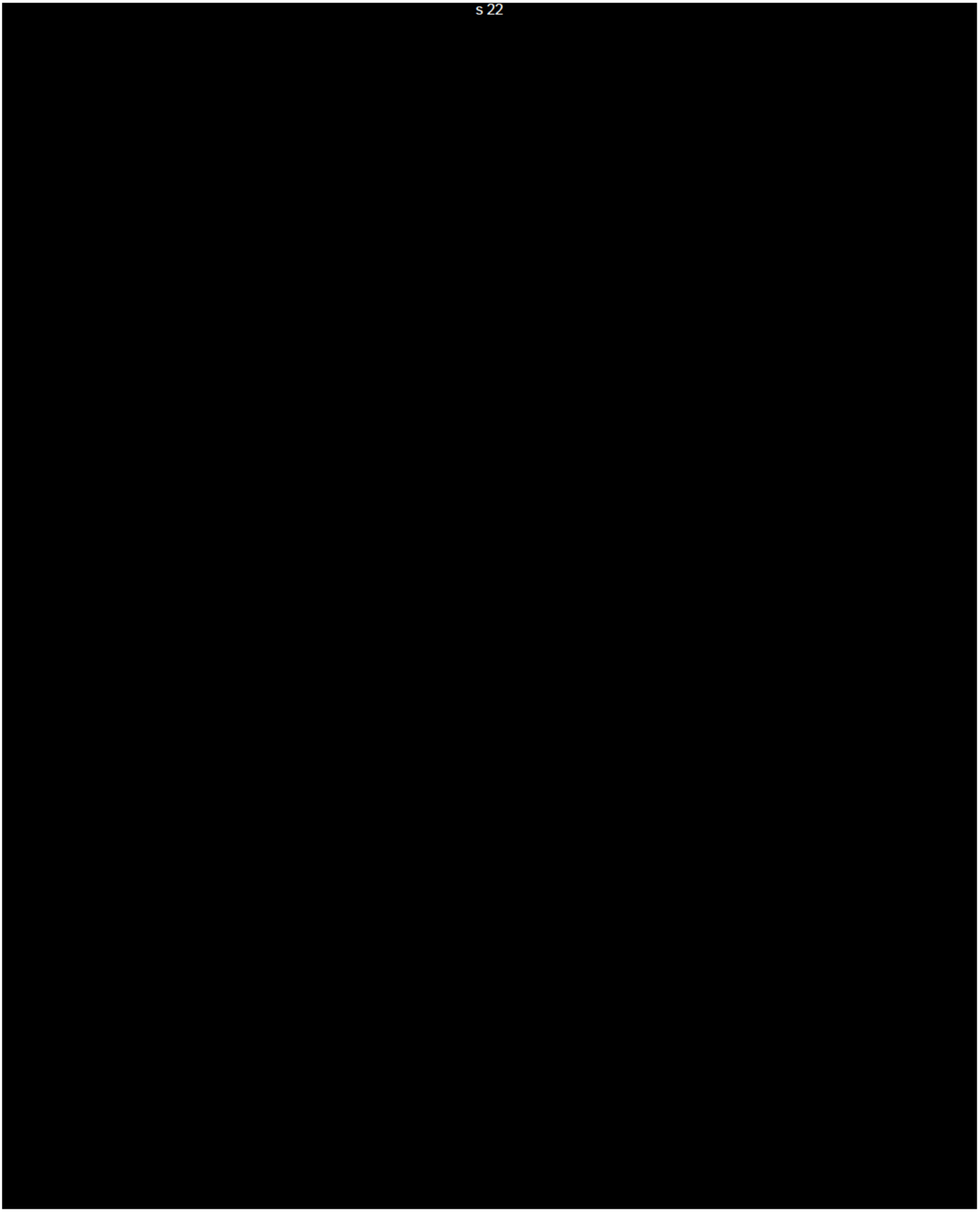
The 2018 Plan comprises the following:

1. **CSIRO's Commitment to Fraud Risk Management and Control**
2. **CSIRO's Fraud and Corruption Control Framework**
3. **Regulatory Framework & Governance**
4. **Fraud and Corruption Prevention & Detection Strategies**
5. **Fraud and Corruption Response & Reporting**

Importantly, other parts of CSIRO's Fraud and Corruption Control Framework include the CSIRO Code of Conduct, CSIRO Fraud and Corruption Control Strategy 18-20, FRA, Fraud Control Procedure, strong tone from the top, adequate team resourcing, ethical culture, strong anti-fraud culture, fraud education and awareness program, and consistent consequence management for policy breaches.

For the full CSIRO 2018 Fraud and Corruption Plan ('The Plan') refer to the following pages.

TABLE OF CONTENTS


s 22

2 INTRODUCTION

2.1 Organisational Foreword

CSIRO'S COMMITMENT TO FRAUD RISK MANAGEMENT AND CONTROL

The Commonwealth Scientific and Industrial Research Organisation (herein referred to as CSIRO), does not tolerate fraud or corruption. Having fraud occur within CSIRO in the past, we are aware that fraud can have tangible effects on our organisation such as limiting the funding intended for our science; and in so doing, limiting our capacity to deliver national impact. It can and has also had a profound effect on our staff. No one wants that.

CSIRO is committed to nurturing an anti-fraud culture which predicts, pre-empts and prevents fraud, and in the detection, reporting and investigation of dishonest conduct affecting CSIRO. We will take steps to recover financial losses to CSIRO caused by fraud.

Fraud is defined as '*dishonestly obtaining a benefit, or causing a loss, by deception or other means*' by the Commonwealth Fraud Control Framework 2017 and can be prosecuted under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), *Crimes Act 1914*, and *Criminal Code Act 1995*. Corrupt conduct and Fraud are breaches of CSIRO policy and will result in disciplinary action.

CSIRO will investigate all reported alleged fraud and corrupt conduct, and any fraud disclosures made in line with CSIRO's Public Interest Disclosure (PID) Scheme will be handled in accordance with this policy.

All staff members and CSIRO affiliates have a responsibility to understand what fraud is, and to report it via the available mechanisms. CSIRO expects everyone to act ethically and with integrity.

All staff members and CSIRO affiliates should familiarise themselves with CSIRO policy to assist us in maintaining an effective anti-fraud culture, and importantly, an organisation where we are all proud to work.

2.2 Plan Intent

The Fraud and Corruption Control Plan ('The Plan') documents current organisational fraud risks and assigns control ownership for these risks. The Plan is developed and maintained by CSIRO's Senior Fraud Control Advisor. The Fraud Risk Assessment (FRA) and Plan comprise a part of CSIRO's Fraud and Corruption Control Framework.

The Fraud Rule of the Framework which is binding to Corporate Commonwealth entities requires fraud risk assessments to be conducted *'regularly and when there is a substantial change in the structure, functions or activities of the entity'*. The Fraud Guidance (fraud control better practice) defines 'regularly' as at least every two years, with consideration to be given to an entity's function and operation; if activities are associated with high fraud risks, or the entity operates in high fraud or corruption risk areas, assessments should be undertaken at more frequent intervals. It remains a crucial part of CSIRO's Fraud and Corruption Control Framework and complements the 2018 FRA. This Plan should not be considered in isolation and it recognises that there are additional fraud controls in place within the organisation which are managed by the respective risk control owners (e.g. HR, Finance Support, Governance, IM&T). The FRA and Plan are both submitted for Board Audit & Risk Committee (BARC) endorsement. The intent of the Plan is to:

- Identify organisational fraud and corruption risks and document controls for these risks
- Provide recommendations based on FRA findings to strengthen existing controls
- Assist staff to know what fraud is, and what their responsibilities are, and
- Detail reporting mechanisms for alleged fraud and corruption.

The following guidance has been incorporated into the development of the Plan:

- Australian Standards Fraud and Corruption Control (AS 8001 – 2008)
- PGPA Act, Framework, and
- CSIRO policy and procedure.

2.3 Fraud and Corruption within CSIRO

CSIRO, like any large Corporate Commonwealth entity, is not immune to fraud. Despite our best efforts, fraud has occurred within CSIRO.

Examples of fraud and corruption that have occurred within CSIRO include:

- Misuse of power, position or Delegation for a benefit
- Manipulation of payment procedures
- Creation and/or utilisation of fictitious identities
- Misusing CSIRO resources (e.g. internet, mobile, fleet, corporate credit card, QBT system, assets)
- False or inflated invoicing
- Submitting excessive or unauthorised travel claims
- Submitting false or inflated reimbursement claims
- Overstating timesheet hours
- Falsely attributing authorship
- Supplying incorrect or misleading information.

s 22

[redacted]

3.3 2018 CSIRO Fraud Risk Assessment (FRA)

Governance's Security & Fraud Control (S&FC) and Risk completed the 2018 FRA on CSIRO's behalf. The FRA was undertaken in the context of internal and external environments, and the impact of these elements on

CSIRO's exposure to fraud. In brief, the FRA is a point in time snapshot of CSIRO's fraud risk profile. 2018's FRA highlighted that the organisation's internal environment played a significant part in this year's process, with misconduct, security and fraud incidents contributing to the crystallisation of risk scores for those risks.

Other factors included in the 2018 FRA analysis included a review of findings in CSIRO's Organisational Risk Profile (ORP), the 'mood' within the organisation, CSIRO's journey to realising Strategy 2020, internally driven elements (compliance and controls, policy and procedure, Enterprise and Business Unit governance) and external fraud, bribery and corruption findings which when taken together, clearly depicted where the organisation's risks and challenges lie.

The PGPA/Fraud Rule is the legislative framework for CSIRO's FRA and remains a mandatory fraud requirement for all Commonwealth entities. Conducting a FRA also ensures that the current risk framework in place continues to be effective for its purposes. The top ten fraud risks are as follows:

1. **Data & Sites** s 22
2. **Scientific Misconduct and Research Fraud** s 22
3. **Unauthorised practices in overseas jurisdictions** s 22
4. **Modes of theft utilising CSIRO corporate credit cards (CCCs)** s 22
5. **Modes of theft utilising Accounts Payable & Procurement** s 22
6. **Fraudulent activities in joint ventures, UJVs, CRCs, Partnerships etc.** s 22
7. **Unauthorised or untimely disclosure or theft of IP** s 22
8. **Abuse of Travel** s 22
9. **Improper, unreasonable or excessive use of CSIRO resources** s 22
10. **Theft or inappropriate use and/or disposal of assets** s 22

This year's FRA has outlined a set of recommendations (in Appendix) to further improve the existing preventative controls for high fraud risk areas, taking risk causes into account. Risk ratings are consistent with the Enterprise Risk Rating Methodology.

s 22

4 REGULATORY FRAMEWORK & GOVERNANCE

4.1 Regulatory Framework

- **PGPA Act**

The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requires CSIRO to govern ethically, resource manage, perform and be accountable for its activities.

- **Commonwealth Fraud Control Framework 2017**

As a Corporate Commonwealth Entity (CCE), CSIRO must adhere to the Fraud Rule which is section 10 of the Public Governance, Performance and Accountability Rule 2014 and is detailed below.

> *The accountable authority of a Commonwealth entity must take all reasonable measures to prevent, detect and deal with fraud relating to the entity, including by:*
>
> *(a) conducting fraud risk assessments regularly and when there is a substantial change in the structure, functions or activities of the entity; and*
>
> *(b) developing and implementing a fraud control plan that deals with identified risks as soon as practicable after conducting a risk assessment; and*
>
> *(c) having an appropriate mechanism for preventing fraud, including by ensuring that:*
>
> *(i) officials in the entity are made aware of what constitutes fraud; and*
>
> *(ii) the risk of fraud is taken into account in planning and conducting the activities of the entity; and*
>
> *(d) having 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; and*
>
> *(e) having an appropriate mechanism for investigating or otherwise dealing with incidents of fraud or suspected fraud; and*
>
> *(f) having an appropriate mechanism for recording and reporting incidents of fraud or suspected fraud.*

Whilst not mandatory for CSIRO, it is considered fraud control best practice to apply the Framework's Fraud Policy (Commonwealth Fraud Control Policy) and Fraud Guidance (Resource Management Guide No. 201).

- ***Science and Industry Research Act 1949* (SIR Act)**

CSIRO is an Australian Government Corporate entity, constituted and operating under the *Science and Industry Research Act 1949* (SIR Act). Section 22 of the PGPA Act allows the Finance Minister to issue government policy orders to CSIRO in relation to Australian Government policy.

- **Legislation related to fraud and corruption control for CSIRO**

- Australian Government Information Security Manual (ISM)
- Australian Government Investigations Standards (AGIS)
- Commonwealth Procurement Rules (CPRs)
- *Crimes Act 1914*
- *Criminal Code Act 1995*
- *Freedom of Information Act 1982*
- *PID Act*
- *Privacy Act 1988* (and Australian Privacy Principles)
- *Proceeds of Crime Act 2002*
- *PSPF*

- **CSIRO Policies and Procedures – detailed below**

s 22

[redacted]

CSIRO's Governance structure:

- **CSIRO Board**
- **CSIRO Leadership Team** – comprising Chief Executive, Chief of Staff, Executive Team, Business Unit Directors and Enterprise Support Directors. Teams are supported by SICOM, MTC, Science Council, and other Governance and Management Committees and Offices.
- **Delegated authorities** – Authorised Delegates (e.g. Line/Senior Management, Project, Group and Program Leaders, and Delegations by Policy Area and Authority Ranking).

s 22

[redacted]

s 22

s 22

s 22

s 22

s 22

s 22

s 22

7 APPENDICES

7.1 Appendix A: Additional FRA Recommendations

The below table highlights the top risk factors, future mitigations and additional FRA recommendations with the acknowledgement that existing preventative and mitigating controls are in place.

RISK TITLE & OVERVIEW	s 22 [redacted]
Risk 1: Data & Sites – s 22 [redacted]	
Risk 2: Scientific Misconduct and Research Fraud – s 22 [redacted]	
Risk 3: Unauthorised practices in overseas jurisdictions s 22 [redacted]	
Risk 4: Modes of theft utilising CSIRO corporate credit	

RISK TITLE & OVERVIEW	s 22
cards – [redacted]	[redacted]
Risk 5: Modes of theft utilising Accounts Payable & Procurement [redacted]	[redacted]
Risk 6: Fraudulent activities in joint ventures (JVs), unincorporated joint ventures (UJVs), Cooperative Research Centres (CRCs), Partnerships, Spin-off Companies, CSIRO formed and/or controlled companies/partnerships/trusts, companies for which CSIRO holds shares, and/or similar arrangements.	
Risk 7: Unauthorised or untimely disclosure or theft of Intellectual Property (IP) – [redacted]	[redacted]

RISK TITLE & OVERVIEW	s 22
s 22 **Risk 8: Abuse of Travel** – s 22	
Risk 9: Improper, unreasonable or excessive use of CSIRO resources – s 22 s 22	
Risk 10: Theft or inappropriate use and/or disposal of assets – s 22	
Risk 11: Conflicts of interest with the intent to defraud – s 22	
Risk 12: Falsification of payroll s 22	
Risk 13: Qualification and/or identity misrepresentation - s 22	

RISK TITLE & OVERVIEW	s 22
Risk 14: Falsification of funding submissions or deliberately circumventing funding approval processes - s 22 s 22	
Risk 15: Inappropriate application of HR Policy with the intent to defraud - s 22	