Financial and Performance Reporting Forum

Friday, 5 July 2024

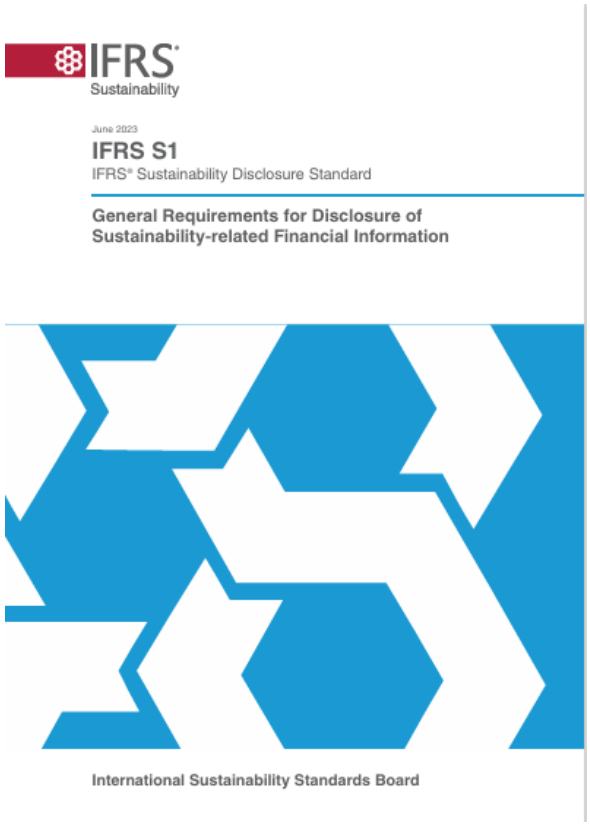
Welcome and opening remarks

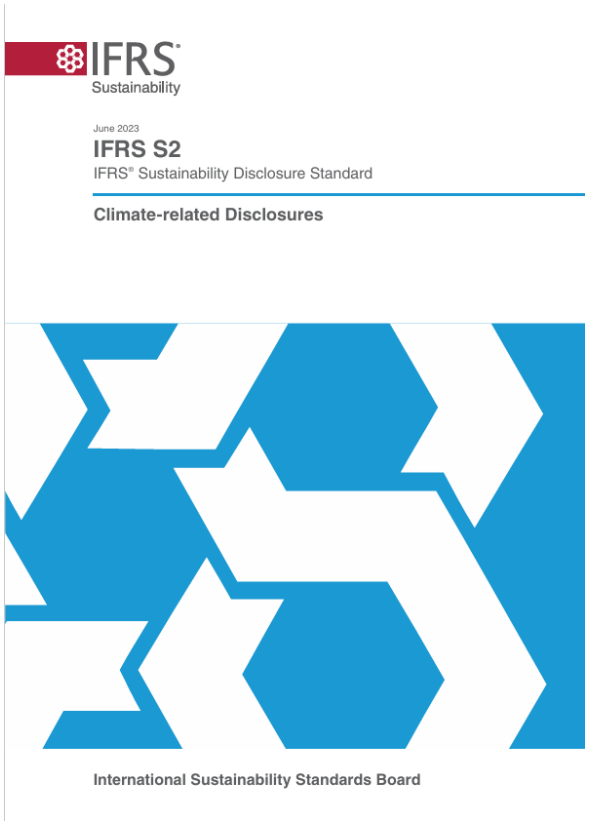
Carla Jago
Acting Deputy Auditor-General

Developments in sustainability reporting

Jane Meade
Group Executive Director
Professional Services Group

Global developments





Australian context - Consultation processes

POLICY

Discovery consultation (Dec 2022-Feb 2023)	Design consultation (Jun 2023-July 2023)	Exposure draft legislation consultation (Jan 2024-Feb 2024)	Legislation introduced to Parliament (March 2024)

STANDARDS

ED legislation – ASIC Act (Nov 2022-Dec 2022)	ASIC Act amendments introduced to Parliament (Feb 2023)	AASB standards consultation (October 2023-March 2024)	AASB issues climate disclosure standards

Policy Architecture

Climate Disclosure Policy Architecture

	Climate-related Financial Disclosure (Treasury-led)	Commonwealth Climate Disclosure (Finance-led)	
	Private sector	Stream 1	Stream 2
Thresholds	Listed and unlisted entities equivalent in size, or greater than, large propriety companies	Commonwealth companies equivalent in size, or greater than, ASX300 (*Group 1 or 2*) and Commonwealth companies equivalent in size to large propriety companies with material climate risks (*Group 3*)*	Commonwealth companies that do not meet the thresholds for inclusion in stream 1*	All non-corporate and corporate Commonwealth entities
Reporting requirements	Climate disclosure standard by Australian Accounting Standards Board		Reporting requirements tailored for affected Commonwealth entities and companies - based on Australian Accounting Standards Board climate disclosure standard	
Legislative instrument	*Corporations Act 2001*		s516A *Environmental Protection and Biodiversity Conservation Act 1999* and ongoing legislative reform under Nature Positive Plan. Supported by Resource Management Guides for annual reporting by entity type (as per the *Public Governance, Performance and Accountability Act 2013*)	
Supported by DCCEEW	*The Australian Government's Approach to Climate Risk Management in the Public Sector 2024-2026* defines 3 objectives to support climate risk management by Commonwealth entities and Commonwealth companies, one of which is climate disclosure. The Climate Risk and Opportunity Management Program is providing the tools and services needed for entities to assess and manage their climate risks.			

*Commonwealth companies that fall in Group 3 of the Treasury-led reform disclose their climate risks in FY2026-27 under stream 2. For those companies that are identified as having material climate risks, subsequent disclosures are made following the Treasury-led reform. All other Commonwealth companies that meet the threshold for Group 3 inclusion, but don't have material climate risks, would continue to make climate disclosures under stream 2, alongside Commonwealth companies that do not meet prescribed thresholds for inclusion in the Treasury-led reform.

Source: Department of Finance website

Phased implementation - companies

First annual reporting periods starting on or after	Large entities and their controlled entities meeting at least two of three criteria:			National Greenhouse and Energy Reporting (NGER) Reporters	Asset Owners
	Consolidated revenue	EOFY consolidated gross assets	EOFY employees		
1 July 2025 Group 1	$500 million or more	$1 billion or more	500 or more	Above NGER publication threshold	N/A
1 July 2026 Group 2	$200 million or more	$500 million or more	250 or more	All other NGER reporters	$5 billion assets under management or more
1 July 2027 Group 3	$50 million or more	$25 million or more	100 or more	N/A	N/A

Source: Mandatory climate-related financial disclosures Policy Statement – Department of Treasury

AASB Exposure draft


AASB Sustainability Reporting Exposure Draft

ED SR1
October 2023

Australian Sustainability Reporting Standards – Disclosure of Climate-related Financial Information

Comments to the AASB by 1 March 2024

[Draft] ASRS 1	*General Requirements for Disclosure of Climate-related Financial Information*
[Draft] ASRS 2	*Climate-related Financial Disclosures*
[Draft] ASRS 101	*References in Australian Sustainability Reporting Standards*

Source: AASB website – AASB Education webinar January 2023

Proposed requirements

Standards architecture

Four core content areas

Governance

Governance processes, controls and procedures an entity uses to monitor, manage and oversee climate-related R&O

Strategy

Strategy for managing climate-related R&O

Risk Management

Processes an entity uses to identify, assess, prioritise and monitor climate-related R&O

Metrics and targets

Approaches to measuring performance in relation to climate-related R&O

Australian Government
Australian Accounting Standards Board

Official

8

Source: AASB website – AASB Education webinar January 2023

CCD phased implementation - Pilot

Governance

- Processes, controls and procedures used to identify, prioritise, monitor, manage and oversee climate-related risks and opportunities

Risk Management

- Progress update on implementing an organisation-wide climate risk and opportunity assessment under the Climate Risk and Opportunity Management Program.

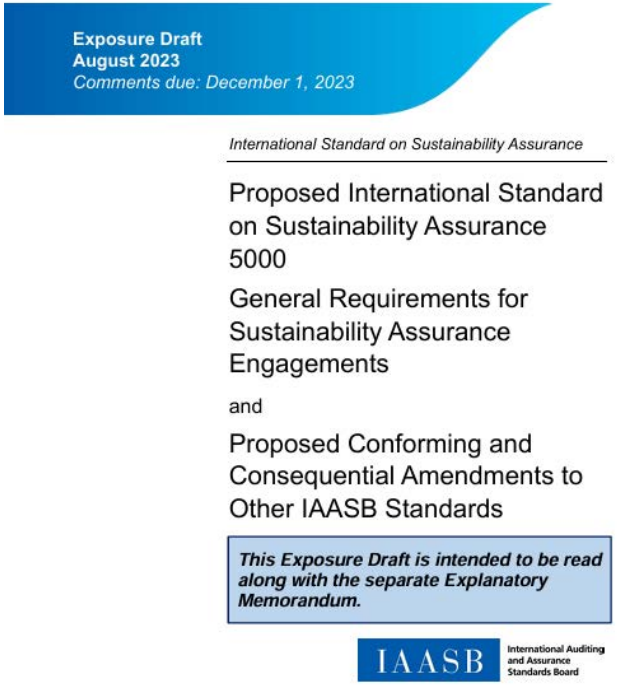
Metrics and targets

- Greenhouse gas emissions profiles and the APS Net Zero by 2030 target being work towards for emissions reduction.

Strategy

- Not included in pilot, this pillar will be included in the full Commonwealth Climate Disclosure requirements.

Assurance over disclosures



Exposure Draft
August 2023
Comments due: December 1, 2023

International Standard on Sustainability Assurance

Proposed International Standard on Sustainability Assurance 5000

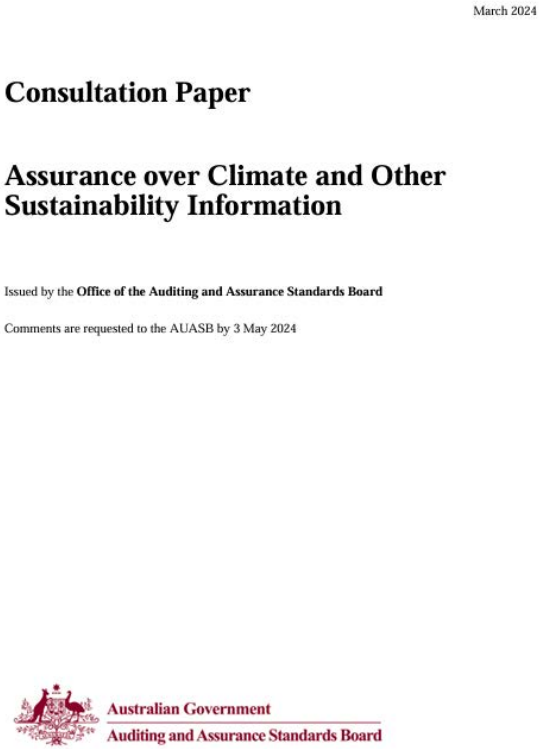
General Requirements for Sustainability Assurance Engagements

and

Proposed Conforming and Consequential Amendments to Other IAASB Standards

This Exposure Draft is intended to be read along with the separate Explanatory Memorandum.

IAASB International Auditing and Assurance Standards Board



March 2024

Consultation Paper

Assurance over Climate and Other Sustainability Information

Issued by the **Office of the Auditing and Assurance Standards Board**

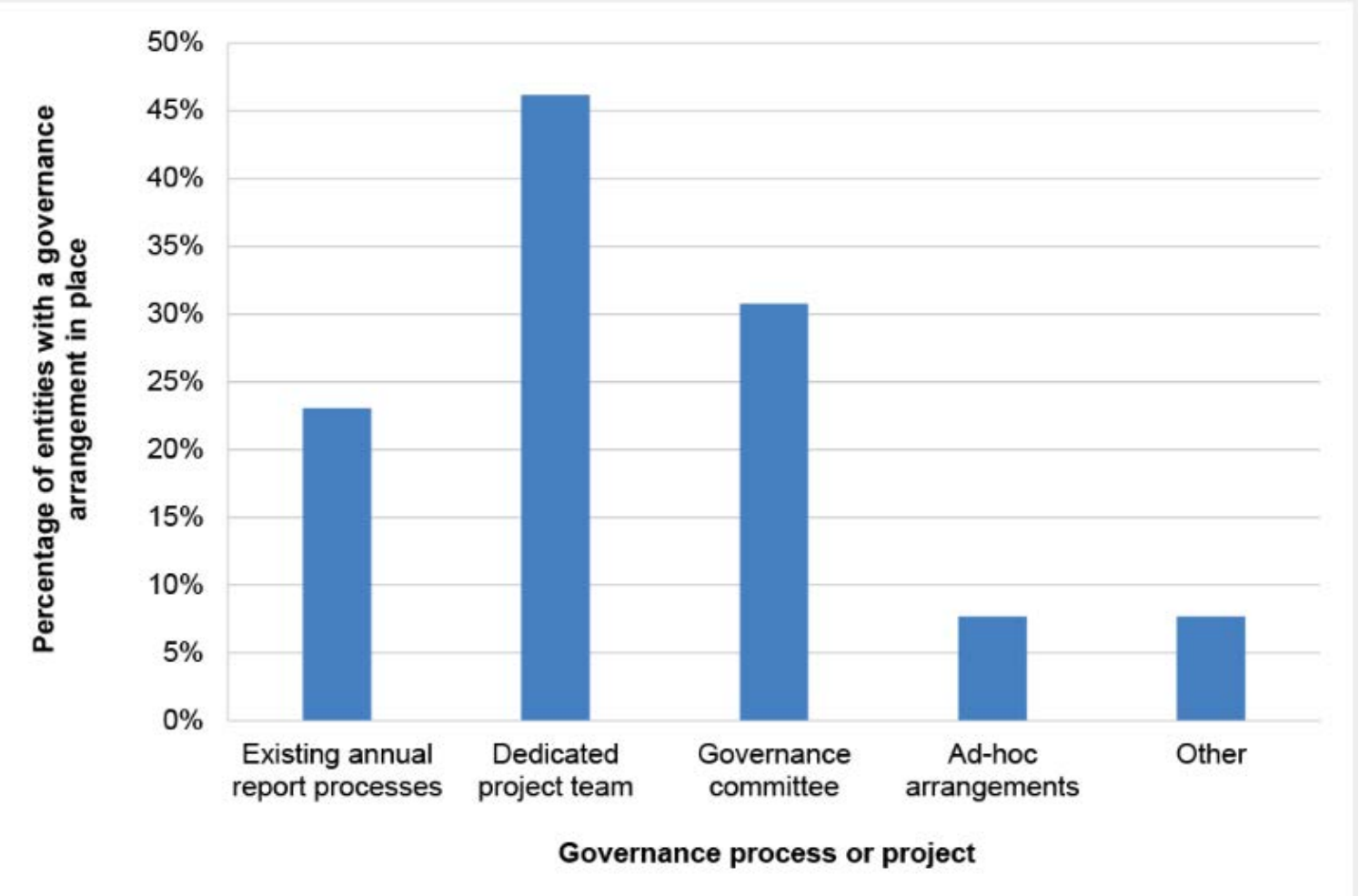
Comments are requested to the AUASB by 3 May 2024

Australian Government
Auditing and Assurance Standards Board

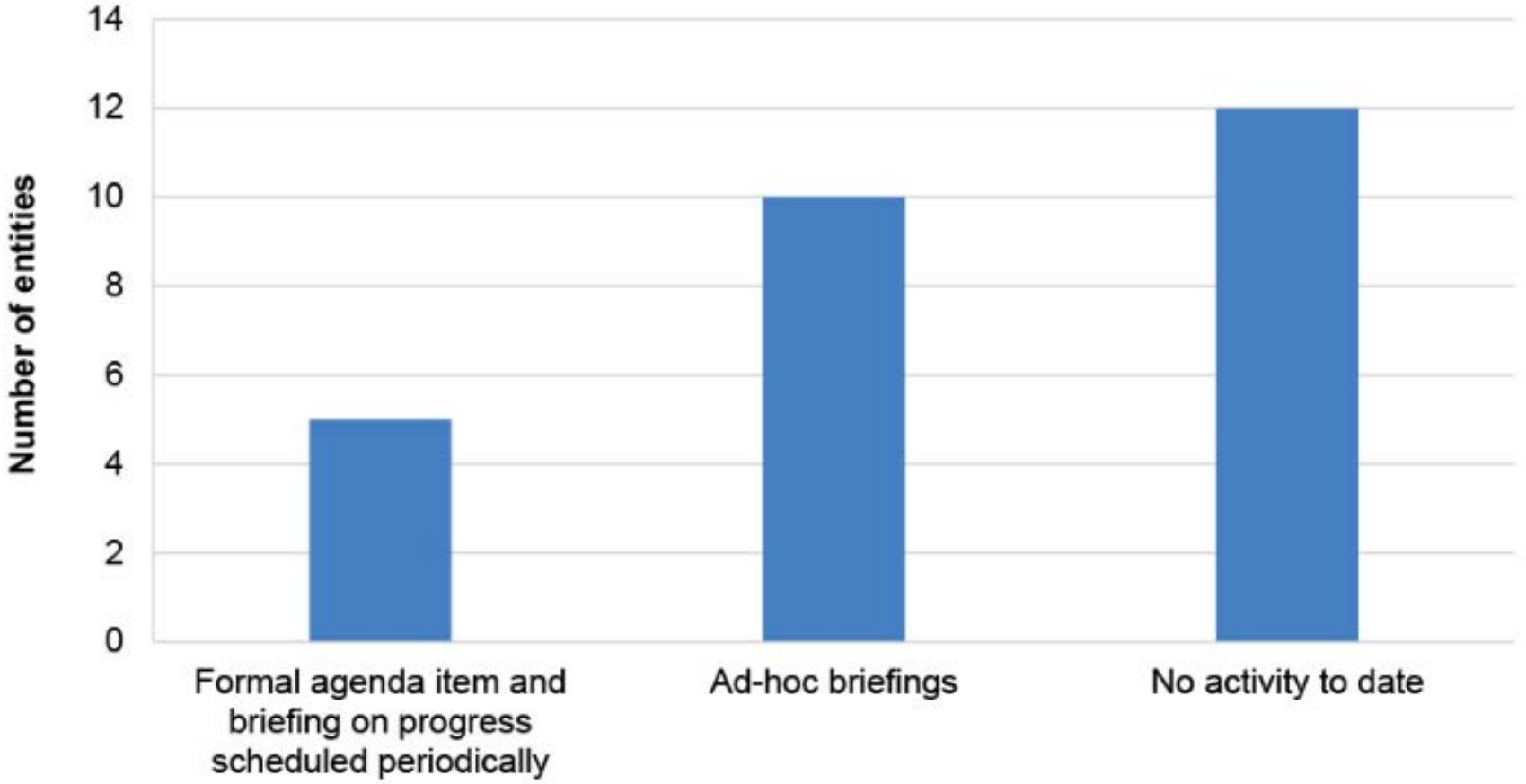
ANAO considerations - readiness

- Audit mandate
- Resources required to undertake the assurance function
- Staff capability
- Specialist expertise
- Sector readiness to report climate-related disclosures
- Market readiness –contract audit firms

Sector readiness - process and projects established by entities



Sector readiness - audit committee oversight



Performance Statements Audit Update

George Sotiropoulos

Group Executive Director
Performance Statements Audit Services Group

Insights on Cyber Security and Data Governance

Xiaoyan Lu
Acting Group Executive Director
Systems Assurance and Data Analytics Group
Australian National Audit Office

Topics

- Key messages from recently published cyber security performance audit report
- Key findings from interim controls report for financial statements audit
- Digital auditing and data acquisition

Cyber security incident management policy requirements

- The Protective Security Policy Framework (PSPF) Policies 2, 4, 5 and 10 outline the requirements for the effective management of cyber security incidents.
- Supporting the PSPF are the relevant Australian Signals Directorate (ASD) Cyber Security Guidelines as well as ASD's Essential Eight Maturity Model.
- It is mandatory for NCEs to report the level of their security maturity each financial year.

31%

of cyber security incidents reported to ASD were by Australian Government entities in 2022–23.

71%

of NCEs self-assessed at Maturity Level Two for the Essential Eight mitigation strategy, Regular backups.

82%

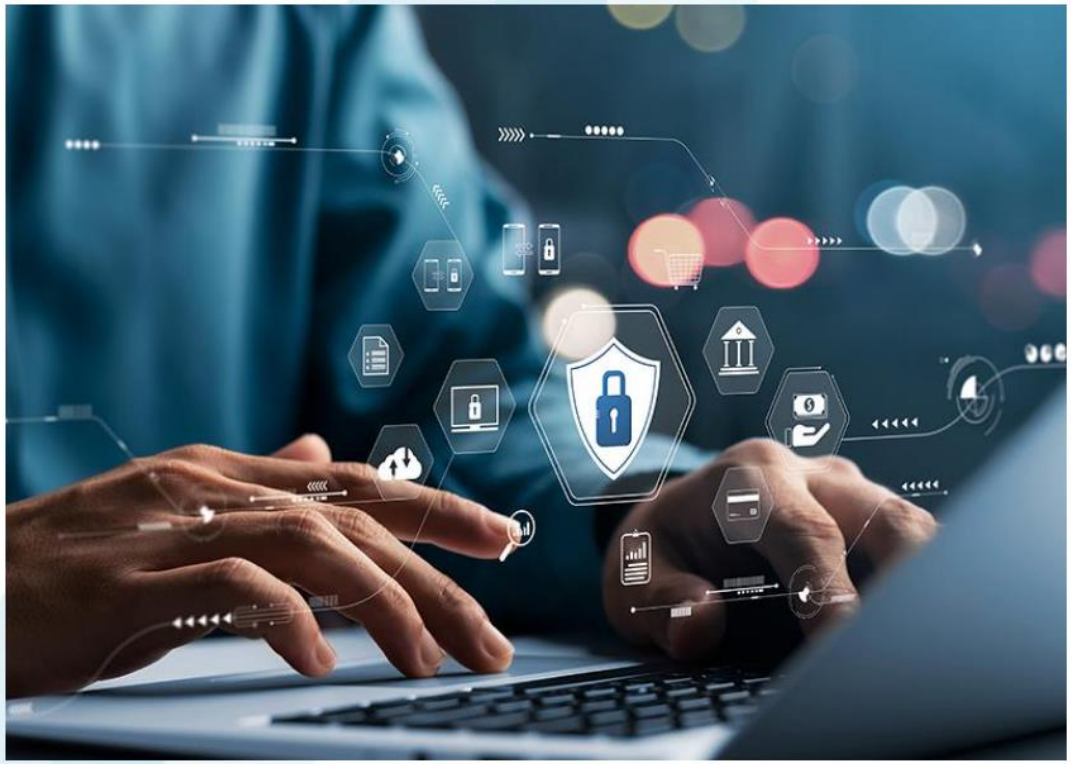
of NCEs self-assessed that they had an incident response plan in place, which was an increase from 2022.

Management of cyber security incidents performance audit

PERFORMANCE AUDIT REPORT | AUDITOR-GENERAL REPORT NO.38 OF 2023–24

Management of Cyber Security Incidents

PUBLISHED Friday 14 June 2024



Portfolio
Cross entity

Entity
Australian Transaction Reports and Analysis Centre; Services Australia

Contact
Please direct enquiries through our contact page.

Activity Governance

Sector Attorney-General's | Social Services

Audit objective and conclusion

Audit objective, criteria and scope

6. The objective of this audit was to assess the effectiveness of the selected entities' implementation of arrangements for managing cyber security incidents in accordance with the Protective Security Policy Framework (PSPF) and relevant ASD Cyber Security Guidelines.

Conclusion

11. The implementation of arrangements by AUSTRAC and Services Australia to manage cyber security incidents has been partly effective. Neither entity is well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber security incident.

Key messages from this audit for all Australian Government entities

Governance and risk management

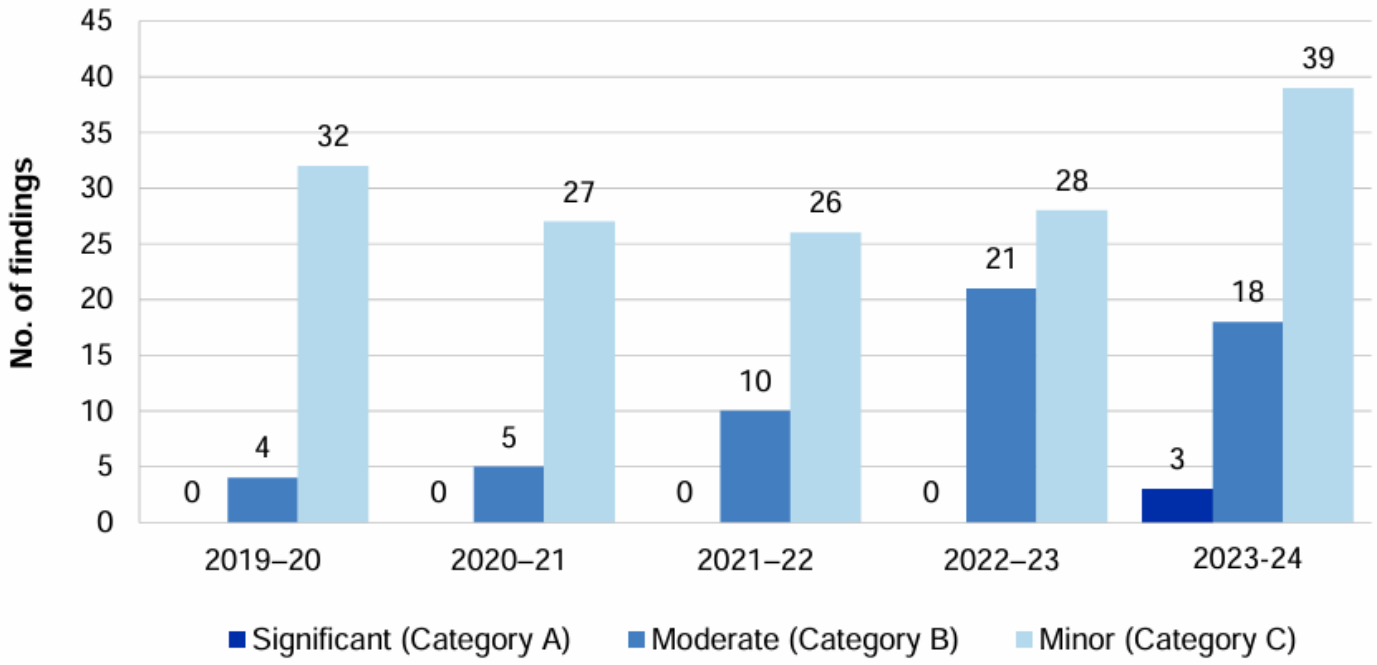
- Public services are increasingly reliant on the availability of systems. Entities should understand and assess the need for critical business continuity and disaster recovery management and frame their security documentation and processes on the basis that cyber security incidents could disrupt or shut down the delivery of digital services to the Australian public.
- Entities should document policies and procedures — which is important for managing staff turnover — particularly for smaller organisations that are critically dependent on the qualifications and experience of key security advisors.
- Entities should leverage post-incident learning to inform a process that reviews, updates and tests all security documentation for the effective management of cyber security incidents. Post-incident learning greatly improves business continuity and recovery prospects following a significant or reportable cyber security incident.
- Entities should implement a trusted insider program which would actively assist an entity to effectively detect and mitigate internal cyberattack threats.
- As Australia's cyber security regulatory landscape evolves and reforms, it is important for an entity to consider how their legal function will support their governance committees during the external reporting process to manage increasing scrutiny and liability risks following a significant or reportable cyber security incident.

Performance and impact measurement

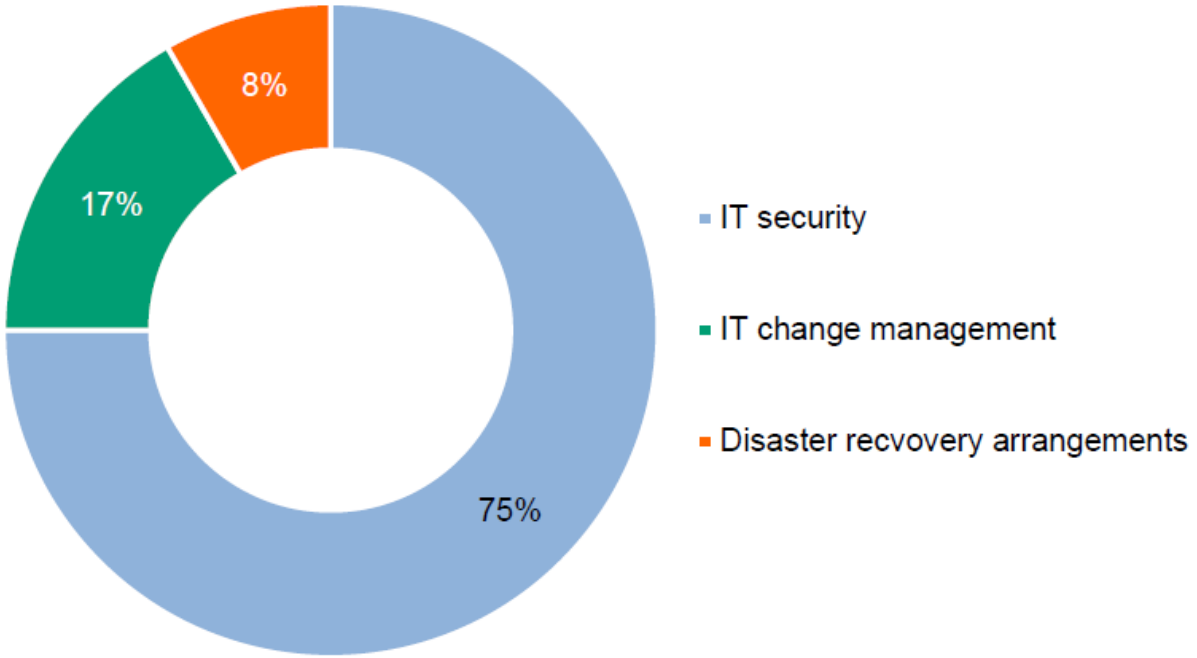
- Entities should implement a systematic and centralised approach to the management of Security Information and Event Management (SIEM) solutions, including automated monitoring and prioritisation of security alerts.

Aggregate IT audit findings for the last four years

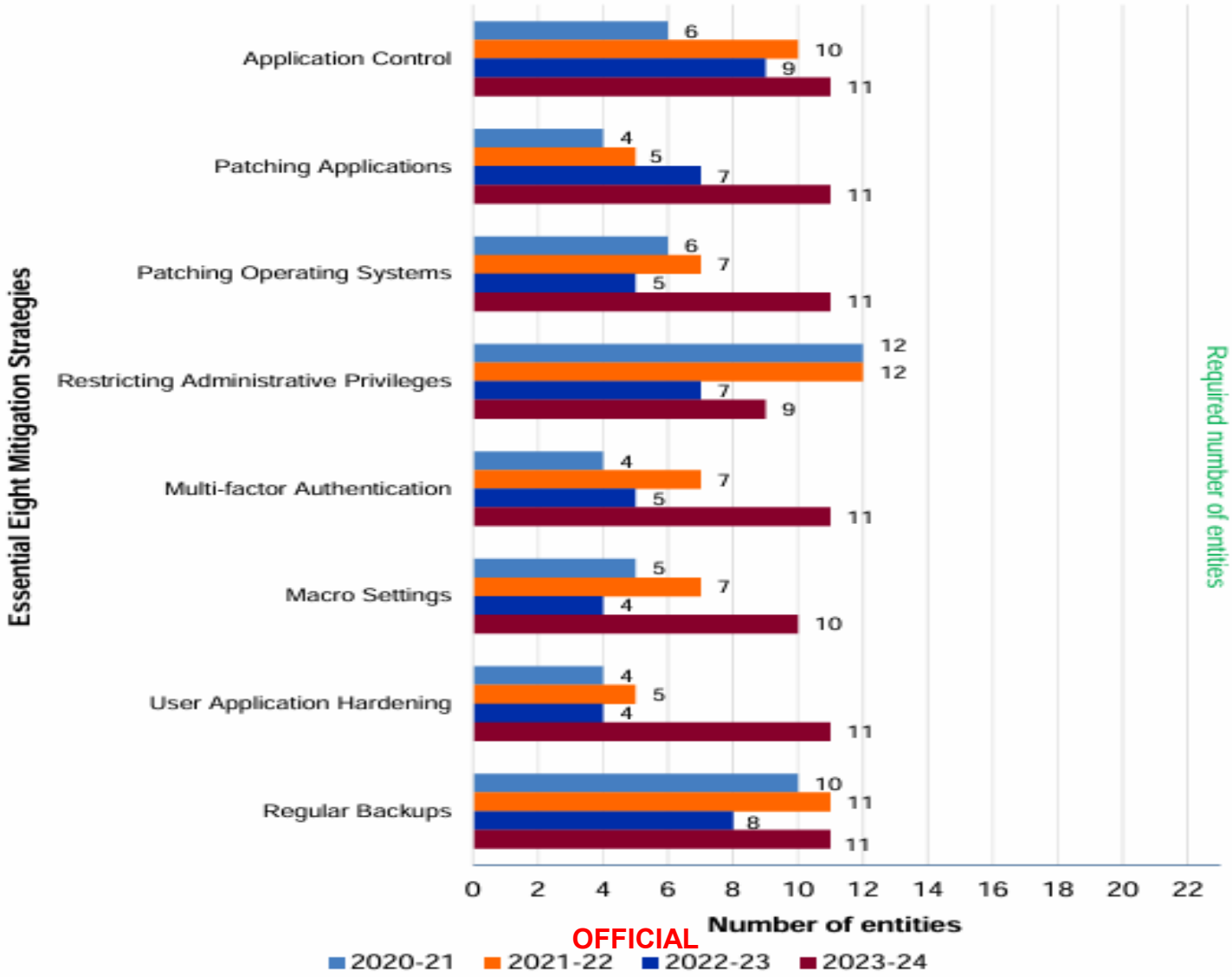
Trend in aggregate interim IT audit findings 2019-20 to 2023-24



2023-24 interim IT audit findings – by category



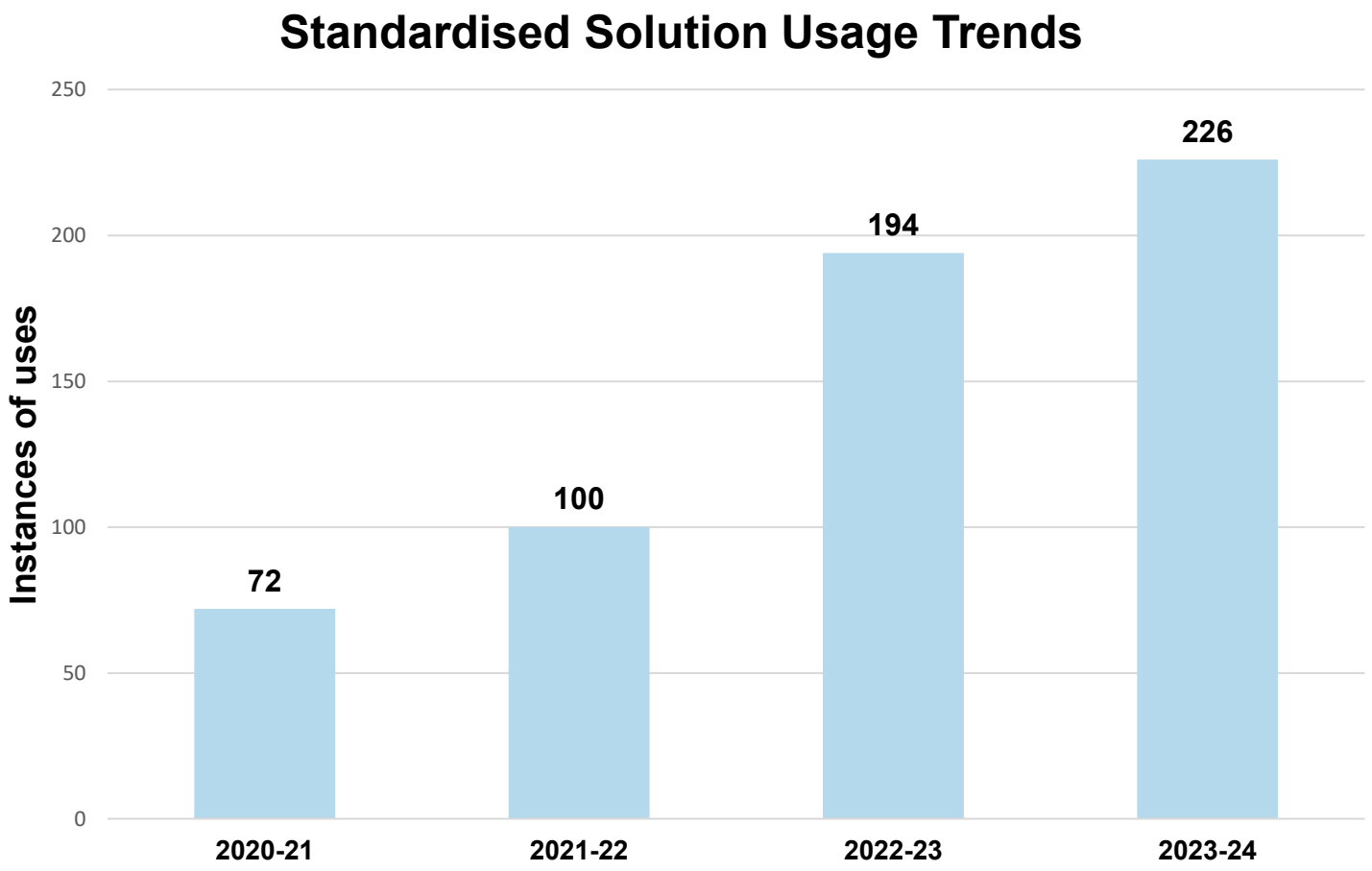
Compliance with PSPF Policy 10 requirements



Emerging technology (including AI)

- Entities are increasingly exploring emerging technologies such as AI generally.
- 36 entities advised the ANAO that they had adopted some form of emerging technology as part of the 2023-24 FSA EOY reporting.
- 27 entities adopted AI, including commercially available products, chatbots and supporting advanced data analysis.
- Of the 27 entities that adopted AI, 15 did not create policies to support their use of AI.
- The lack of governance frameworks for managing the use of emerging technologies could increase the risk of unintended consequences.

ANAO's Digital Audit Journey



Data Challenges and Our Approach

- **Challenges**
  - Lack of standardisation in data extracts.
  - Challenging data quality:
    - Completeness and accuracy.
    - Gap between requested and provided data.
- **Our approach to more efficient and effective data acquisition**
  - Working with SDO to establish streamlined process for entities using their service.
  - Implementing data extraction scripts for some core FMIS datasets (e.g. SAP). Currently implemented at Dept. of Health, Infrastructure, DFAT and AGD.
    - Current: General Ledger extraction focus
    - Future: Extraction of all required FMIS tables
  - Working with a major FMIS vendor on implementing standard reporting (TechOne).
  - Aim to improve data quality, consistency and reduce manual effort from entity and ANAO.

Performance Audit Update

Corinne Horton

A/g Group Executive Director

Performance Audit Services Group

Themes from performance audit

- The ANAO has increasingly brought into scope issues of ethics (as defined in the PGPA Act and Public Service Act), particularly where meeting mandatory requirements is not sufficient to ensure compliance with the high expectations set out in principles-based legislation and frameworks.
- The ANAO has commenced a series of performance audits based on ethics, culture and integrity in the public sector.
  - We have tabled our first performance audit that focused on integrity and ethical conduct in the APS - Auditor-General Report No. 43, *Australian Public Service Commission's Administration of Integrity Functions.*
  - In 2023-24, this has included two series of audits focused on compliance with credit card requirements and gifts, benefits and hospitality requirements.
  - As part of the 2024–25 Annual Audit Work Program the ANAO has included provision for a further series of compliance related audit topics.
- An 'Audit Lessons' product on Grants administration was published on the ANAO website in late June 2024. This lesson's product is targeted at those responsible for administering or overseeing grants programs.

Key lesson – Corporate credit cards

The misuse of corporate credit cards, whether deliberate or not, has the potential for financial losses to the Commonwealth and reputation damage to individual government entities, as well as the public sector. The robustness of controls to detect and prevent misuse of credit cards and action taken on non-compliance are indicative of an entity's culture and integrity.

Entities need to establish policies and procedures which consider their operating context and risks.	A pro-integrity culture supporting credit card compliance includes awareness through appropriate training, periodic messaging and ongoing education.	Both preventative and detective controls should be implemented in managing credit cards, with these controls being tested for effectiveness regularly.	Regular reporting within the entity, on both credit card use, and misuse, is important in providing the accountable authority with visibility of the organisation's fraud and corruption risk profile and how it may be changing over time.

Key lessons - gifts, benefits and hospitality requirements

The APS Code of Conduct requires APS employees to declare the receipt of gifts, benefits and hospitality, and section 27 of the PGPA Act requires an official to not improperly use their position to gain or seek to gain a benefit for themselves.

The creation of policies and procedures addressing the giving or receiving gifts, benefits and hospitality is not sufficient in isolation. The risks associated with giving or receiving of gifts, benefits and hospitality cannot be considered in isolation.

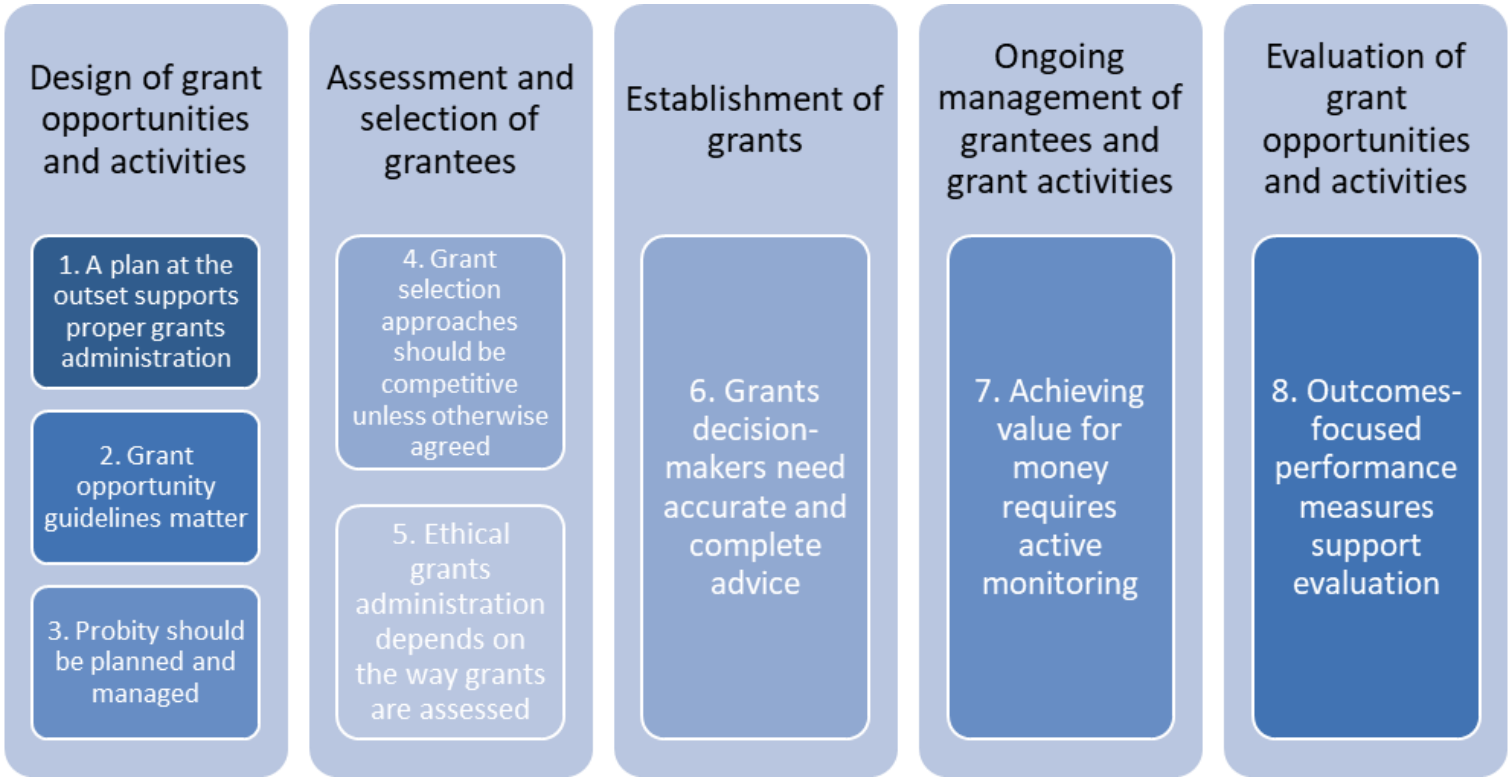
The acceptance of any gift, benefit or hospitality can create a perceived or actual conflict of interest. A decision to accept a gift, benefit or hospitality needs to consider the nature of any benefit accruing to the organisation balanced against the risk of a conflict being created..

Government entities are required to publish on their website a register of accepted gifts, benefits and hospitality. Publication of accepted items should be supported by internal reporting of not just accepted gifts, benefits and hospitality, but also offers received but not accepted.

Valuation of gifts, benefits and hospitality needs to be transparent and defensible.

Audit Lessons – Grants Administration

This edition of Audit Lessons sets out eight lessons aimed at improving grants administration across the five stages of the grants lifecycle, based on insights from ANAO performance audits over the past five years.



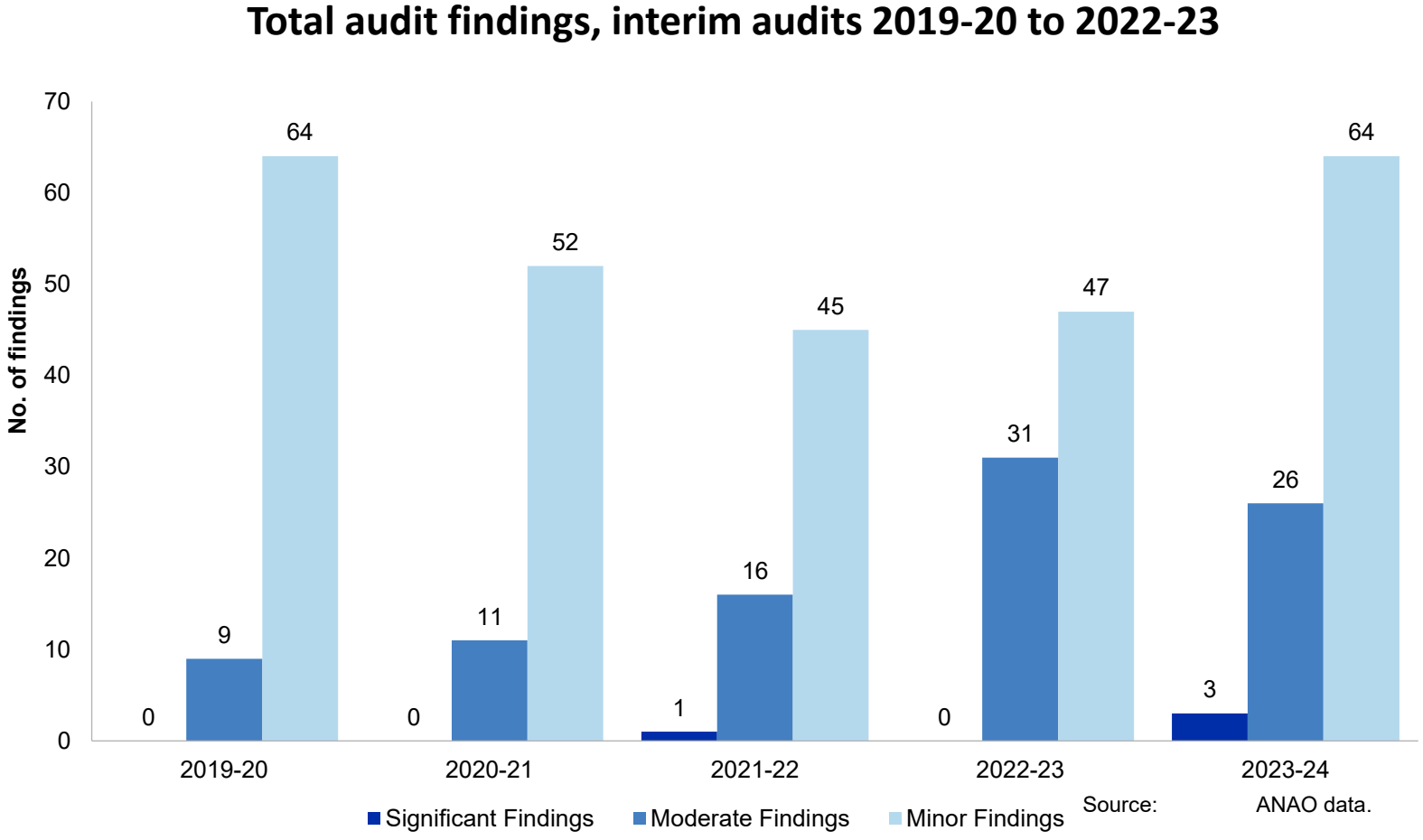
Key themes from the Interim report on key financial controls of major entities (2023–24 Financial Year)

Lesa Craswell
Acting Group Executive Director
Financial Statements Audit Services Group

Discussion Topics

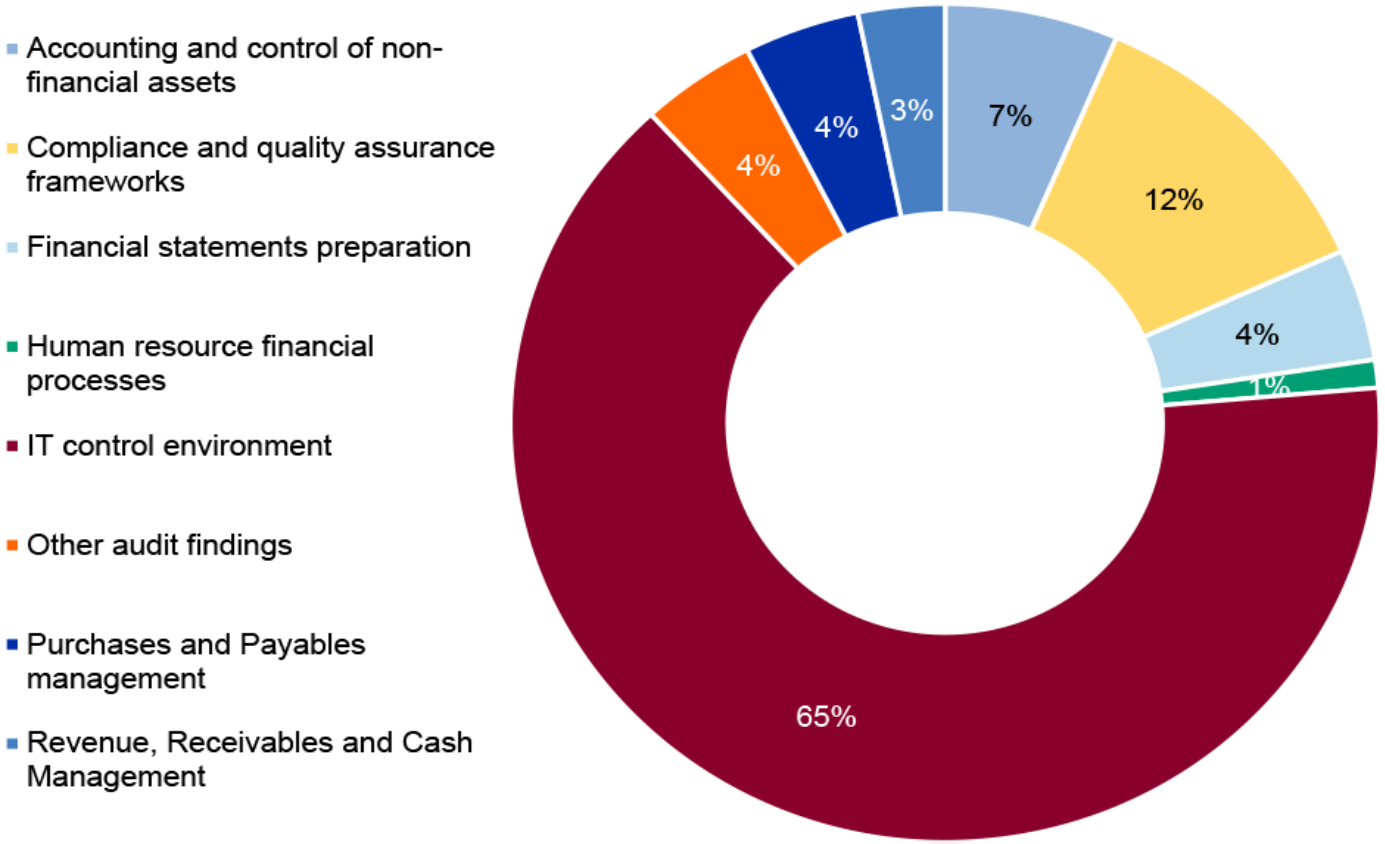
- Audit findings
- Audit committee effectiveness
- Internal audit recommendations
- Computer software
- Year end focus

Audit findings



Audit findings

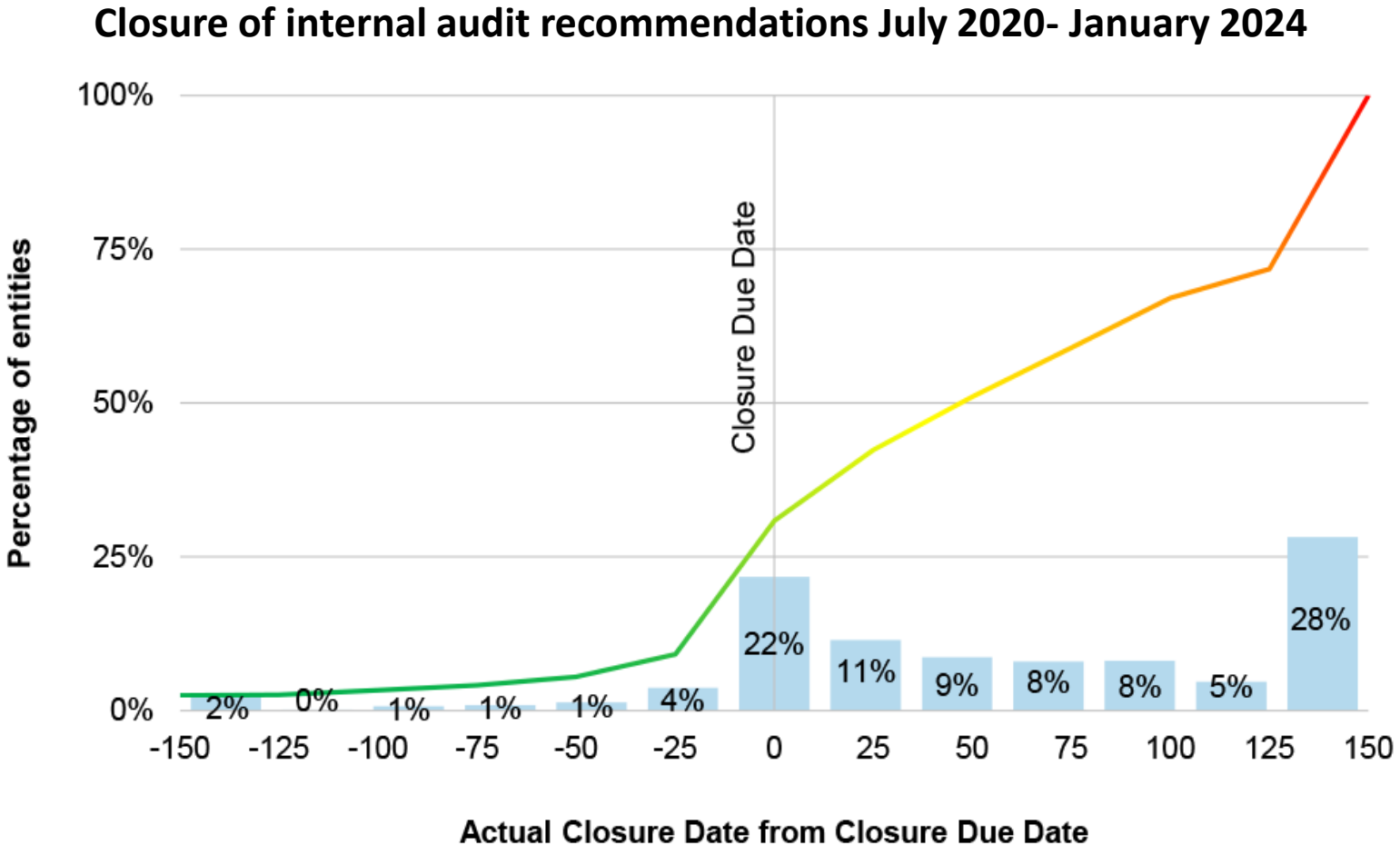
Categorisation of interim audit findings 2023-24



Audit committee effectiveness

- Audit committee performance should be regularly reviewed:
  - Seventy-seven per cent of entities had undertaken a recent review of the effectiveness of their audit committee
  - Reviews mainly relied on self-assessments of committee performance
  - Majority of reviews did not address all of the considerations highlighted in guidance provided by the Department of Finance

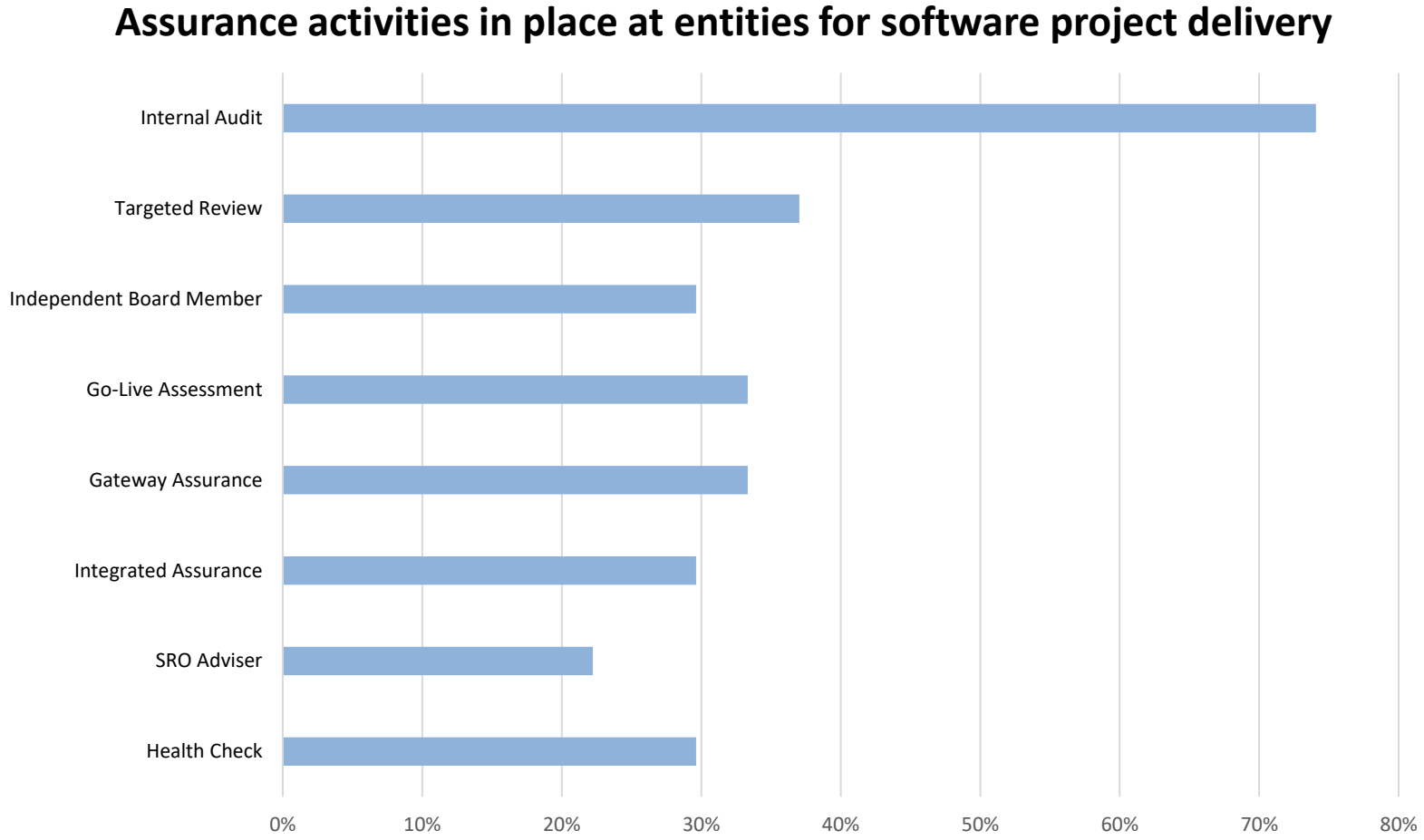
Internal audit recommendations



Computer software

- Delivery of computer software projects:
  - Twenty-five of the 27 entities had established a project management framework or policy
  - Thirteen entities did not provide reports to their audit committees on software projects
  - All entities adopted one or more of the eight project assurance processes examples advised by the Digital Transformation Agency. One assurance process, internal audit, was adopted by the majority of entities

Computer software



Year end

- Key Management Personnel calculation, compliance and disclosure
- Closing audit findings
- Quality of financial statements:
  - Financial statement workplan
  - Prepare and review workpapers
  - Quality assure the financial statements before audit
  - Keep the ANAO advised of timelines, and where agreed timelines may be at risk of change

General questions and closing remarks