8 KEY AUSTRALIAN NATIONAL AUDIT OFFICE PROTECTIVE SECURITY AUDITS 2013-2018

INDUSTRY
RISK

BACKGROUND

Structure and Contents

This summary provides details of audits conducted by the Australian National Audit Office (ANAO) and key recommendations that relate primarily to protective security.

The Summary is most relevant to Agency Security Advisers/Corporate Security Managers who manage enterprise security programs and may gain benefit from reviewing the observations and recommendations.

This summary draws from the ANAO's own website and no guarantee is given that details presented are complete, especially where audits have been omitted from the ANAO site. For example, audits details relating to credit card fraud have been excluded, among others, so as to focus on mainstream protective security functions and elements.

The intent of this summary is to provide a qualitative review of protective security audit findings by the ANAO over recent years and up until 30 May 2018.

Each audit activity conducted by the ANAO has been hyperlinked to enable easy cross-referencing with the original report.

INDUSTRY RISK

INTRODUCTION

Quick facts about the ANAO

The ANAO is a specialist public sector practice providing a full range of audit and assurance services to the Parliament and Commonwealth public sector entities and statutory bodies.

The ANAO has extensive powers of access to documents and information, and its work is governed by its auditing standards, which adopt the standards applied by the auditing profession in Australia.

The annual audit work program sets out the ANAO's strategy and deliverables for the coming year. The annual audit work program presents information on the financial statements audits and other assurance activities that will be finalised in the coming year.

Sensitive information that, in the Auditor-General's opinion, is not in the public interest will not be included in public reports. In exercising their discretion, the Auditor-General has regard to the reasons listed in section 37 of the Auditor-General Act, which include national security and international relations, Cabinet deliberations, Commonwealth-State relations and unfair prejudice to commercial interests.

Years	Security Audits Included
2017-18	3
2016-17	1
2015-16	1
2014-15	1
2013-14	2

Audit 1

Mitigating Insider Threats through Personnel Security.

Key Facts

Published: 11 May 2018.

Entity(s) Audited: Across Entities.

Objective: The objective of the audit was to assess the effectiveness of the Australian Government's personnel security arrangements for mitigating insider threats.

Link: https://www.anao.gov.au/work/performance-audit/mitigating-insider-threats-through-personnel-security

Key Recommendations

In this instance recommendations were presented as 'Key Learnings for all Australian Government Agencies'. The three learnings were grouped as follows:

Procurement:

When procuring a major ICT system that will contain sensitive information, undertaking a thorough risk assessment prior to putting the system into production provides greater assurance that information will be appropriately protected.

Governance and Risk Management:

- Separating policy and operational functions can lead to implementation challenges. If these functions need to be separate, effective oversight arrangements should be established to avoid silos emerging.
- Sometimes the risks of not sharing information are greater than the risks of sharing it. Entities should comply with privacy and information security requirements, but should not use these provisions as an excuse not to share pertinent information.

Policy/program implementation

Policy owners should provide clear, user-friendly guidance and templates that make it easy to comply with policy requirements.

INDUSTRY RISK

Audit 2

The Management of Risk by Public Sector Entities

Key Facts

Published: 15 Aug 2017.

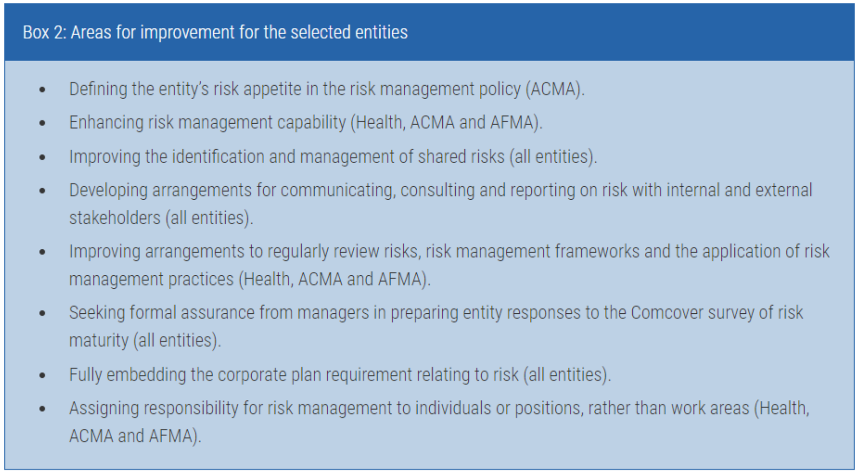
Entity(s) Audited: Department of Employment; Department of Health; Australian Communications and Media Authority; Australian Fisheries Management Authority.

Objective: The audit objective was to assess how effectively the selected public sector entities manage risk, inclusive of security-related risks.

Link: https://www.anao.gov.au/work/performance-audit/management-risk-public-sector-entities

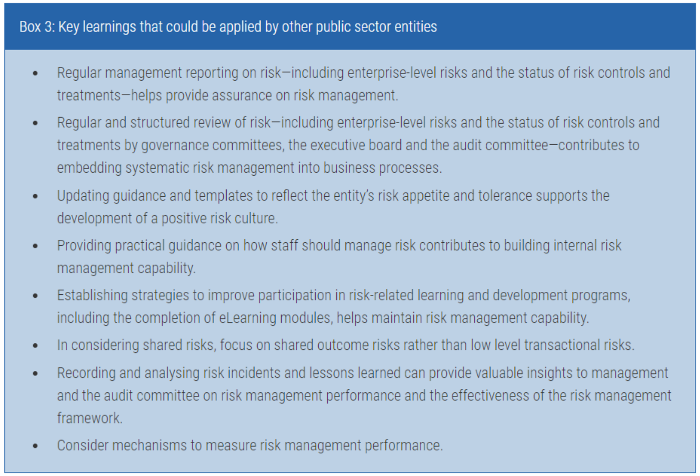
Key Recommendations

In this instance recommendations were presented as 'Areas for improvement and key learnings'. The results are presented below.



Box 2: Areas for improvement for the selected entities

- Defining the entity's risk appetite in the risk management policy (ACMA).
- Enhancing risk management capability (Health, ACMA and AFMA).
- Improving the identification and management of shared risks (all entities).
- Developing arrangements for communicating, consulting and reporting on risk with internal and external stakeholders (all entities).
- Improving arrangements to regularly review risks, risk management frameworks and the application of risk management practices (Health, ACMA and AFMA).
- Seeking formal assurance from managers in preparing entity responses to the Comcover survey of risk maturity (all entities).
- Fully embedding the corporate plan requirement relating to risk (all entities).
- Assigning responsibility for risk management to individuals or positions, rather than work areas (Health, ACMA and AFMA).



Box 3: Key learnings that could be applied by other public sector entities

- Regular management reporting on risk—including enterprise-level risks and the status of risk controls and treatments—helps provide assurance on risk management.
- Regular and structured review of risk—including enterprise-level risks and the status of risk controls and treatments by governance committees, the executive board and the audit committee—contributes to embedding systematic risk management into business processes.
- Updating guidance and templates to reflect the entity's risk appetite and tolerance supports the development of a positive risk culture.
- Providing practical guidance on how staff should manage risk contributes to building internal risk management capability.
- Establishing strategies to improve participation in risk-related learning and development programs, including the completion of eLearning modules, helps maintain risk management capability.
- In considering shared risks, focus on shared outcome risks rather than low level transactional risks.
- Recording and analysing risk incidents and lessons learned can provide valuable insights to management and the audit committee on risk management performance and the effectiveness of the risk management framework.
- Consider mechanisms to measure risk management performance.

INDUSTRY RISK

Audit 3

Protecting Australia's Missions and Staff Overseas: Follow-on.

Key Facts

Published: 8 August 2017.

Entity(s) Audited: Foreign Affairs and Trade.

Objective: The audit objective is to examine the effectiveness of measures taken to strengthen the protection of Australia's missions and staff overseas.

Link: https://www.anao.gov.au/work/performance-audit/protecting-australias-missions-and-staff-overseas-follow-on

Key Recommendations

1. The Department of Foreign Affairs and Trade develop:
   a. a strategic plan that addresses its future security needs and aligns with key activities of the department, including encompassing all the reforms and activities underway; and
   b. a detailed implementation plan for addressing the 2015 internal review recommendations, as one of the reforms captured in the strategic plan.
2. To better inform governance and oversight by the Departmental Security Committee, the Department of Foreign Affairs and Trade:
   a. develop and maintain a comprehensive database of physical and operational security measures at overseas posts; and
   b. develop a more consistent framework for assessing security risks for overseas posts.
3. The Department of Foreign Affairs and Trade develop mechanisms to provide assurance that staff receive the required security training for their posting, and to inform future planning and improvements to the security training program.
4. That the Department of Foreign Affairs and Trade enhance the coordination of the deployment of security measures to achieve greater consistency when determining security measures to be deployed to overseas posts.
5. The Department of Foreign Affairs and Trade refine a framework for risk-based selection of posts for security inspection, improve the deployment of inspection staff resources, and develop consistent standards and accountability mechanisms to enable the timely identification and resolution of security vulnerabilities at posts.
6. The Department of Foreign Affairs and Trade strengthen arrangements for managing and maintaining security measures at overseas posts to ensure the measures appropriately mitigate identified risks.
7. The Department of Foreign Affairs and Trade develop an information system to respond to security breaches, and identify trends and mitigation strategies, based on reliable and useful breach data.

INDUSTRY RISK

Audit 4

Passenger Security Screening at Domestic Airports

Key Facts

Published: 31 August 2016.

Entity(s) Audited: Department of Infrastructure and Regional Development.

Objective: The audit objective was to assess the effectiveness of the Department of Infrastructure and Regional Development's regulation of passenger security screening at Australian domestic airports.

Link: https://www.anao.gov.au/work/performance-audit/passenger-security-screening-domestic-airports

Key Recommendations

1. That, independently of other projects being conducted, the Department sets a date at which the grandfathering provisions for the 2011 passenger screening equipment requirements will cease, and amends the Aviation Screening Notices accordingly.

2. That the Department:

   a. establishes an analysis function to identify non-compliance trends based on accurate, reliable compliance activity data; and

   b. incorporates the results of the analysis into the compliance program, focusing on areas at risk of non-compliance.

3. That the Department, in consultation with stakeholders, develops performance measures for passenger screening that are practical, achievable and measurable.

4. That the Department conducts a training needs analysis for users of the regulatory management system, delivers appropriate training, and monitors its effectiveness.

5. That the Department provides targeted reporting to its stakeholders, based on accurate data, which enables an assessment of the effectiveness of passenger screening, and promotes improved passenger screening effectiveness.

Audit 5

Records Management in Health.

Key Facts

Published: 1 December 2015.

Entity(s) Audited: Department of Health.

Objective: The audit objective was to assess the effectiveness of the Department of Health's records management arrangements, including Health's progress in transitioning to digital records management.

Link: https://www.anao.gov.au/work/performance-audit/records-management-health

Key Recommendations

1. To improve the governance of information and records management, the ANAO recommends that Health develops and implements an overarching information management framework which incorporates an information and records management strategy, against which performance can be measured.

2. To place the TRIM EDRMS remediation project on a sound footing, the ANAO recommends that Health:

   a. identifies a Senior Responsible Officer (SRO) with accountability for project implementation and delivery of outcomes;

   c. establishes a governance framework to oversee implementation of the project;

   d. implements a performance reporting framework to assess progress and outcomes; and

   e. develops a risk management plan for the project, including a strategy and timeframe for shared drives to become accessible as 'read only'.

3. The ANAO recommends that Health prepares guidelines for sentencing digital records upon creation within TRIM EDRMS, and incorporates version control dates as part of its digital file titling protocols within the Business Classification System, to enable staff to more effectively sentence digital files.

4. To strengthen the management and control framework for the finalisation, deletion and destruction of records, the ANAO recommends that Health:

   a. develops criteria for the finalisation of records in TRIM EDRMS and requires staff to finalise records in accordance with the criteria; and

   b. documents files/records authorised for destruction and obtains confirmation that files/records are destroyed in accordance with the Australian Government Protective Security Policy Framework.

Audit 6

Fraud Control Arrangements.

Key Facts

Published: 30 October 2014.

Entity(s) Audited: Across Entities.

Objective: The audit objective was to examine the selected entities' effectiveness in implementing entity-wide fraud control arrangements, including compliance with the requirements of the 2011 Commonwealth Fraud Control Guidelines (2011 Guidelines), and the overall administration of the fraud control framework by the Attorney-General's Department..

Link: https://www.anao.gov.au/work/performance-audit/fraud-control-arrangements

Key Recommendations

1. To facilitate the timely preparation of the annual Fraud Against the Commonwealth Report and the annual Compliance Report to Government, the ANAO recommends that the Attorney-General's Department formalises its business arrangements with the Australian Institute of Criminology.

Audit 7

The Management of Physical Security.

Key Facts

Published: 24 June 2014.

Entity(s) Audited: Australian Crime Commission, Geoscience Australia, Royal Australian Mint.

Objective: The audit objective was to assess the effectiveness of physical security arrangements in selected Australian Government agencies, including whether applicable Australian Government requirements are being met.

Link: https://www.anao.gov.au/work/performance-audit/management-physical-security

Key Recommendations

1. To strengthen security assurance and monitoring arrangements, the ANAO recommends that agencies implement a security assurance strategy that outlines their approach to monitoring:

   - compliance with the PSPF and the agency's security policies; and
   - the ongoing effectiveness of the agency's security policies and control measures.

2. To assist agencies to adopt and maintain an effective approach to the management of physical security risks, the ANAO recommends that agencies, in the context of their discrete operating circumstances:

   - integrate security risk management activities with other organisational risk activities;
   - tailor procedures for the conduct of security risk assessments that align to the requirements of the PSPF; and
   - update security policies and plans to reflect the outcomes of security risk assessments.

Audit 8

Explosive Ordnance and Weapons Security Incident Reporting.

Key Facts

Published: 18 December 2013.

Entity(s) Audited: Department of Defence

Objective: The audit objective was to assess the effectiveness of the Department of Defence's arrangements for monitoring and reporting explosive ordnance and weapons security incidents.

Link: https://www.anao.gov.au/work/performance-audit/explosive-ordnance-and-weapons-security-incident-reporting

Key Recommendations

1. To facilitate timely and complete explosive ordnance and weapons security incident reporting, the ANAO recommends that Defence streamline reporting requirements and improve arrangements to coordinate the dissemination of the information reported to relevant Defence stakeholders.

2. To further contribute to Defence's visibility over explosive ordnance security incidents and account for items recovered, the ANAO recommends that Defence establish a formal reporting and acquittal process for explosive ordnance handed in during amnesties.

INDUSTRY RISK

CONCLUSION

There's a lot to be learned from observing the scrutiny of others. This is very much the case in protective security, where recommendations made in similar contexts can be of use in benchmarking and validation in general.

Taken in concert with the significant amount of related material that can be found on the ANAO website, this summary is considered useful for those managing security programs, especially by those in the government sector.

Industry Risk hopes that this summary has been of use to readers.

RAISING AUSTRALIAN SECURITY &
BUSINESS RESILIENCE TO NEW HEIGHTS

Leverage our security threat, risk & compliance expertise.
Take comfort in our crisis, continuity & emergency management prowess.

Level 40 Northpoint Tower
100 Miller St
NORTH SYDNEY NSW 2060

Phone: 1300 299 484
Fax: 02 8078 6999
Email: info@industryrisk.com.au

INDUSTRY
RISK