

For Official Use Only

BRIEF FOR SECRETARY/CDF: Proposals for an optimal system of assurance and audit
(Re-think of Defence's systems of inquiry, investigation, review and audit)

Group: **OSCDF**Reference: **AFCD/OUT/CAE/2014/32**Due Date: **25 February 2014****EXECUTIVE SUPPORT UNIT****20 FEB 2014***SEC/IN/2014/212***Recommendation**

That you:

- (a) **Note** the key issues identified proposals for an optimal system of audit arising from consultation on an optimal system of audit (at Attachment 1); and
- (b) **Refer** them for incorporation into the First Principles Review of Defence.

Background

1. In March 2013, following the first stage of the re-think of Defence's systems of inquiry, investigation, review and audit, you asked the CAE to consult with all Groups and Services on possible models for an optimal system of audit. A consultation paper was circulated in October 2013, and the CAE met with all Group Heads and Service Chiefs in November and December 2013. The outcomes are consolidated at Attachment 1 and provided for your consideration, including proposals for an optimal system of assurance and audit.

Outcomes of the consultation

2. Groups and Services expressed very strong support for an independent Internal Audit function in Defence. The majority saw Internal Audit as helping them achieve Defence's strategic goals. Groups and Services agreed that annual risk and assurance mapping would be useful and would improve Defence's risk management culture.
3. Groups and Services also expressed a preference for the appointment of a Chief Risk Officer responsible to the Chief Operating Officer. While the role of the Chief Risk Officer is not yet determined, it could potentially include responsibility for overseeing Groups and Services' annual mapping of risks and associated assurance activities.

Issues

4. The findings reflect certain problems that arise from Defence's federated model. Audit and assurance activities are spread across the Groups and Services, such that the total cost is much higher than would be expected when compared to other organisations of similar size. The audit function of Audit and Fraud Control Division accounts for 45 staff with a personnel budget less than \$6 million and an operating budget of under \$2 million, out of a total of at least 400 FTE audit and/or assurance positions across Defence costing more than \$47 million per year.
 - The high total staff numbers is due, in part, to the practice of assigning the title of audit or assurance to staff performing the ordinary checks and balances of good administration.

- It may also reflect line managers' applying additional resources to oversee business activities of which they have limited visibility (eg: inventory) and/or experience and knowledge (eg: fuel management).
 - There is limited quality control over the processes followed, the standards applied and the competencies of those performing the work, with the consequent risk of over-estimating the resulting assurances.
 - There is overlap and duplication of assurance activities.
5. Best practice in other public sector and commercial entities is for the internal audit area to undertake all audit and assurance activities, independent of line management. In Defence this is not the case: there is a very strong desire for line management to retain their existing audit and assurance activities.

Consultation

6. The CAE consulted the COO on 13 February 2014. COO strongly supported the findings and suggested that they be referred to the First Principles Review of Defence, as they addressed issues of organisational design and governance.

Geoffrey Brown Chief Audit Executive Tel: (02) 6266 4210 M: 0419 429 607 19 February 2014		(a) Noted / Please discuss (b) Agreed / Not agreed Dennis Richardson Secretary 28 February 2014	(a) Noted / Please discuss (b) Agreed / Not agreed D. J. HURLEY, AC, DSC GEN CDF 16 Mar 14
Branch Head	Ms Dianne Leak	W: (02) 6266 4204	Mob: 0420 979 183
Action Officer	Mr Kim Bond	W: (02) 6266 3218	Mob: 0467 767 110

Attachments

1. Proposals for an optimal system of assurance and audit, February 2014.

**Re-thinking systems of inquiry,
investigation, review and audit in Defence**

**Proposals for an optimal
system of assurance and
audit**

February 2014

for the Secretary and Chief of the Defence Force

What We Did

In December 2011, the former Secretary requested that, as part of a broader review of investigations and legal proceedings, I should look into Internal Audit and Assurance processes across Defence. I surveyed the extent and cost of internal audit and assurance processes across Defence, and studied those processes in larger private sector and public sector organisations. The results were presented to you in March 2013. You requested a second phase of review and, in October 2013, I circulated a paper to all Groups and Services on possible models for an optimal system of audit. Face-to-face meetings with all Group Heads and Service Chiefs followed in November and December 2013.

What we found

There is very strong support for an independent Internal Audit function in Defence. Groups and Services also expressed support for internal audit as an enabling function, helping them achieve Defence's strategic goals.

We found that audit and assurance activities are spread across a number of Groups and Services. The audit function of Audit and Fraud Control Division accounts for 45 staff with a personnel budget less than \$6 million and an operating budget of under \$2 million, out of a total of at least 400 FTE audit and/or assurance positions across Defence costing more than \$47 million per year.

The total cost is much higher than would be expected when compared to other organisations of similar size. It reflects overlap and duplication, as well as the practice of assigning the title of audit or assurance to the ordinary checks and balances of good administration by line areas.

Best practice in other public sector and commercial entities is for the internal audit area to undertake all audit and assurance activities, independent of line management. In Defence this is not the case: there is a very strong desire for line management to retain their existing audit and assurance activities.

So what?

Line management may be devolving their responsibility for ensuring risks are identified and properly managed to their own internal audit and assurance activities.

Defence is likely to be spending significantly more than is needed on audit and assurance activities. These activities are not coordinated or coherent. There is duplication of effort, 'over-auditing', inefficiency, and higher-than-required costs. We do not clearly know which staff are auditing and which are simply administering the ordinary checks and balances of good administration. At a time when improving efficiency and productivity is paramount, we continue to invest resources to perform compliance tasks that can and should be integral to and performed by line management.

There is limited quality control over the processes followed, the standards applied and the competencies of those performing audit and assurance work in Defence. Line management may be over-valuing the assurances they derive from that work.

What now?

To improve quality and consistency and to improve the Department's efficiency and productivity, I recommend, the progressive centralisation of all audit-like activity under the direct supervision of the Chief Audit Executive (CAE). The Chief Operating Officer (COO), Chief Finance Officer (CFO) and Deputy Secretary Support and Reform (DSSR) all support this. In making this recommendation, I acknowledge that line management must continue to have the authority to request investigations and reviews of the governance of their organisations, using whoever they feel is best suited. I would however add the caveat that this should occur in consultation with the CAE.

There is broader support for an independent CAE in charge of Defence's audit and assurance job family, responsible for its professional development and standards.

To better apply our scarce resources to our risks, I recommend that each year all Groups and Services map their risks and their assurance processes over those risks. All Groups and Services support this action. Through it, we can better align Defence's assurance activities with its risks, detect overlaps or gaps in assurance, and improve the coordination of audit and assurance activities. We can identify line managers' routine checks and balances, and distinguish them from audit-like functions that are to come under CAE supervision.

All Groups and Services support the appointment of a Chief Risk Officer to improve Defence's risk management culture. I recommend that the Chief Risk Officer oversee the Enterprise Risk Framework, and coordinate Groups and Services' risk and assurance mapping. The CAE would be available to advise and to test the assurance arrangements in place to manage the risks.

Background and purpose

Defence is re-thinking its systems of inquiry, investigation, review and audit. The aim is to develop models for optimal systems that will function in a clear, decisive and coordinated manner.¹

The review of audit and audit-like activities commenced in November 2012 with a survey of all Groups and Services to obtain quantitative data on all audit and audit-like activity, along with the quantum of resources applied to those activities. That survey found that, as of March 2013, Defence's audit and audit-like activities involved 419 full time personnel, at a total estimated cost of \$47 million per annum, including the \$8 million and 45 audit staff under the direct control and supervision of the CAE. Data from the Institute of Internal Auditors (IIA) and from private and public sector organisations indicated that, even allowing for size, Defence's total audit and assurance costs were considerably above those expected for similar organisations of similar size and complexity.

Even allowing for size, Defence's total audit and assurance costs were considerably above those expected for similar organisations of similar size and complexity.

However, opportunities for achieving more efficient and effective arrangements were difficult to identify. There is a widespread practice in Defence of assigning the title of audit or assurance to the work of administering the ordinary checks and balances of good administration. The November 2012 survey identified a particular need for further work to distinguish audit and assurance activities from managers' ordinary administration and monitoring of controls over the execution of their duties.

There is a widespread practice in Defence of assigning the title of audit or assurance to the work of administering the ordinary checks and balances of good administration.

As a result of this observation, CAE commenced work with People Group to better delineate the audit and assurance job family, in conjunction with a project undertaken separately by the Chief Joint Logistics (CJLOG) who sought assistance from CAE to assess the status of the Logistics Assurance activities put in place in 2006, to address serious deficiencies in the control of inventory.

These activities coincided with the Secretary and CDF commissioning CAE to consult with all Groups and Services on possible models for an optimal system of audit. A consultation paper canvassing possible systems of audit was circulated for comment in October 2013.² Face-to-face meetings with all Group Heads and Service Chiefs followed during November and December 2013.

¹ See Information Defgram No. 342/2012, 24 May 2012.

² Review of audit and audit-like systems in Defence, *Report on Stage B (Possible models for an optimal system of audit)*, May 2013, approved by the Secretary and CDF for consultation in September 2013.

Outcomes of consultations

There was unanimous agreement that audit was essential to fostering a culture of accountability, with the CAE identified as the logical principal adviser to the Secretary and CDF on audit and assurance. There was strong support for the role of the CAE independent of line management.

There was strong support for the role of the CAE independent of line management.

To support the CAE discharge duties, Groups and Services envisaged Defence Audit as a centre of audit and assurance expertise and excellence, expressing a preference to maintain the function 'in-house' supplemented by co-sourced commercial audit partners.

Groups and Services expressed strong support for audit as an enabling function, able to identify and advise on the treatment of risks that might otherwise defeat or diminish the achievement of Defence's strategic outcomes.

There was also agreement to proposed steps to complement the role of audit by:

- each Group and Service mapping their assurance activities for their key business processes and risks; and
- Defence establishing a Chief Risk Officer as an essential step toward a more strategic risk-management culture.

Groups and Services expressed strong support for audit as an enabling function, for mapping their risks and assurance activities, and for establishing a Chief Risk Officer.

There was acknowledgement that, to ensure the quality and consistency of audit and assurance activities, the CAE was best-placed to take responsibility for the audit and assurance job family. This included establishing and monitoring audit and assurance work standards and practices, and to defining the scope of audit and assurance activities.

There was acknowledgement that...the CAE was best-placed to take responsibility for the audit and assurance job family.

Best practice in other public sector and commercial entities is for the internal audit area to undertake almost all audit and assurance activities, independent of line management. In Defence this is not the case as the majority of audit and assurance personnel are not independent of line management. Consultation identified significant management quality assurance activities³ undertaken separately from Defence Audit, including:

- technical regulation (such as for airworthiness and seaworthiness) to inform line management of the safety and reliability of critical systems;
- DMO's management quality assurance processes directed at monitoring and maintaining ISO9000 certification;

³ These activities include 'management monitoring, evaluations, quality assurance and control self-assessment arrangements that are all designed to provide confidence and assurance to Chief Executives that management is meeting its responsibilities and the entity is achieving its objectives.' See ANAO *Public Sector Internal Audit: Better Practice Guide*, page 1.

- Army Compliance and Assurance Agency (ACAA) activities that inform the Chief of Army, through the Adjutant-General, of Army's compliance with relevant policy and legislation, including on matters of technical regulation and work health safety; and
- Logistics Compliance and Assurance activities that inform Joint Logistics Command of the accuracy and reliability of records of inventory.

It is a very strong desire of line management to retain their existing assurance activities.

These assurance activities are mainly regulatory in nature, providing compliance assurance and reporting to support line management. They comprise a first line of defence (as shown in Figure 1 overleaf), defining risks and implementing controls to manage those risks. A second line of defence is provided by the assurance activities of other functional areas, such as those responsible for finance and personnel. The third line of defence is provided by Defence Audit, which provides assurance that strategies exist to mitigate risks to the achievement of Defence's strategic objectives. Over the longer term, it is highly desirable that, where these assurance activities include component audit functions, those components come under the supervision of the CAE.

It is highly desirable that the audit components of these assurance activities progressively come under the supervision of the CAE.

The 3 Lines of Defence

Where does Internal Audit stand?

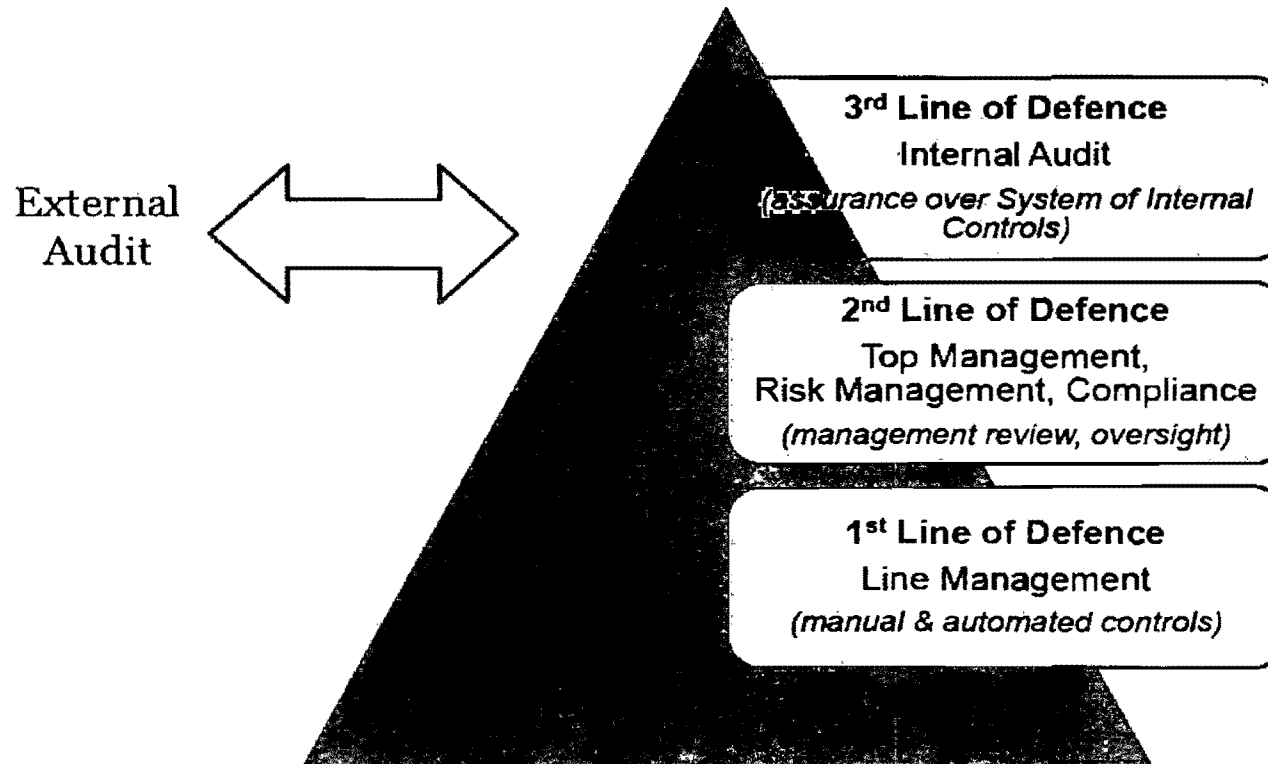


Figure 1 –Three Lines of Defence Model

The role of the Defence Chief Audit Executive

Defence CAE is uniquely positioned to provide independent and objective review and advisory services to the Secretary, CDF and the Chief Executive Officer of the Defence Materiel Organisation (CEO DMO). The CAE reports directly to the Secretary and CDF on matters of audit and risk, with administrative support for the audit function managed separately through the COO.⁴

The CAE has regular access to the Secretary, CDF and the chairs of the Defence Audit and Risk Committee (DARC) and the Materiel Audit and Risk Committee (MARC), so that serious issues of risk and exposure can be raised and acted upon. This includes the CAE meeting privately with the DARC Chair and other committee members to allow a discussion on critical areas of risk or control weakness without management being present. The CAE also meets regularly with the Auditor-General for Australia to keep abreast of broader developments in the public sector. These practices support the independent role of internal audit and the continuing effectiveness of the audit function, including follow-up and action on audit and assurance findings and recommendations.

The CAE is uniquely positioned to provide independent and objective review and advisory services.

The CAE is supported by Defence Audit, which has evolved from assurance and compliance checking to a focus on the risks to Defence achieving its strategic objectives by assessing the efficiency and effectiveness of systems for risk mitigation and internal control. Defence Audit provides:

...Defence executive management, and the Defence Audit and Risk Committee (DARC), with an objective assessment of the adequacy of processes and procedures employed by management to both identify and manage risk. In addition, Audit Branch provides assurance to the Secretary, CDF and to a lesser extent, CEO DMO that the financial and operational controls designed to manage those risks are operating efficiently, effectively and ethically. Audit facilitates these objectives through reports that are prepared for management at the conclusion of each audit which include recommendations to address controls weaknesses or that identify improvement opportunities.⁵

Defence Audit provides the specialist audit and assurance skills and knowledge to support the CAE acquit the role of improving Defence's business performance, particularly in a resource-constrained environment. In addition, Defence Audit has unrestricted access to staff, facilities and records as appropriate, by virtue of Defence Chief Executive Instruction (CEI) 4.4 and the CAE Joint Directive signed by the Secretary, CDF and CEO DMO providing Defence Audit staff with:

⁴ This is consistent with the ANAO's better practice guideline that 'Chief Executives may choose to delegate administrative responsibility for internal audit. Where this occurs, it is better practice to ensure that the delegate is a senior manager of the entity.' See XXX page VV

⁵ Defence Audit Branch website.

full, free and unrestricted access to all necessary records, assets and personnel and premises to fully discharge their responsibilities.

Defence Audit provides the specialist audit and assurance skills and knowledge to support the CAE.

Organisationally, Defence Audit's independence of line management and unique access powers distinguish it from other Defence assurance activities. This is consistent with better practice and is essential to effectively manage the audit risk that assurance opinions are poorly formed or unsubstantiated. The consultation process highlighted that the management of this risk would be markedly improved if Audit's access was complemented by Groups and Services informing the CAE of significant review and assurance activities, including consulting on proposals to establish dedicated assurance teams to respond to significant realised risks.

Under the proposed optimal system of audit:

- the CAE will continue to report directly to the Secretary, CDF and the CEO DMO on matters of audit and risk;
- the CAE will continue to report to the Secretary and the Defence Committee on progress in implementing audit recommendations, including those overdue;
- the CAE will work with Defence business areas to support management assurance and compliance functions, and to manage audit risk by deploying Defence Audit teams through the rolling audit work plan; and
- all significant management assurance and review activities undertaken or commissioned by Defence business areas would be notified to the relevant Group Head or Service Chief, the CAE and the Chief Risk Officer prior to their commencement, particularly where dedicated assurance teams are proposed to be established, or where the proposed assurance activity examines the economy, effectiveness and efficiency of activities (including regulatory and compliance activities).

Audit risk would be reduced if all Groups and Services informed the CAE of significant review and assurance activities, prior to their commencement.

Audit and assurance standards and skills

The CAE is responsible for ensuring that Defence Audit staff are appropriately trained and qualified to conduct assurance activities, with appropriate qualifications, experience and competence to undertake tasks approved by the DARC or assigned by the Secretary and CDF. Where specialist skills are not available internally, the CAE obtains them either through the outsource service provider or specialist contracted service providers.

The CAE is responsible for ensuring that Defence Audit staff are appropriately trained and qualified

The CAE is responsible for the audit and assurance job family in Defence, and is currently settling the definitions for the job family, along with the learning and development requirements for each level of assurance officer. Consultation revealed strong support for these steps, which will distinguish audit and assurance from regulatory and management assurance functions, and will be completed by July 2014.

Defence Audit conducts its assurance activities in accordance with the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA). The most recent 'External Quality Assessment' of Defence internal audit conducted for the DARC in 2011 by Ernst and Young concluded that Defence internal audit is compliant with the standards.

Defence Audit carries out its work in accordance with established standards.

Simultaneously with developing options for an optimal system of audit, Defence Audit has supplemented the IIA framework by adopting additional relevant standards issued by the Australian Government Auditing and Assurance Standards Board⁶ (AASB) including:

- ASAE 3000 – Assurance Engagements other than Audits or Reviews of Historical Financial Information;
- ASAE 3100 – Compliance Engagements; and
- ASAE 3500 – Performance Engagements.

The standards address fundamental professional requirements (independence, objectivity, proficiency and due professional care) and the five key steps of the assurance process (planning and conducting assurance engagements; setting objectives, scope and assurance criteria; collecting evidence; undertaking and documenting analysis; and reporting.)

Financial assurance activities continue to be governed by the relevant AASB audit standards, and ICT audits by standards promulgated by ISACA (formerly the Information Systems Audit and Control Association).

The CAE has adopted a rolling program of assurance activities able to respond flexibly to address emerging risks and tailored to provide appropriate levels of assurance in accordance with the standards. Defence Audit assurance services include reviews and compliance audits, as well as performance audits.

The CAE has adopted a rolling program of assurance activities, able to respond flexibly to address emerging risks.

Under the proposed optimal system of audit, the CAE would be responsible for:

- the development and maintenance of the Defence audit and assurance job family, including learning and development profiles;

⁶ Under the authority of section 227B of the *Australian Securities and Investments Commission Act 2001*.

- the setting of audit and assurance standards, in accordance with Australian government standards and industry best-practice;
- defining the scope of audit and assurance activities;
- maintaining a risk-based rolling program of assurance activities; and
- monitoring audit and assurance work standards.

Risk management culture and assurance mapping

Defence's risk management culture continues to evolve through multiple avenues, including through the development of the Defence Annual Plan, quarterly reporting against the plan, and the development of the Enterprise Risk Management (ERM) framework. Responsibility for both these functions lies with the COO.

Consultation revealed a preference for appointing a Chief Risk Officer responsible to the COO. It would be a senior appointment, working closely with the CAE to provide assurance to the Chief Executive (generally through the Audit Committee) that appropriate risk management arrangements are in place and operating effectively.

Accordingly, Defence Audit has adopted the Defence Enterprise Risk framework to inform its work program, ensuring that assurance tasks address areas of key risk at the enterprise level. Close liaison between a Chief Risk Officer and the CAE would facilitate the review of line management's risk assessments and the associated risk mitigation controls and actions.

Consultation revealed a preference for appointing a Chief Risk Officer responsible to the COO.

Consultation also revealed continuing concern that effective risk mapping at Group and Service level remained an area of weakness.⁷ The intention of risk and assurance mapping is to identify all risks and ensure that appropriate controls are in place and operating effectively to manage the risks. While the risk and assurance maps developed by DMO are worthy of consideration for broader implementation across Defence, Groups and Services are concerned by the quantum of work and the expertise required to deliver effective outcomes. However, until risks are mapped and controlled, duplication of effort (including by Defence Audit) is likely to continue, gaps in assurance activities will persist, and failures in control will not be addressed in a timely fashion.

Until risks are mapped and controlled, duplication of effort (including by Defence Audit) is likely to continue.

While, ideally, risk and assurance mapping would occur independently of the internal audit function, there may be merit in Defence Audit becoming an active partner with Groups and Services to progressively implement Risk and Assurance Maps.

⁷ Mapping of fraud related risk is achieved through the Defence Fraud Control Plan (currently at Version 10). However, outside the DMO there is no comprehensive mapping of Group/Service risks and associated assurance strategies.

Under the proposed optimal system of audit:

- a Chief Risk Officer would be appointed in a senior role, responsible to the COO;
- CAE, in consultation with the Chief Risk Officer, would assist Groups and Services progressively develop risk and assurance maps to effectively and efficiently address identified risks;
- the Chief Risk Officer and CAE would ensure the alignment of assurance activities with enterprise risks; and
- the Chief Risk Officer and CAE would work closely to ensure that appropriate risk management arrangements were in place and operating effectively.

Chief Risk Officer and CAE would work closely to ensure that appropriate risk management arrangements were in place and operating effectively.