ARMY COMMAND STANDING ORDER

NO 9001

THE ARMY POLICY FOR AUDIT AND INSPECTION

ISSUED JULY 2017

Sponsored By:

Authorised By:

The Army Inspector

Deputy Chief of the General Staff

ARMY COMMAND STANDING ORDER NO 9001
(FIRST REVISE)

THE ARMY POLICY FOR AUDIT AND INSPECTION (A&I)

Context

1.   The statutory, regulatory and policy environment in which the Army lives, trains and operates is increasingly demanding, as is the level of external scrutiny of Army activity. Commanders need to know that they have achieved their objectives and have done so whilst complying with and conforming to the regulations and policies relevant to those objectives. The challenge is, therefore, to ensure that the Army's operating environment does not stifle Commanders and accepts that there will always be some risk; it should minimise the burden on those charged with delivering the Army's outputs *whilst maintaining the appropriate levels of safety and assurance.*

2.   Defence defines assurance as 'an evaluated opinion, based on evidence gained from review, on an organisation's governance, risk management and internal control framework.'[1] For the Army, the assurance function allows ECAB to understand the ongoing level of risk to the delivery of the Army's outputs, the lives of its soldiers and its reputation. This understanding is drawn from a broad network across the Army whose daily business includes an assurance function. It involves, amongst others, the chain of command from bottom to top, Army Competent Advisers and Inspectorates (ACAIs), discrete A&I teams and, operating independently to ECAB, the Army Inspector. An effective assurance mechanism allows the Army to demonstrate that it is 'doing the right things and doing them properly'.

3.   This assurance 'network' – the Army's Assurance Framework – is shown schematically at Figure 1, below. It illustrates the new assurance taxonomy and the division between the 1st, 2nd, 3rd and 4th Lines of Defence Assurance[2], allowing a spectrum of activity from unit level to 4 Headquarters and beyond to external inspection teams. This activity confirms compliance with statute, policy or direction.
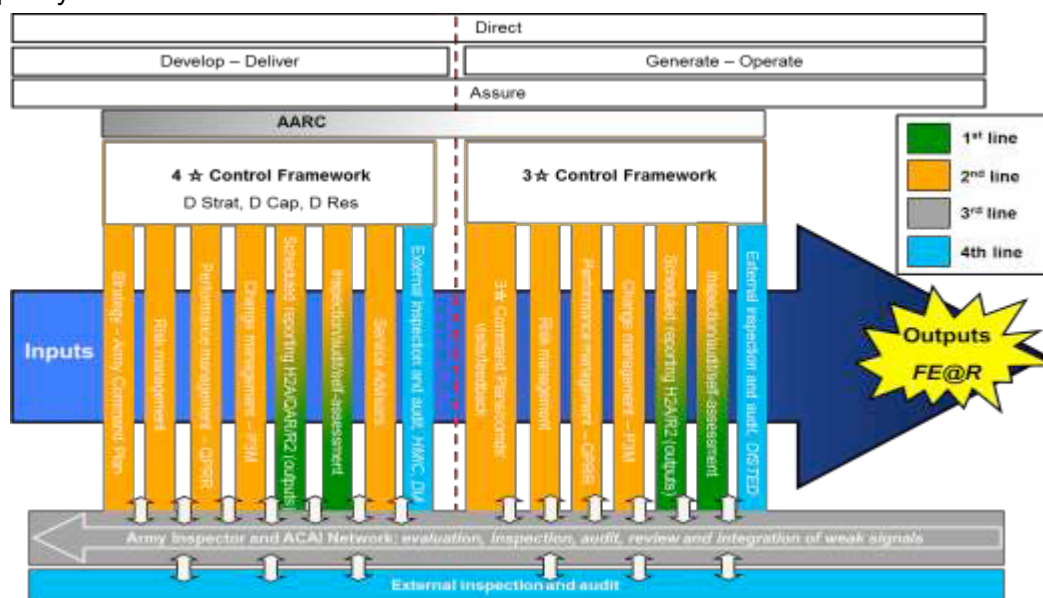

Figure 1 – Army Assurance Framework

---

[1] JSP 525: Corporate Governance, version 1 dated Dec 14.
[2] This is the new Defence-wide terminology that the Army has adopted. It replaces the legacy 1st, 2nd and 3rd Party *Layers of assurance activity* classifications.

4.   Within the Army's Assurance Framework is a spectrum of control measures. Alongside routine management checks, self-assessment and advisory visits, and reinforced by external scrutiny, is a regime of A&I that are applicable to *all* units and organisations regardless of role[3] (known as non-specialist). In addition there are a number of A&I that pertain to specific units or capabilities (known as specialist). In a number of areas, A&I are vital to licence essential activities, capabilities and facilities and in the identification and mitigation of risk. However, in the past this increasingly onerous regime has become more of a prescriptive management tool that imposes on the chain of command and is based on an assumption that levels of safety and assurance are in direct correlation to depth and frequency of A&I. Too often it has been seen as a means for finding fault and not as an effective method of identifying and then dealing with risk.

5.   On 19 Jun 15, the 472nd ECAB endorsed a set of principles to address this and to give overarching guidance to all who are involved with Army A&I as follows:

    a.   Encourage initiative and openness, providing appropriate freedoms to delegated Commanders and be operationally focused.

    b.   Improve operational effectiveness, for example by:

        (1)   Improving operational efficiency.

        (2)   Delivering a safe environment.

        (3)   Optimising the potential of our people.

    c.   Be tailored to readiness and role:

        (1)   One size does not fit all.

        (2)   Tailored inspections for Training, Reserve and Cadet Units.

    d.   Be delivered for the Chain of Command in the most efficient manner:

        (1)   Informed by Commanders' priorities.

        (2)   'Comply or Explain'.

        (3)   Based on frequency of inspection, geography and efficient use of SQEP.

    e.   Be ruthlessly focused on those functions that can only be checked through visits:

        (1)   Focused on 'must' and some 'should'.

        (2)   Exclude 'could' and some 'should'.

    f.   Utilise single sources of truth:

        (1)   Capture once and use many times.

        (2)   Make maximum use of simplified Reports and Returns and Management Information Systems.

    g.   Balance advisory visits and formal inspections[4].

---

[3] LEA, LSA, G1A, Climate Assessment, FEPA, FHPA, PDA, PSA, IDEA

[4] There was no distinction between A&I as inspection included all audit activity.

h.   Be informed by a robust Army Policy which provides coherence to all functional inspections.

Aim

6.   The aim of this ACSO is to provide overarching direction and guidance for the new regime of control measures in the 3 control framework as part of the Army's Assurance Framework.

Scope

7.   Directed by CGS through ECAB, the A&I regime creates an intelligent and bespoke programme of activity for each unit and organisation across the Army that ensures the chain of command is not stifled in its ability to empower and delegate; that allows Commanders to manage risk according to context and learn from genuine errors whilst not accepting recklessness and/or negligence; and that sees A&I as a means to identify risk and share good practice in the interests of continuous improvement. It is about making mission command work in peacetime or 'empowering decision makers and their staff whilst simultaneously removing unnecessary bureaucracy and process.'[5]

8.   This ACSO defines a new approach. Part 1 gives direction which all must adhere to[6] and Part 2 gives guidance for those involved in the new regime. It applies to all Army units and establishments, including all those that lie outside the Army TLB. It has been written to align with International Standardisation Organisation (ISO)[7] standards. The ISO family of quality management system's standards is designed to help organisations meet the needs of customers and other stakeholders while meeting statutory and regulatory requirements related to a product.

Glossary

9.   A glossary of key terms and definitions can be found at Part 3, but the following are critical to the understanding of all:

a.   **Assurance.** As described above, assurance is 'an evaluated opinion, based on evidence gained from review, on an organisation's governance, risk management and internal control framework.'[8]

b.   **Audit.** An audit is a 'systematic, independent and documented process for obtaining objective evidence and evaluating it…'[9]. All audit activity should be focussed on providing advice and assistance to Commanders, identifying areas of risk that will inform their risk management process; audit should encourage good practice and inform a continuous improvement cycle. As an audit is conducted against a published standard, auditors do not necessarily need to be SMEs. In audit, there may be a degree of subjectivity[10].

c.   **Inspection.** An inspection is a formal examination or review of performance and outputs, designed to assess effectiveness and to ensure fitness for purpose and defined as a 'determination of conformity to specified requirements'[11]. The requirement for inspection will

---

[5] ACP 15 dated 9 Apr 15.
[6] There is a small number of specialist A&I whose governance lie outside of the auspices of the Army. While these will involve external stakeholders the principles and mechanisms described in this ACSO still apply.
[7] An independent, non-governmental membership organisation and the world's largest developer of voluntary International Standards. These standards are internationally recognised and are used as a benchmark for quality. The ISO 9000 standards are based on seven quality management principles that senior management can apply for organisational improvement.
[8] JSP 525: Corporate Governance, version 1 dated Dec 14.
[9] ISO 9000:2015(E).
[10] Less for financial audit, which is an objective examination and evaluation of the financial statements to make sure that the records are a fair and accurate representation of the transactions they claim to represent. It can be facilitated internally at unit level by a suitably trained officer, or externally by an outside agency.
[11] ISO 9000:2015(E).

normally be imposed by national or international legislation or by a licensing authority in order to licence an activity, capability or facility. Unlike an audit, it is objective. An inspection usually results in a pass/fail grade and should be carried out by an SME.

Summary

10. The policy for A&I has been driven by the requirement to reduce the overly burdensome nature of the previous regime and empower the OPCOM chain of command through increased delegation, responsibility and trust. A change in culture is necessary that sees A&I as a constructive means to identify risk and how things can be done better as opposed to the current approach that seeks to find fault. In making these changes, the overall level of assurance across the Army will increase as a result of the chain of command's improved understanding and ownership of assurance together with its use of risk as a means to drive continuous improvement.

Part 1 – Direction

1.   The Army 3☆ control framework incorporates a number of internal control measures that are delivered via the mechanism illustrated at Figure 2 below. An effective and efficient control framework must be flexible, risk-based and focussed on continuous improvement, whilst encouraging a culture of excellence. While much of the activity should be conducted as Business as Usual (BaU), empowering Commanders and reducing the weight of assurance activity, the two key activities requiring policy and governance are A&I.
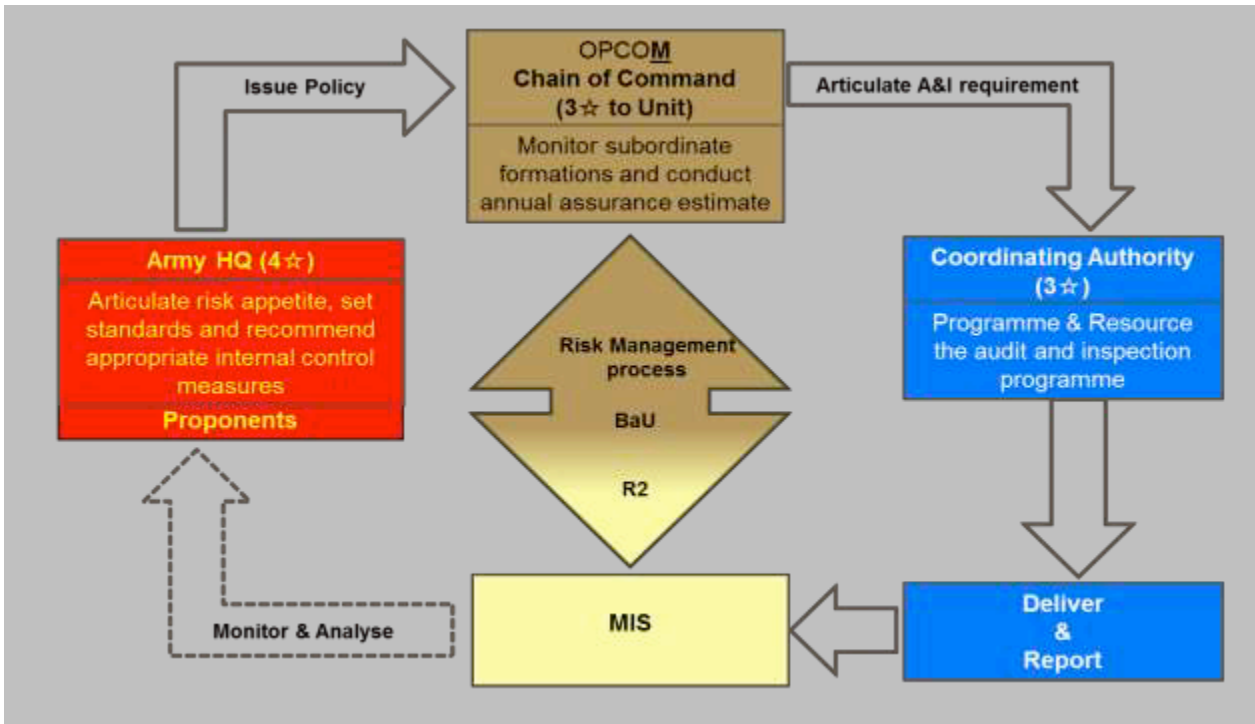

Figure 2 – 3   Internal control measures – delivery mechanism

Roles and Responsibilities

Creative tension. *The tension between those setting functional standards and those delivering capability helps ensure compliance and contributes to delivering effective self-regulation. In the Army this is achieved through those responsible for policy and regulation (4☆ Army HQ proponents) being in separate commands from those responsible for the Army's outputs (Field Army & Home Command).*

2.   **ECAB.** In accordance with Army Risk Policy[12], ECAB will routinely communicate the Army's risk appetite through the Army Command Plan and ECAB meetings. In doing so, ECAB will identify by exception the level of risk the Army is willing to tolerate in specific areas. This will be an iterative process, identifying where risk is acceptable through a clear understanding of ECAB's priorities, its view on new and emerging policies, feedback from ongoing A&I activity and, over time, an improved understanding of A&I trends.

3.   **Proponents.** Proponents – who are mainly, but not exclusively, in the Develop/Deliver areas of the 4☆ Army HQ – are responsible for setting Army policy, identifying the standards applicable within their area of expertise that the chain of command is required to achieve[13]. They are also

---

[12] Army Risk Policy 2016.
[13] For example Hd Trg (A) is the Proponent for Physical Development; he has ACAI responsibilities for PT, Sport and Adv Trg.

required to provide advice to the chain of command on the execution of activity. Proponents' responsibilities are as follows:

a. **Set the standards.** When setting standards, Proponents must consider changes in legislation, track new Defence and Army policies, analyse trends and interpret the Army HQ's appetite for risk in their area. Standards will be communicated to the chain of command through the publication of policies[14]. These are the standards to which the 3 formations must operate and against which internal control measures will report. These standards will be categorised as follows (further guidance can be found at Part 2, para 3):

   (1) **Must (non-discretionary)** – directed by statute, legislation or safety critical activities, informed by current risk appetite.

   (2) **Should (discretionary)** – directed by Defence or Army Policy.

   (3) **Could (recommended)** – 'good practice' as identified by the Proponent.

b. **Recommend appropriate internal control measures.** The term 'internal control measures' describes the range of activities available to provide assurance, ranging from routine internal management checks to formal inspections. Proponents will make recommendations on the most effective and efficient internal control measure required to provide the necessary levels of assurance to the chain of command and appropriate authorities, whilst minimising the impact on units. All internal control measures will meet the ECAB-endorsed principles. (Further guidance can be found at Part 2, para 4).

c. **Monitor, analyse and report.** Proponents will be required to continuously monitor and analyse the outcomes of control measures (remotely unless this is not possible owing to MIS or other practical limitations). This will ensure that they are equipped to make informed decisions on the development of future policy; inform standards; provide functional advice to the chain of command and report to the appropriate authorities. Proponents will regularly review their standards and recommended control measures to ensure continual optimisation of the internal control framework, informing the Army Inspector of the outcomes and informing the 2 pillar lead of any requirement to adjust risk appetite. ACAIs[15] are responsible to CGS, through the Army Inspector, for tracking the extent to which the chain of command is complying with policy. (Further guidance can be found at Part 2, para 2).

4. **OPCOM chain of command.** The OPCOM chain of command will undertake the following activities:

a. **3 and 2 Commanders' priorities.** 3 and 2 Commanders will routinely communicate their priorities and risk appetite through their annual directive. This will empower subordinate 1 Commanders to undertake an annual assurance estimate and take risk cognisant of the strategic context.

b. **Routine management checks and self-assessment.** The OPCOM chain of command is required to monitor its subordinates to assure itself that activity is being undertaken as it should be and in accordance with the standards. This BaU activity may represent the primary method of providing assurance; thus the data provided via routine management checks and self-assessment must be accurate and up to date. In line with the principles of R2A2 (as described in the AOM) the chain of command has the authority to determine the appropriate assurance activity based on BaU data supplied and COs can

---

[14] The philosophy and principles enshrined in ACSO 9001 set the parameters that will govern all A&I activity in the Army. Subordinate ACSOs relating to the practices and procedures for each A&I regime will be published beneath this ACSO as a hierarchy of A&I policy.
[15] All ACAIs are Proponents. There are 2 principal determinants that might require a Proponent to become an ACAI: Risk (to life, capability or reputation) or discrete legislation (a number of activities and policy areas are subject to discrete legislation where failure to comply would incur sanction; and thus where a greater degree of surety, in terms of compliance, is required).

expect to be held to account for the information they are responsible for providing. (Further guidance can be found at Part 2, para 7).

    c.   **Setting the requirement – the annual assurance estimate.** The conduct of the *annual assurance estimate* is fundamental to the process of 'setting the requirement'. This is the critical element of the A&I Regime, which allows each unit to be set an intelligently designed programme based upon a number of factors (for example, past performance, recent history and experience, personalities, and ongoing commitments). This will allow 1 Commanders to consider the policy set by Army HQ[16] and higher formations and gather advice from subject matter experts[17] before developing the annual A&I requirement for their subordinate formations, units and establishments. Once completed this estimate should be discussed with subordinates and subsequently agreed by the higher formation HQ. (Further guidance can be found at Part 2, para 8-10).

    d.   **Risk Management.** All A&I reports are to be made available promptly to the OPCOM chain of command. Where an area of non-compliance/conformance has been identified, these reports should offer advice to Commanders, allowing them to judge whether risks should be treated, tolerated, transferred or terminated[18] or transferred to higher authority.

Comply or Explain. *The accepted trademark of corporate governance in the UK is the 'Comply or Explain' approach[19]. In this context it allows Commanders, based on their annual assurance estimate, to take risk against policy and standards, giving their subordinates greater empowerment and responsibility for the delivery of outputs on their own terms. It allows assurance activity to be more agile; giving Commanders the opportunity to decide on the balance to be struck between conducting assurance activity and the risks of non-compliance. The comply or explain principle allows the chain of command to acknowledge the standards set by the Proponent but to make an informed decision not to apply the recommended internal control measures and be held to account.*

5.   **Coordinating Authority (CA)**[20]**.** Home Command (HC) will act as the 3 single CA for the delivery of all Army A&I with effect Apr 16. This is central to realising future efficiencies and reducing the burden on units. The CA's role centres on programming and resourcing the A&I regimes determined by the 1 assurance estimates. Specified tasks are detailed in Part 2, and will include:

    a.   **Designing the A&I programme and directing the teams to deliver A&I.** The programme for all A&I will be based on the calendar year. Once the overall requirement has been agreed with the OPCOM chain of command, the CA will be directed to design an audit programme across the Army and coordinate its delivery. (Further guidance can be found at Part 2, para 12.a-c.)

    b.   **Reporting.** Reporting should be an input to the risk management process and not an output in its own right. This is a critical element of the cultural change required in delivering this regime. It will ensure that reports reinforce that internal control measures are a vehicle for *'Risk management'* rather than *'Performance management'*. All reports should seek to identify risk rather than highlight failure and are to be made available promptly to the

---

[16] The subordinate ACSOs, written by the appropriate Proponent, will provide advice to the 1 OPCOM Commanders when formulating their annual assurance estimates. They will also offer advice on the management of risk in their SME area.
[17] 1 Commanders may request expertise from their higher formation to provide advice where they do not have integral assets.
[18] Army Risk Policy 2014.
[19] "It is recognised that an alternative to following a provision may be justified in particular circumstances if good governance can be achieved by other means. A condition of doing so is that the reasons for it should be explained clearly and carefully…In providing an explanation, the [company] should aim to illustrate a…clear rationale for the action it is taking, and describe any mitigating actions taken to address any additional risk and maintain conformity…"
[20] As defined in AJP-3(B) – Coordinating Authority or DIRLAUTH (Direct Liaison Authority) is the authority granted to a Commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more countries or commands, or two or more Services or two or more forces of the same Service.

OPCOM chain of command. In effect, A&I reports will be seen as *a constructive consultancy service*. (Further guidance can be found at Part 2, para 12.d.)

c.   **Using appropriate MIS.** The CA will maximise the use of current MIS and contribute towards the development of future MIS solutions and the supporting IT infrastructure. This will improve remote audit, reduce the time spent with units during A&I and enable A&I to be targeted on specific 'weak signals'. All A&I will be reported via the Army Reporting Management Suite v2 (ARMS)[21]. The CA will act as the ARMS 'Senior User' and is required to ensure that the application is fit for purpose, driving a programme of continuous improvement. This will require investment and prioritisation in the development and management of the application. (Further guidance can be found at Part 2, para 12.e.)

d.   **Leading the Army Assurance Delivery Steering Group (ADSG).** There is a requirement for a steering group to bring together all elements of the A&I regime. This will be co-ordinated and chaired by the CA with representation from the chain of command, policy proponents, A&I teams and the Army Inspectorate. The CA will continually monitor the introduction of new A&I. These will also be reported via the ACAI network. (Further guidance can be found at Part 2, para 12.f.)

6.   **The role of the Army Inspector.** The Army Inspector's role is to assure ECAB that the Army is not being exposed to unnecessary or avoidable risk. He will be responsible for monitoring the implementation of this policy on behalf of DCGS. He will track the ongoing optimisation of the regime and monitor the efficiency and effectiveness of all elements of the control framework and report periodically to the appropriate authority. Dependent on weak signals, the Army Inspector will formally review the regime on a routine basis.

Cultural change and continuous improvement

7.   The requirement for cultural change is critical to the implementation of the A&I regime. It is dependent upon importing mission command and genuine empowerment into peacetime leadership, management and administrative activity. Everyone involved must recognise that the product of the revised A&I regime is the improved understanding of risk and how to use this to drive business and improve output from a qualitative, quantitative and safety perspective. This regime is about making the most of what amounts to a well qualified consultancy service. It is not about passing or failing and should not be used as a performance management tool or for MS purposes. Equally, it is not an excuse for recklessness or negligence and Commanders, in setting their priorities, will make it very clear where the line should be drawn.

8.   All those involved in this process must be committed to a continuous improvement programme that will consolidate the effectiveness of the regime and exploit efficiencies as they are identified. It is critical that proponents and the chain of command continue to drive down overlap and duplication, in particular maximising the use of MIS rather than relying on a physical visit or demanding excessive, burdensome and outmoded Reports and Returns (R2).

---

[21] ARMS is a web based reporting tool for A&I reports. With further development, the system, combined with the facility for analysis and data mining within the ADW, will provide a common repository for all A&I activity and enable the chain of command to identify and understand where they hold risk.

Part 2 – Guidance

1.   The mechanism to be used for the Army's new regime of A&I is shown schematically at Figure 3 below. The paragraphs which follow in this section describe the overall process in detail.
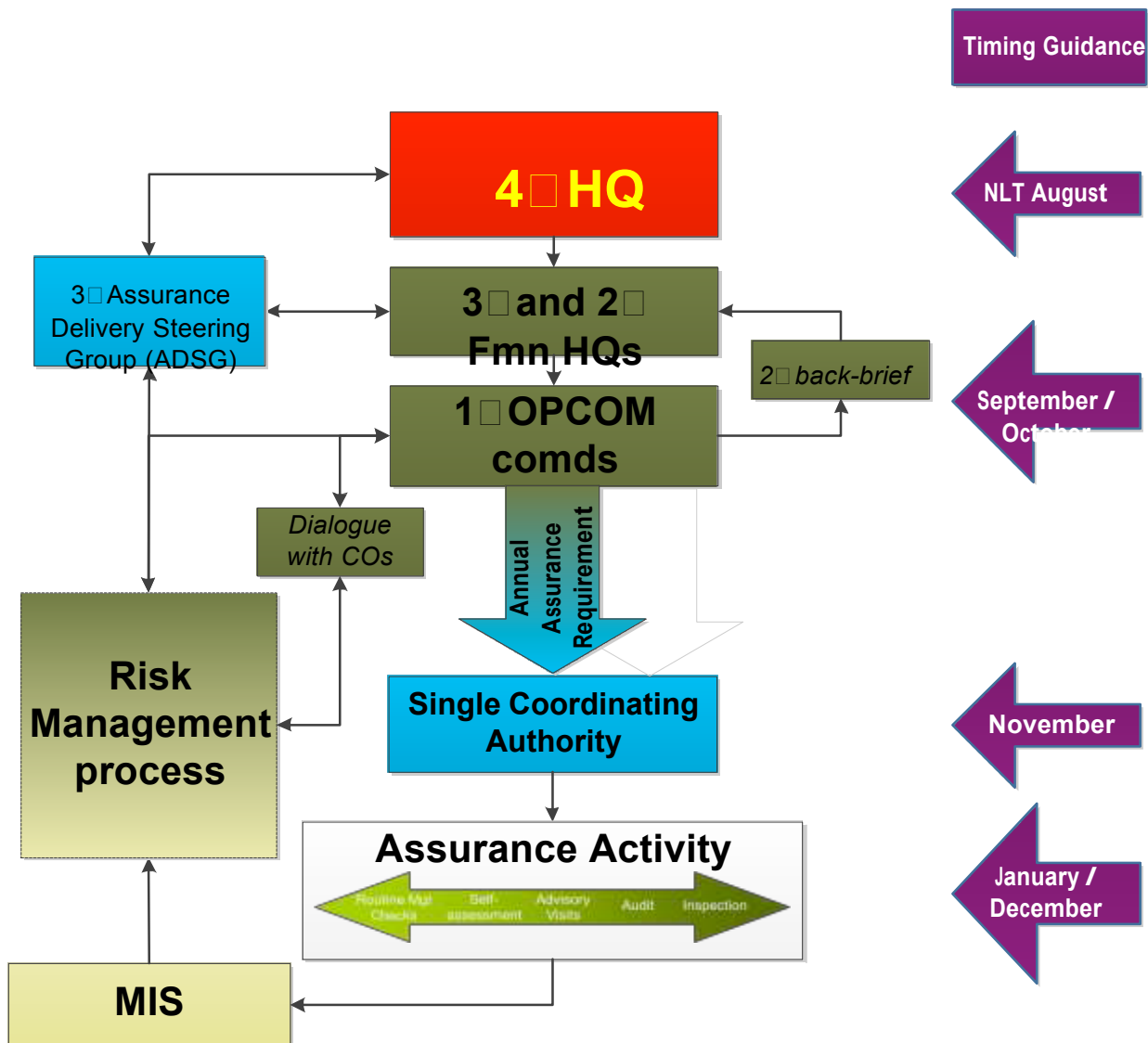

Figure 3 – Annual Army A&I Schematic

2.   **Use of MIS – current and future.** MIS is a key enabler for the A&I regime. It will allow:

a.   The chain of command to understand and manage risk across A&I regimes (in a common format), empowering Commanders and removing the need for most R2.

b.   'Intelligent reporting'. In conjunction with the Army Data Warehouse (ADW), data can be pulled from other applications to 'auto populate' answers to questions, reducing the burden on inspectors and units.

c.   A common format which enables one regime to ask a question and share the data with other regime owners, removing overlap and duplication.

d.   Standardisation of reporting rather than using stand-alone Word documents, Spreadsheets and PDFs on MOSS sites.

e.   Improved visibility of activity and co-ordination.

f.   Options for future-proofing against overlap and duplication.

g.   A measurement of effect process for the A&I system.

h.   Trends to be identified, better informing ECAB as it sets its appetite for risk.

Guidance for Proponents

3.   **Setting standards.** Proponents are responsible for setting standards. On an annual basis, Proponents should conduct a self-evaluation of their standards to rationalise against the 'must, should and could' criteria as illustrated in Figure 4 below. They should undertake a ruthless, but realistic prioritisation of all standards to ensure that they protect the Army from risk and maintain operational outputs, whilst minimising the impact on units. In brief, proponents should aim to:

a.   Reduce the 'must' to the minimum appropriate level.

b.   Address the 'should' by identifying the current MOD or Army imposed policies. These should be reviewed and, where appropriate, challenged. Proponents should report non-conformance at the 6 monthly Army Assurance Working Group (AAWG)[22].

c.   Drive out the 'could' from the formal A&I regime.
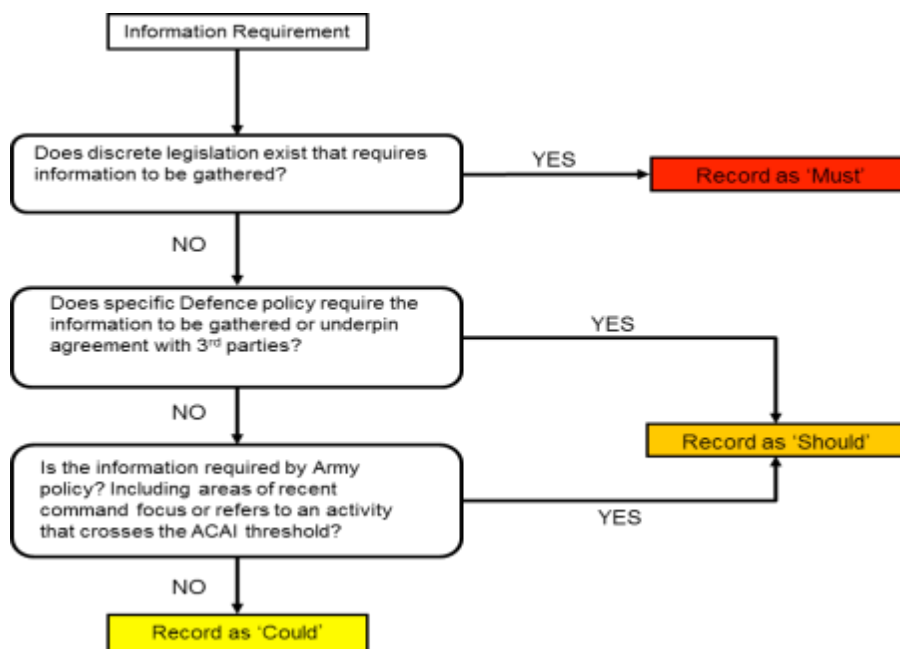

Figure 4 – Rationalisation Flow Chart

4.   **Recommending appropriate internal control measures.** Once a standard has been set, Proponents should recommend the most efficient and effective internal control measure to provide assurance both to the chain of command and the appropriate authority. The spectrum of internal control measures is illustrated in Figure 5 below. Proponents should continually review the control

---

[22] Chaired by the Army Inspector, the AAWG is the forum for ACAI reporting, an important source of information for the Army Inspector's quarterly report to ECAB.

measures within their regime to ensure that they remain appropriate and also that they meet the ECAB endorsed principles.

Figure 5 – Spectrum of Internal Control Measures

5.   **The spectrum of internal control measures.**   The recommended spectrum of internal control measures is detailed as follows:

    a.   **Routine management checks.**   These are the BaU activities conducted at unit level by the relevant specialists and duty personnel. These should be managed by the CO with the following considerations**:**

        (1)   Internal management checks should be measured against the standard set by the Proponent.

        (2)   Formation SMEs should provide assistance and advice routinely and react to issues/risks as they arise.

        (3)   Eventually, all such BaU activity will be reported via ARMS; however, it is recognised that until the MIS has fully matured, some R2 may still be required where necessary and appropriate though this should be minimised.

    b.   **Self-assessment.** This should be BaU activity directed by the Formation Commanders and managed by Formation SMEs in conjunction with the CO. This self-assessment will increase Commanders' awareness of the standards and provide assurance to the chain of command that the standards are being met or where risk is being carried. Reported routinely via MIS, it will allow the chain of command to remotely monitor, in many cases negating the requirement for a physical audit. The data from self-assessment activity will also inform the 1   annual assurance estimates**.**

    c.   **Advisory visits.** Advisory visits should be undertaken by formation SMEs. They should not be routine, instead being intelligently targeted based on:

        (1)   Weak signals identified via remote monitoring.

        (2)   Trigger events, for example a change of key personnel.

        (3)   The invitation/request of a CO or Formation Commander.

    d.   **Audit.** The majority of physical unit visits should take the form of audit rather than inspection. However, Proponents should only resort to physical audit when there is robust justification that less intrusive control measures are not sufficient. All audits should be informed by BaU activity, the output of which should be used to identify 'weak signals'[23] and inform the 1   annual assurance estimate.

        (1)   **Audit Intensity.** In their respective ACSOs, Proponents should provide 1 Commanders with a range of the following levels of audit:

---

[23] Weak Signal describes an area where sufficient evidence has been detected to suggest an activity or safeguard is either not present or not functioning as it should. They are analysed to identify linked issues and distinguish between cause and effect.

(a)   **Light** (non-discretionary elements only). This is likely to be the 'must' elements of the standards plus those elements considered non-discretionary due to the prevailing risk appetite.

(b)   **Medium** (all elements covered by the Light audit and selected elements directed by Defence and / or Army policy).

(c)   **Full** (including all elements covered by Light and Medium audit and any other additional requirements).

(2)   **Principles.** If deemed essential and approved by the appropriate authority[24], in addition to the ECAB endorsed principles, Proponents are to ensure that all audits comply with the following design principles:

(a)   They are aligned with Defence requirements and governed through the ACAI framework (ie each audit must be sponsored by an ACAI, aligning authority, accountability and responsibility).

(b)   They support effective risk management and adopt a risk based approach to determine frequency**.**

(c)   Every audit should be preceded by a thorough examination of unit documentation and data held on MIS. This will minimise the time physically spent in unit and allow auditors to focus on areas of risk identified in the preparatory work.

(d)   They reward good practice. For example, those units that are clearly utilising routine management checks and self-assessment to good effect will operate in an even less intrusive A&I regime.

e.   **Inspection.** A proponent should only recommend inspection when a formal statute or licensing requirement exists and therefore the instances of inspection will be minimal. In addition to the ECAB endorsed principles all inspections should adhere to the following criteria:

(1)   The outcome is a simple pass or fail (ie issue a licence or not).

(2)   Undertaken at the minimum allowable frequency to maintain licencing.

(3)   Programmed by the CA and de-conflicted with the audit programme.

(4)   Delivered by established specialist teams[25].

6.   **Removing and preventing 'overlap and duplication'.** Proponents should eradicate overlap and duplication within their own SME area and identify overlap and duplication between their area and others. Where this is not possible, they must ensure that units are only audited or inspected once and the findings shared with those who require it via MIS. Where it is essential to have an SME auditor or inspector the Proponent, in conjunction with CA, should ensure that a joint audit is conducted.

---

[24] HC as coordinating authority and Army Inspectorate.
[25] Specialist team personnel must be SQEP

Guidance for the OPCOM Chain of Command

7.   **Routine management checks / self-assessment.** Commanders will wish to have a sound understanding of the risks (to life, capability and reputation) of the activities conducted within their command. It also follows that assurance and the associated risk appetite must be an integral part of the Army's day to day battle rhythm. The internal control measures of routine management checks and self-assessment allow the chain of command to maintain situational awareness and enable it to undertake the following tasks:

    a.   Provide advice and assistance via SMEs.

    b.   React to issues and risks, elevating to proponents and appropriate authorities where necessary.

    c.   Conduct trend analysis to identify issues and risks.

    d.   Manage risk in accordance with the Army Risk Policy.

    e.   Provide formal feedback and contribute to future policy via the ADSG.

8.   **'Setting the Requirement'.** The OPCOM chain of command should have the freedom to influence the timing, frequency and intensity of internal control measures. In the majority of cases the assurance estimate will be undertaken by 1   Commanders and back briefed to 2   and possibly 3   Commanders.

9.   **Assurance estimate.** The 1   Commander is responsible for undertaking an annual assurance estimate where, in discussion with COs and formation SMEs, the requirement for A&I will be determined. This estimate should be conducted in sufficient time to allow programming to be carried out for the following calendar year. The Commander should ensure that findings are recorded and briefed to the OPCOM higher formation, in particular where it is considered appropriate to deviate from the minimum internal control measures recommended by the Proponent. When conducting the estimate the following factors should be considered:

    a.   3   and 2   Commanders' priorities and risk appetite. b.

        Unit role and readiness state.

    c.   Command and leadership experience.

    d.   Planned unit tasks and activities and manpower churn.

    e.   Historical performance.

    f.   Availability of unit Suitably Qualified and Experienced Personnel (SQEP).

    g.   Relevant SME and functional area advice.

10.   Once the 'requirement' is set across the formation, it should be presented to the single CA, which will resource the A&I programme. Only at this stage should the requirement be reconsidered and adjusted based on resource constraints if necessary.

Guidance for the Coordinating Authority (CA)

11. HQ HC is the single CA[26] and is responsible for programming and resourcing the A&I regime in accordance with the chain of command's needs as determined by the 1 assurance estimate process. It will gain traction and coherence based upon its OPCON command relationships with the Regional Points of Command. The CA will aim to remove stove-piping and prevent units being over-burdened by a plethora of external visits at the same time. ISO 19011[27] gives excellent guidance, detailing the principles of auditing as:

   a. Integrity.

   b. Fair presentation.

   c. Due professional care.

   d. Confidentiality.

   e. Independence.

   f. Evidence based approach.

12. **Role of the CA.** Tasks include:

   a. **Design the A&I timetable and matrix.** The programme for all A&I should be based on a calendar year cycle. 1 Commanders will carry out their estimate with sufficient time to ensure that the CA can programme the activity accordingly. When designing the A&I programme the CA should consider:

      (1) Audit programme objectives.

      (2) Roles, responsibilities and competence of the individuals managing the programme.

      (3) Identifying and evaluating programme risks.

      (4) Establishing processes and procedures.

      (5) Identifying and coordinating resources.

   b. **Direct teams to deliver A&I.** The CA should consider:

      (1) Defining objectives, scope and criteria for all A&I.

      (2) Selecting audit methods and auditors.

      (3) Monitoring and reviewing the audit programme.

      (4) Managing reports and maintaining records.

---

[26] Comd HC has delegated the task of routine coordination to HQ Regional Command (RC).
[27] The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies. This standard provides guidance on auditing management systems.

c.   **Direct the conduct of audits and evaluate auditors.** ISO 19011 gives detailed guidance on the conduct of audits and the competence and evaluation of auditors. Of note the CA should consider that all auditors should:

(1)   Meet the highest standards of personal behaviour and possess the KSE required to fulfil the role.

(2)   Undergo formal audit training[28].

(3)   Be evaluated regularly.

d.   **Audit reporting.** The CA is responsible for audit reporting. A standardised reporting method should ensure that audits do not produce a pass/fail result but instead conform to the new culture of identifying risk, bench-marking with others and encouraging good practice and continuous improvement. Audit reports will adopt the following categories:

(1)   **Conformance / identified good practice** (areas where the unit has met the standard/applied good practice).

(2)   **Opportunity for improvement** (based on good practice).

(3)   **Observations** (compliant / conforming, but close to becoming non).

(4)   **Non-conformance** (breach of policy).

(5)   **Non-compliance** (a breach of legislation / a safety critical problem).

e.   **Act as ARMS senior user.** The future regime will rely on effective and interactive MIS to support A&I. Initially, ARMS will be the primary MIS reporting platform and, combined with the facility for analysis and data mining within the ADW, will enable the chain of command to identify and understand where they hold risk. It should be used to protect from future overlap and duplication and remove the need for additional R2.

f.   **Lead the Army Assurance Delivery Steering Group (ADSG).** The ADSG will provide a natural 'Customer Executive Board' focus to deliver a lessons process, ensure continuous improvement, export good practice and review risk appetite. It will recognise and consider areas for continuous improvement to policy and procedures, promote best practice, identify and highlight areas of risk, within the services provided by the AI and Proponents, its subordinate formations. It will be the opportunity to recommend, to the Army Inspector, DCGS or ECAB as appropriate, areas for policy amendment or change

---

[28] As a minimum undertaking the IRCA approved 'Audit and Evaluation Skills Course' at Defence Academy or demonstrable equivalent.

Part 3 – Glossary of terms and definitions

Term	Definition
ACAI - Army Competent Advisor	A Suitably Qualified and Experienced Person (SQEP) appointed by CGS, on the advice of the Army Inspector, supported by a committee and/or staff [Inspectorate], who is the recognised Army Proponent and/or functional subject matter expert for an Army activity across Defence, which has a higher than normal degree of risk associated with it, or which is subject to discrete legislation.
and Inspectorate	An Inspectorate is an organisation that is recognised by the ACAI, but not necessarily owned by them, which is responsible for conducting A&I activity. The ACAI will use the results of inspectorate activity to inform assessments of their Proponent area.
Army Assurance Framework	The totality of the myriad control frameworks, the collective purpose of which is to assure the Army's outputs.
Assurance	An evaluated opinion, based on evidence gained from review, on an organisation's governance, risk management and internal control framework.[29]
Assurance Estimate	An annual risk based process, usually conducted at 1 level, which sets the requirement for the conduct of each discrete A&I regime.
Audit	Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.[30]
Business as Usual (BaU)	The normal execution of standard functional operations within an organisation, particularly in contrast to a project or programme which would introduce change (although that change may itself become *business as usual*).
Conformity	Fulfilment of a requirement.[31]
Control	An activity or measure that is expected to reduce the likelihood of a risk event occurring.[32]
Control Framework	A standardised and formal approach to defining and operating controls. It is a list of appropriately designed controls that mitigate departmental risks in an effective and efficient way.'[33]
Compliance	If the audit criteria are selected from legal or other requirements, the audit finding is termed compliance or non-compliance.[34]
Corporate Governance (MOD)	Corporate governance covers the way the Ministry of Defence is directed and controlled to deliver our strategic objectives. It comprises the checks and balances that regulate what we do, and provides the Permanent Secretary with the necessary formal assurance that the Department is being well run.[35]
Could	Developed to categorise those issues that are deemed to be good practice and are recommended.
Inspection	Activity conducted to confirm compliance with an established standard.
International Organisation for Standardisation (ISO)	International Organisation for Standardisation is responsible for the ISO 9000, ISO 14000, ISO 27000, ISO 22000 and other international management standards.

---

[29] See JSP 525 Corporate Governance, dated December 2014.
[30] ISO 9000 (2015). Quality management systems: fundamentals and vocabulary, p.30.
[31] ISO 9000 (2015). Quality management systems: fundamentals and vocabulary, p.19.
[32] JSP 892 Risk Management. Part 2 – Guidance, p.6.
[33] Integrated Risk. Control and Assurance Framework and the Defence Assurance Team Strategic Plan, p.6, para 33.
[34] ISO 19011 (2011). Guidelines for auditing management systems, p. 2.
[35] See JPS 525 Corporate Governance, dated December 2014.

Layers of assurance activity[36]	Assurance activities **were** categorised into three discrete layers. This legacy terminology has been replaced by the *Lines of Defence*.
1st Party Assurance	Assurance activity conducted across all levels of the chain of command for the self-declaration of conformity.
2nd Party Assurance	Separate assurance activity conducted by, or on behalf of CGS or ECAB.
3rd Party Assurance	Assurance activity carried out by independent organisations external to the Army or Defence. Usually there is a statutory basis for this assurance activity.
Lines of Defence[37]	This is the new Defence-wide terminology that the Army has adopted. It replaces the legacy 1st to 3rd Party *Layers of assurance activity* classifications.
1st Line of Defence	Assurance provided (internally) by those responsible for delivering the output.
2nd Line of Defence	Oversight (of first line) provided from within the chain of command in order to ensure policy compliance.
3rd Line of Defence	An assessment, achieved through internal audit, of the effectiveness of control, risk and performance frameworks.
4th Line of Defence	Assurance conducted by external auditors and regulators.
Must	Developed to categorise non-discretionary matters, directed by legislation.
Proponent	A Proponent is the SME that is responsible for setting functional standards and giving advice, however they are not necessarily ACAIs.[38]
Remote Monitoring	The use of Management Information Systems to gather and analyse A&I data when geographically dislocated from the target organisation.
Reports and Returns (R2)	There are two types of R2: *operational*, the information requirement to generate and maintain situational awareness; and non-operational, official correspondence and the formal passage of information.
Risk	An uncertain event or set of events that, should they occur, will have an effect on the achievement of objectives. Risk is measured by combining the probability of a perceived threat or opportunity occurring with the magnitude of its likely impact on objectives.[39]
Risk Appetite	The level of risk that the Army (organisation) is willing to accept.[40]
Routine Management Checks	Daily assurance activity initiated by the unit to provide Commanders at the lowest level enough information to understand the risks held.
Self-assessment	An internal assurance mechanism used by units.
Suitably Qualified and Experienced Personnel	An individual who has achieved a level of competence through appropriate formal training, recognised qualifications and sufficient practical experience in a relevant context. This combination results in an individual with a level of acquired knowledge that qualifies him/her to provide expert functional advice.
Should	Developed to categorise those issues that are driven by Defence or Army policy and which are discretionary.
Stakeholder	A person or *organisation* that can affect, be affected by, or perceive itself to be affected by a decision or activity.[41]
Subject Matter Expert	An individual who has thorough knowledge of a job, functions/tasks, or a particular topic, which qualifies him/her as an expert (for example, to consult, review, analyse, advise, or critique),or a person who has high-level knowledge and skill in the performance of a job.
Weak Signal	Describes an area of Army activity where it has detected sufficient evidence to suggest that the activity is either not present or is not functioning as it should. The term is deliberately distinct to mark it out as an Army Inspectorate rather than chain of command observation.

---

[36] For more information, see: Army Operating Model v.2.0, dated 30 Apr 16, Section 8.
[37] For more information, see: Integrated Risk, Control & Assurance Framework and the Defence Assurance team, October 2014.
[38] AGAI Vol 2 Chapter 56, Regulations for Training Requirements Authorities.
[39] Army Risk Policy, 2014-15, p.4-2.
[40] Army Risk Policy, 2014-15, p.4-2.
[41] ISO 9000 (2015). Quality management systems: fundamentals and vocabulary, p.12.