Information Assurance Strategy for the Driving Standards Agency
Executive Summary

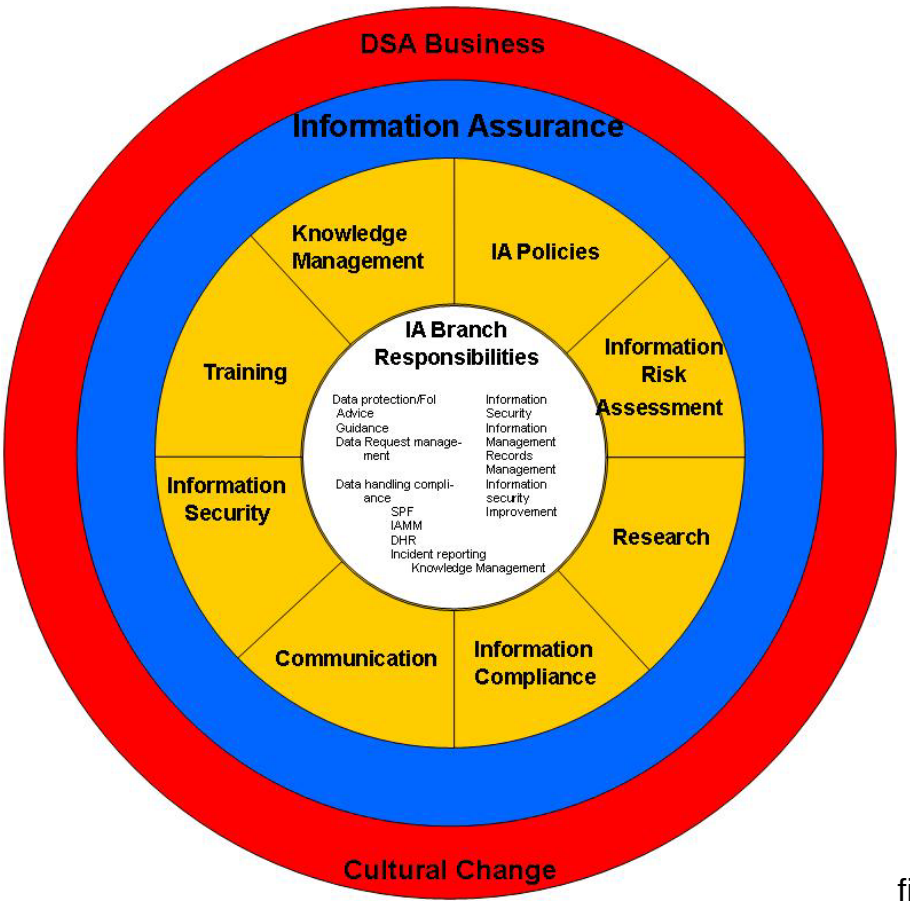

fig.1

1. Background

The Information Assurance Strategy is a description of what the DSA will do to meet its information management, protection and security responsibilities. The business and its customers, internal, external and major partners/suppliers need confidence that the information we hold, both personal and non-personal, is done so with due regard to its value and risk. This Executive Summary is intended to précis the attached Strategy (Appendix A), outlining the key activities associated with good information management and the assurance of it. Delivery partners and 3rd party suppliers are recent areas of emphasis from the Cabinet Office and plans are in hand to meet new assurance requirements.

2. Recommendations

That the Strategy be adopted and any deliverables (identified in italics) be undertaken in line with existing (and developing) policy/protocols.

3. Consideration

This Strategy examines information assurance against a background of various Key themed areas (described below). The term ‘information assurance’ (IA) is used to describe confidence in the processes of information risk management. Effective IA should ensure appropriate levels of availability, integrity, confidentiality, non-repudiation and authentication of data, information and information systems. This confidence is particularly important in the present environment, which is subject to unprecedented levels of malicious activity with intent to compromise UK information and information systems. Confidence is also improved through good Information Assurance where there exists the risk of non-deliberate loss, such as data sticks, papers left on trains etc.

IA is often described as a sub-set of information management. For DSA, IA is taken to include all information management activities. It is against this background that this strategy has been written, and is not just ‘information assurance’ in isolation.

3.1. The Business (Outer Wheel, fig.1)

Activities undertaken in relation to information assurance must have a relationship with DSA business. The IA Strategy has been designed around the business rather than around the IA function. As such, all IA activities are to be regarded as support activities to the business. In delivering advice on the management of information, four key “actors” are engaged:-

- People
- Process
- Information
- Technology

In delivering solutions/services for the business, IA will have regard to these actors alongside the core business requirement, which includes records and knowledge management, compliance and security.

Ownership and governance is described as well as the relationship between Information Asset Owners and their IA Information Partners (IP). The IP’s role is to provide information assurance advice, guidance and direction within a consistent corporate IA framework. In addition, IP’s will collect returns required by DfT and Cabinet Office with regard to IA.

3.2. IA Activities

IA will relate to government and/or business requirements, otherwise the activity is self fulfilling and not contributing to any viable requirement.

Whilst these activities are identified in great detail within the Strategy, the key components can be described as:-

- Information Management
- Information Security
- Compliance
- IA Reporting
    - Leadership and Governance
    - Training, Education and Awareness
    - Information Risk Management
    - Through-Life IA Measures
    - Assured Information Sharing
    - Compliance
- Knowledge Management
- Records Management

IA reporting is worthy of specific note. DSA are obliged to report on its activities in relation to information assurance maturity.

The Information Assurance Maturity Model (IAMM) expects the DSA to develop cultural change around the six key themes identified above under IA Reporting, the model itself is no more than a reporting tool, but provides value as a measure of change. DSA are currently measured as being at Level 1 of the IAMM and IA activities are designed to facilitate constant improvement whereby DSA will meet level 2 of the IAMM once assessed. It is important to note that the assessment does not deliver change, it merely measures it. The activities described in this report and the accompanying Information Assurance Strategy are intended to identify key deliverables which will drive IA maturity forward.

3.2.1. Leadership and Governance

The driving force behind any strategy and plan of action lies with the vision supported by the DSA Executive Board. It is the Board who are charged with recognising the importance of IA and establishing it as an integral requirement of corporate governance. The DSA Executive Board has already made this commitment. The next step is to endorse this strategy.

Beyond the Executive Board there is an established role of Information Asset Owner, this role is provided to staff who have service based responsibility for information assets. The DSA currently has 30 Information Asset Owners (IAOs) across the business estate. These IAO's are supported by Information Partners (IPs) from within the Information Assurance Branch. The role of the IP is to provide advice and guidance within a framework of consistency. The Head of Information Assurance acts as a conduit between central government and IAO's in relation to best practice and advice.

3.2.2. Training, Education and Awareness

Every member of staff is engaged in IA and is expected to participate in good information handling. Training, via the Cabinet office e-learning tool, is delivered to all staff. Specific training for IAOs is delivered by DSA and in turn DSA staff attend training events organised by the Information, Security and Assurance Branch of GCHQ supported by CESG who are also part of GCHQ, and the Centre for the Protection of the National Infrastructure (CPNI), part of the Security Services. The Senior Information Risk Owner (SIRO) has also received directed training from the aforementioned.

3.2.3. Information Risk Management (IRM)

A fundamental element of information Assurance relates to the delivery of information audits, privacy impact assessments and systems accreditation to provide assurance that the information held by DSA is done so within a risk managed environment. Information Audits are not carried out just on DSA held information, but also on its 3rd party suppliers and major delivery partners. Such major delivery partners include Pearson Vue, 3rd party suppliers include Capita, or Iron Mountain who provide off-site records storage.

3.2.4. Through-Life IA Measures (TLIA)

This concerns ensuring that plans exist to determine the status of all existing Information systems and ensuring new systems are subject to accreditation. Whilst similar to IRM, TLIA is activity based in relation to managing the full range of vulnerabilities and threats to information. Activities to inform this area includes compliance with the Security Policy Framework and assessing and base-lining security culture.

3.2.5. Assured information Sharing

There is a need to ensure that information sharing within and across organisational boundaries is done safely and proportionally to the value of the information in question. This requires the DSA to take an architectural approach to the security of new information systems.

3.2.6. Compliance

Relates to the Executive Board and ARMC receiving timely and relevant reports on activities developed and delivered to help improve assurance and compliance with the SPF. This should allow DSA to challenge assurance.

DSA will develop activities which will, through the IAMM, evidence improvement in IA Maturity.

3.3. Information Assurance Policies

DSA will deliver Information assurance policies against which the whole business will operate, supporting the consistent IA framework described earlier. In addition to the Policies, which are loosely described as the “what” there are (and will be) a number of Standard Operating Procedures SOPs), at least one for each policy.

DSA will develop an Information Assurance Policy Set and associated Standard Operating Procedures to inform and assist the delivery of IA objectives throughout the Business.

3.4. Information Risk Assessment

Information risk is managed in accordance with existing risk management principles. Information risk is evidenced, allocated an inherent risk score and then mitigation is applied followed by a residual risk score. The information asset is linked to the relevant risk register to align the two types of risk.

DSA will manage information risk in accordance with DSA Information Risk Management Policy.

3.5. Information Research

This involves the examination of reporting tools and information solution tools to facilitate improvement in information management, and, by default, information assurance. IA staff are in regular contact with other government departments and regularly attend assurance related events hosted by the Cabinet Office.

DSA will research information assurance to ensure its development is informed by best practice.

3.6. Information Assurance Compliance

This section details statutory compliance, government mandated compliance (Statement on Internal control, Data Handling Review etc), incident management and reporting, the information Assurance audit programme and compliance surrounding information sharing. Whilst the IAMM measures compliance, this section deals with the activity of compliance.

DSA will ensure that activities are developed and delivered to aid maturity in information assurance.

3.7. Information Assurance Communications

This chapter deals with identifying and embedding communication channels for the delivery and dissemination of information assurance related communications.

DSA will ensure that information assurance and security related communications reach intended customers and are easy to read, understand and comply with.

3.8. Information Security

This section expands upon previous chapters which mention the Security Policy Framework and accreditation. Information Security is governed through 7 key policies mandated upon all HM Government Departments and Agencies. Information Security also involves many other activities including virus and malware activity, cryptography and personal and physical security measures.

DSA will ensure that mandatory accreditation and best practice in relation to information security standards are followed where necessary, and if not mandated, where practicable.

3.9. Information Assurance Training

Training relates to all staff as well as specific training to Information asset owners, the SIRO and IA staff. Mentioned previously, training is an ongoing activity which requires constant attention if the information we handle is done so confidently. The DSA training plan carries a number of IA training courses aimed specifically at IA staff, who then use that training to educate and provide advice and guidance to DSA staff and its third party suppliers and main delivery partners.

DSA will ensure that Information assurance specialists receive training commensurate with business objectives.

3.10. Knowledge Management

Knowledge Management is a specific function within IA and seeks to deploy information resources in such a way as to obtain best value from that information. Knowledge management is about finding ways to best use the tacit and explicit information held by DSA, its staff and partners.

DSA will develop Knowledge Management related initiatives and develop a culture towards good knowledge management practice.

3.11. Cultural Change

Cultural change is identified throughout the strategy. However, to ensure that roles and responsibilities are clear, this has been defined as a specific plan and is consistent with the DfTc cultural change plan.

DSA will ensure the Cultural Change plan is embedded to assist in delivering IA maturity.

3.12. Conclusion

DSA has recognised the importance of IA and the Executive Board has mandated activities to deliver IA maturity and security culture change. The IA Strategy records that commitment and details the work to be undertaken by the business, its delivery partners and third party suppliers, supported by the IA Branch.