

Information Governance a structured Approach



Background

The past few years has seen a number of dramatic changes coming across the Local Authority Information Assurance landscape. The 2007 National Information Assurance Strategy, which was drafted to cover the whole of UK PLC, was published in June 2007, further changes began with the introduction of the Government Connect work programme, which was catapulted forward by the loss of the HMRC CDs, in November 2007, this in turn led to the Data Handling review.

Subsequent to the Data Handling Review, Kieran Pointer wrote his review of what actually happened at HMRC, Sir Edmund Burton, produced a report into the loss of various MoD laptops and a combined report was produced by former Information Commissioner Richard Thomas and Matthew Walport, around information sharing. Added to that, the government has reviewed its entire IA policy framework, replacing the Manual of Protective Security, with the Security Policy Framework (SPF), which contains the entire CESG policy framework.

Whilst all of this was going on, the Government Connect work programme had introduced the technical requirements for Local Authorities to be able to connect to a GSi (Government Secure Intranet), sub network, called GCSx. Because Local authorities do not have a method of formally accrediting the networks, another document called a code of connection was used, to ensure all Local Authorities were and are adhering to baseline HMG security policies and guidance. To ensure the effective measurement of these aspects in Government, the Information Assurance Maturity Model (IAMM) and the Information Assurance Assessment Framework (IAAF).

Moving Forward

The landscape today is complex, there is however a route through it. The key point to remember in all of this is that underpinning all of the technical requirements, is cultural change management.

The entire Information Assurance journey, needs to be engrained into the organisation, like Health & Safety. Information Assurance is not going away, it is a key requirement for the effective delivery of Shared Services and must be in place to facilitate the secure, effective sharing of information between, systems, organisations and agencies in an automated fashion. Manual interventions will always support work around, however to enable transformation in service delivery, effective automated information sharing needs to take place. This automation will need to happen to ensure the expected levels of cost reduction are materialised.

To help take this process forward, the CRIAG model has been developed;



Looking at the legal and regulatory aspects of Information Management, such as Data Protection Act, Freedom of Information Act, Computer Misuse Act, Regulatory Investigative Powers Act, Human Rights Act and where applicable, the Official Secrets Act.



Looking at the Government IS1 Risk Management model, the Business impact tables and how to apply those to a Local Government and Wider Public Sector audience. Risk Management should be at the heart of all business planning as it covers Financial risk, Operational risk, Corporate Risk, User Risk and Security Risk, which can be thought of as the FOCUS model.



Looking at Confidentiality, Integrity and Availability, where Confidentiality is keeping information safe, Integrity is keeping Information accurate and availability is keeping the information available. The CIA model helps understand the context for all of this.



Having the right structure in place to manage and monitor what is going on. Governance pulls everything together. There needs to be a convened governance group, governance roles; the SIOR, Information Asset Owners and Information asset administrators for large complex systems and where external or outsourced partners are involved.



Summary:

Compliance is often the business driver behind **WHY** we have information governance, risk gives us the intelligence and data to understand **WHAT** the threats, vulnerabilities and exploits our information is exposed to. **Information Assurance** gives us a practical framework to know **HOW** to deal with the risks, through operational processes, procedures and scrutiny. Governance gives us the formal structure **WHERE** and **HOW** we implement, monitor, audit and improve **WHAT** we are doing. This in the long run, will save money, improve efficiency and effectiveness by reducing risk.

You cannot reduce risk until you can quantify the risks you are dealing with. A car cannot know how fast it is going, unless you have a speedometer, brakes to slow it down and an accelerator to speed it up. You wouldn't want to rely on speed cameras and speeding fines to monitor your speed for you!

Resources and references

There are a number of interlinked documents and resources to help with the information governance piece. We have produced job roles, a business case for the SIRO role, terms of reference for the Information Governance Board and some guidance on how all of the frameworks slot together.