Information Assurance

Key Questions

- Following widespread reporting in the press and record fines for controlling personal information improperly, are you worried about your information? Do you know who has access to it, where it's kept, how it's processed and have you consciously accepted the risks around these activities?
- If you are a Government organisation or a supplier to Government, are you successfully complying with the required standards? Are you looking for a way to turn this compliance activity into a business enabler?
- Are you maximising the usefulness and return on investment on the information your company holds?
- Are your suppliers and partners asking about ISO 27001?
- What is Information Assurance (IA) and how does its implementation affect my business?

Why do I need IA?

Adequate protection of personal, financial, or other sensitive information is a legal requirement in many cases. Although private sector businesses with sensitive business information and information assets at stake will also benefit greatly from the confidence that their information risks are adequately managed. Information Assurance (IA) ensures that this protection is adequate through managing information risk – the conscious process of deciding what level of risk is appropriate to accept, which risks require treatment (to accept, reduce, avoid, or transfer risk), and where investment is best directed in order to meet the organisation's strategic aims.

Increasingly business is dependent on maintaining the confidentiality of its key information, in order maximise the return on investment from, for example, R&D activities, maintain a competitive advantage and comply with legislative requirements (for example, comply with the Data Protection Act).

Consideration should also be given to the integrity and availability of information, from a Disaster Recovery and Business Continuity perspective. This is especially important in the context of Industrial Control Systems (ICS). As these systems move from analogue communications to digital, ICS must be defended from Internet borne threats in order to ensure its availability and integrity so that the plant continues to run safely.

Information Assurance is the activity that enables these activities to be safeguarded, risks managed and investment where appropriate, justified. IA is therefore a strong business enabler, helping to

safeguard business activities, prevent legal challenges, maintain a competitive advantage and protect reputation.

Whilst government information security breaches provide most of the high-profile newspaper headlines, the impact of such breaches on commercial organisations can be just as severe as witnessed by fines imposed by both the FSA and the Information Commissioner's Office (ICO). For example, the FSA fined Nationwide £1M following the theft of an unencrypted laptop from an employee's home, Nationwide were unaware that this laptop contained personal information at the time of its loss. The ICO awarded over 27 penalties ranging between £60K and £440K for breaches of the DPA in the first year of its new legal power to impose fines.

How Does Implementing IA Affect My Business?

As information is now the lifeblood of most organisations; managing information risk effectively is a key part of good corporate governance, holding the organisation accountable for ensuring that information risk is assessed and managed to an appropriate level. As well as keeping the organisation safe from harm, it enables the acquisition of new business, re-use of information, justifies appropriate investment and becomes a selling point in its own right.

In the same way as the management of business risk, or financial or Health and Safety risk; the level at which Information Assurance is implemented depends on the nature of the business and

needs to be sensitively balanced with the organisation's culture. Managing information risk is more about the perceptive and insightful management of people and processes to ensure that information is used and protected correctly, than the implementation of technical controls – though appropriate use of technology has a useful part to play.

Organisations often worry that the measures needed to implement good IA practise will not only be expensive but will make IT systems harder to use. As with any requirement, building Information Assurance in at the start of any project is more cost effective and ensures that the management of information risk is pragmatic and balanced with business need; preserving the elegance of the original concept.

At Regency IT Consulting, we know that the key to success is to tailor the controls precisely to the varying needs of each organisation. We will provide you with IA recommendations that fulfil all of your legal obligations and provide adequate security for your systems, without proposing a 'gold-plated' solution that is impossible to live with.

Let our existing customers speak for us by having a look at some examples of Our Work.

Meeting Government Standards

UK Government organisations and suppliers to government are required to meet a plethora of standards, including those published by the Cabinet Office, CESG and in some cases CPNI.

Regency has deep experience in this area and employs a team of Government-approved CLAS consultants. All of our consultants have had high-ranking and successful careers in business, Government and the MoD; all of this experience ensures that Government Standards are applied in a way that is a business enabler rather than a millstone which chokes efficiency and creativity.

Contact us for more information on how we can help integrate IA requirements into the strategic direction of your organisation.

Maximising the Usefulness of Information

Information Assurance systematically identifies information that carries a value to the organisation, prioritises its importance in terms of Confidentiality, Integrity and Availability before analysing the relevant risks.

This process allows all important and valuable information to be identified; allowing its re-use throughout the organisation, increasing efficiency and saving money.

Using IA to Generate New Business

In the same way as ISO 9001 demonstrates a commitment to quality, ISO 27001 demonstrates a commitment to management of information risk. This standard has now become a key requirement of any contract where the customer shares its information with the supplier; and has never been more

important in qualifying for a place on Government framework contracts and winning new Public Sector business.

Regency IT Consulting have a deep understanding of both ISO 27001 and the Information Assurance requirements of Government and Public Sector organisations; through its provision of Information Assurance consultancy to both industry and Government. Contact us for advice to ensure that security requirements are built in at the start of a procurement or response to an invitation to tender. Building security in at the end is inevitably more difficult and expensive.

What can Regency offer me?

In short, business-literate services.

Regency knows that you have a business to run and will work closely with your people to deliver IA consultancy that points you in the right direction and is exactly fitted to your needs.

A number of objectives can often be achieved by putting in place just a few simple measures to address the most obvious IA shortcomings. Sometimes, these measures will involve changes in your existing business or procedures, rather than leading to great expenditure on new technical solutions.

ISO 27001

BS ISO/IEC 27001:2005 is recognised as the standard against which best commercial practice is measured in the IA field. The first stage in Regency's involvement with a customer will often be to carry out a gap analysis of your

current IA practice against ISO 27001, allowing us to suggest areas for improvement and to identify areas for immediate improvement. Our customers invariably find this a useful exercise, even if they are not pursuing formal certification to ISO 27001.

Regency ITC doesn't only talk a good ISO27001, Regency ITC currently holds ISO/IEC27001:2005 Certification for its Managed Encryption Service, Secure Data Centre and its general office systems.

IS 548043

All ISMS documentation for this Certification was produced and is maintained for ongoing Certification by our own personnel.

Legal Compliance

If your organisation handles significant amounts of personal data then Regency can advise on compliance with the Data Protection Act and your responsibilities under Freedom of Information legislation. If you process debit or credit card data then we can advise you on PCI-DSS Compliance.

Other IA Services

If you have more specific technical needs, then you might be interested in our Managed Encryption or Protective Monitoring services.

Other areas where Regency can provide you with authoritative IA advice include:

- Information Security Management System (ISMS) scoping, implementation and improvement;
- Development of security policies and procedures;
- Risk Assessment – HMG IAS 1&2; CRAMM, ISO 27005:2008 etc.;
- Preparation of Privacy Impact Assessments (PIAs);
- Physical and Environmental Security audits, including List-X;
- System hardening and lockdown;
- Firewall design and implementation;
- Organising network penetration testing or IT Health Checks;
- Business Continuity and Disaster Recovery planning;
- Forensic Readiness strategies and testing;
- Cryptographic standards and deployment;
- IA training packages tailored to your requirements.