



CESG
A2j, Hubble Road
Cheltenham, Gloucestershire
GL51 0EX

General Enquiries
Tel: +44 (0)1242 709 141
Date: 21 December 2009

Information Assurance in a Cost Cutting Climate

As the public sector enters a period of financial stringency, what effect will this have on Information Assurance (IA)? Will expenditure be slashed as an optional extra, favouring items with more immediate, tangible and measurable benefits, or will IA thrive as an indispensable enabler to delivering many valuable services? If the IA profession is to serve the long term interests of the public, it needs to explain why investing to improve IA skills and controls still makes good business sense. This article aims to help those who need to deliver that message.

For most Information Systems, IA costs are only a small part of the Total Cost of Ownership (TCO). If IA costs are less than 10% of the TCO, a 5% increase in IA costs to achieve a 1% reduction in TCO still delivers a healthy return on investment. Even higher returns may be achieved if improved IA enables new ways of doing business that were previously too risky to be accepted.

For large organisations that desperately need to reduce costs but also face increased necessity of widespread sharing of sensitive information, improving IA can actually be a great enabler. Below are 10 ways in which good IA can help organisations cut costs. References are provided for further information.

It should also be noted that investment to protect information invariably delivers much greater returns when applied at the start of the project lifecycle rather than after the main design decisions have been made, by which time the security of the end solution may already be severely constrained. CESG can provide consultancy to help design security in from the start.

1. **Home or Mobile Working**. More people working away from the office reduces the need for expensive office accommodation and can increase business agility and flexibility. But home or mobile working bypasses the office safeguards. [CESG Good Practice Guide No 10 on Remote Working](#) provides advice on managing the risks of doing so and in addition to this provides guidance on the use of bootable media. Further information of products that have been approved under the CESG Assisted Products scheme are available from http://www.cesg.gov.uk/find_a/caps/index.cfm.

NOT PROTECTIVELY MARKED

2. **Improved IT Capacity Management**. Many IT departments wish to reduce costs by consolidating their applications onto a smaller number of servers. Virtualisation is a common technology for achieving this but it comes with risks. [CESG Good Practice Guide No 12 on the Use of Virtualisation Products for Data Separation: Managing the Security Risks](#) helps organisations judge how far they trust virtualisation products to separate data of differing sensitivities.
3. **Outsourcing IT Services**. Specialist commercial IT service providers can often deliver services more cheaply than government can. But if the supplier fails to protect your data, you still remain accountable for the consequences. ISO 27001 details the requirements for an Information Security Management System and is widely used in industry. However simply demanding that your supplier be certified as compliant with the standard is not sufficient to ensure your data is appropriately protected. The standard does not mandate any particular level of security but it does mandate how it will be managed and that is sufficient for the client IA professional to monitor information security and drive changes where required. Ask for sight of the 'Statement of Applicability' which details which controls will be applied and ask for the option to participate in the management review process. A Google search on 'ISO 27001' provides a mass of information on certifiers and training.
4. **Offshoring**. Offshoring is the delivery of services from outside the European Economic Area (EEA) often realising savings from low labour costs. Under EU law, countries inside the EEA are obliged to implement law equivalent to the UK Data Protection Act. Countries outside the EEA may not provide this legislation. [CESG GPG No 6](#) provides guidance on Offshoring: Managing the Risks.
5. **Shared Services**. Rather than develop your own application or IT infrastructure it may be cheaper to share use of a service developed for other parts of government. Cabinet Office is driving the use of shared services particularly in the areas of networking, data storage and desktop services. How can you trust the security of services that you don't own or control? The Pan Government Accreditation service now provided by CESG aims to meet this need, making judgements on behalf of, and in consultation with data owners on whether the residual risks of an information system are acceptable. Enquiries on the service may be made to the CESG PGA Service Manager, Steve Drum via Stephen.Drum@cesg.gsi.gov.uk. Information on products and services already under collaborative development through the IA Technical Programme are available from http://www.cesg.gov.uk/products_services/iatp/index.shtml.
6. **Use of Untrusted Networks**. Organisations increasingly need to make connections to the Internet to share information with the public and business partners. The Internet can also provide a cheap network for supporting home or mobile working and enabling team working across disparate geographic areas. [CESG GPG No 8 – Protecting External Connections to the Internet](#) describes how to manage the risks of doing so.

NOT PROTECTIVELY MARKED

7. **Application Hosting**. Application Hosting (AH) is a term for an IT infrastructure designed to host multiple applications. AH can substantially reduce the TCO per application and the time taken to deploy a new application. But it is akin to putting a lot of eggs in one basket. Vulnerabilities in the AH infrastructure and even vulnerabilities in a single application can compromise all data hosted. Advice on developing AH systems can be obtained through CESG consultancy services or through some CLAS consultants. [CESG GPG No 9](#) provides advice on Taking Account of the Aggregation of Information. Penetration testing of an AH system can be obtained through the CHECK scheme detailed at www.cesg.gov.uk/products_services/iacs/check/index.shtml.
8. **Improved Risk Analysis & Treatment**. Many organisations accept security constraints that have evolved over time on the way they do business. In some cases scrutiny will reveal that whilst the constraint removes multiple risks, some can be cost effectively mitigated by other means and the rest are worth accepting, thereby enabling removal of the constraint. [HMG IA Standard No 1](#) provides a methodology for risk assessment and treatment.
9. **Centralised Controls**. A common practice in IA is to mandate policies or practices that need to be implemented by many users, project managers or system managers. The total implementation costs may be large but mainly hidden from management. Access management, anti-virus defences, network management and patching can come into this category. In such cases it is often cheaper to implement controls centrally and at the same time a higher level of assurance can be obtained.
10. **Use of KVM Switches**. Some users need access to multiple IT systems that cannot be logically connected due to different sensitivities. [CESG GPG No 11](#) provides advice on the use of Keyboard, Video and Mouse (KVM) switches that enable one user terminal to access multiple systems without permitting transfer of data between them.