

[This article is published in Public Service Review: Home Office]

CESG is the National Technical Authority for Information Assurance. Part of Government Communication Headquarters, CESG provides advice, products and services to protect UK Government communication and information systems. In this article CESG introduces the new Assurance Model. This Model expresses CESG's whole-life approach to the management of information risk and is designed to help both CESG and information risk managers meet the challenges posed by the increasingly complex Government ICT environment.

Information is important to any business. This is equally true for Government and the public sector, which rely on accurate and timely information to set policy and provide services. The Transformational Government Strategy has been established to transform the business of Government by making better use of information and communications technology (ICT) for the delivery of the public services and policy outcomes that impact on citizens' daily lives.

With such a revolution comes business risk. Risk should be managed throughout the delivery of any change. However, with the growing reliance of public sector organisations on information comes an increase in the impact of the post-delivery failure of the operational information infrastructure. Managing the risks to business information is known as 'Information Assurance' (IA). IA gives us confidence that our information systems will protect the information that they handle and will function as they need to, when they need to, under the control of legitimate users. This confidence is becoming increasingly important and IA is an essential enabler of the Transformational Government vision, as recognised by the 2007 UK National IA Strategy.

In recent years the focus for IA in Government has moved from those Departments whose information was at greatest risk during the Cold War to those Departments where the failure to protect information assets would significantly impact on life within the UK. The needs of these Departments are different, with many as concerned with the reliability of and access to their information as they are with its privacy.

Customer expectations have also changed. The growth of internet services has led to an expectation that Government will provide services in the same convenient, easy to use way. Under Transformational Government, Departments must share information and data in order to achieve their goals more than ever before. The use of information by Government has become greater in scope, and the supporting ICT systems more complex in nature. It is no longer possible to examine the risks associated with an information-handling asset when it is commissioned and regard that as sufficient.

The technology poses challenges too. ICT systems are no longer easily defined or bounded, as interconnections and data sharing blur the edges between the ICT of collaborating organisations. System improvements, new users and software patching mean that configurations quickly move away from the risk assessed base-line. Faster development times, frequent software upgrades and shorter component life-cycles

decrease the effectiveness of 'traditional' product evaluations and accelerate the throughput of new technologies and products.

It is to address these issues of need, expectation and complexity that CESG is developing a new Assurance Model. The Model is CESG's contribution towards addressing these challenges, and should help those managing risks to do so in a more consistent and balanced fashion. The Model is underpinned by four principles:

- that IA is an essential part of normal business risk management;
- that IA is a whole-life issue for information systems;
- that the responsibility for managing information risk is owned by the data owner;
- that having a requirement for IA need not necessarily prescribe specific risk mitigation activities.

The Model is for anyone who manages the technical risks to information assets, whether they are a Departmental ICT system Accreditor, a product manufacturer, or an ICT user. The Model can be used to identify alternative ways of mitigating the impact or likelihood of a risk, or to provide new sources of evidence in support of risk management. Ultimately the Model expresses CESG's understanding that mitigations for information risk exist across the life of an ICT solution and need not be exclusively focussed on a single evaluation event in the life cycle.

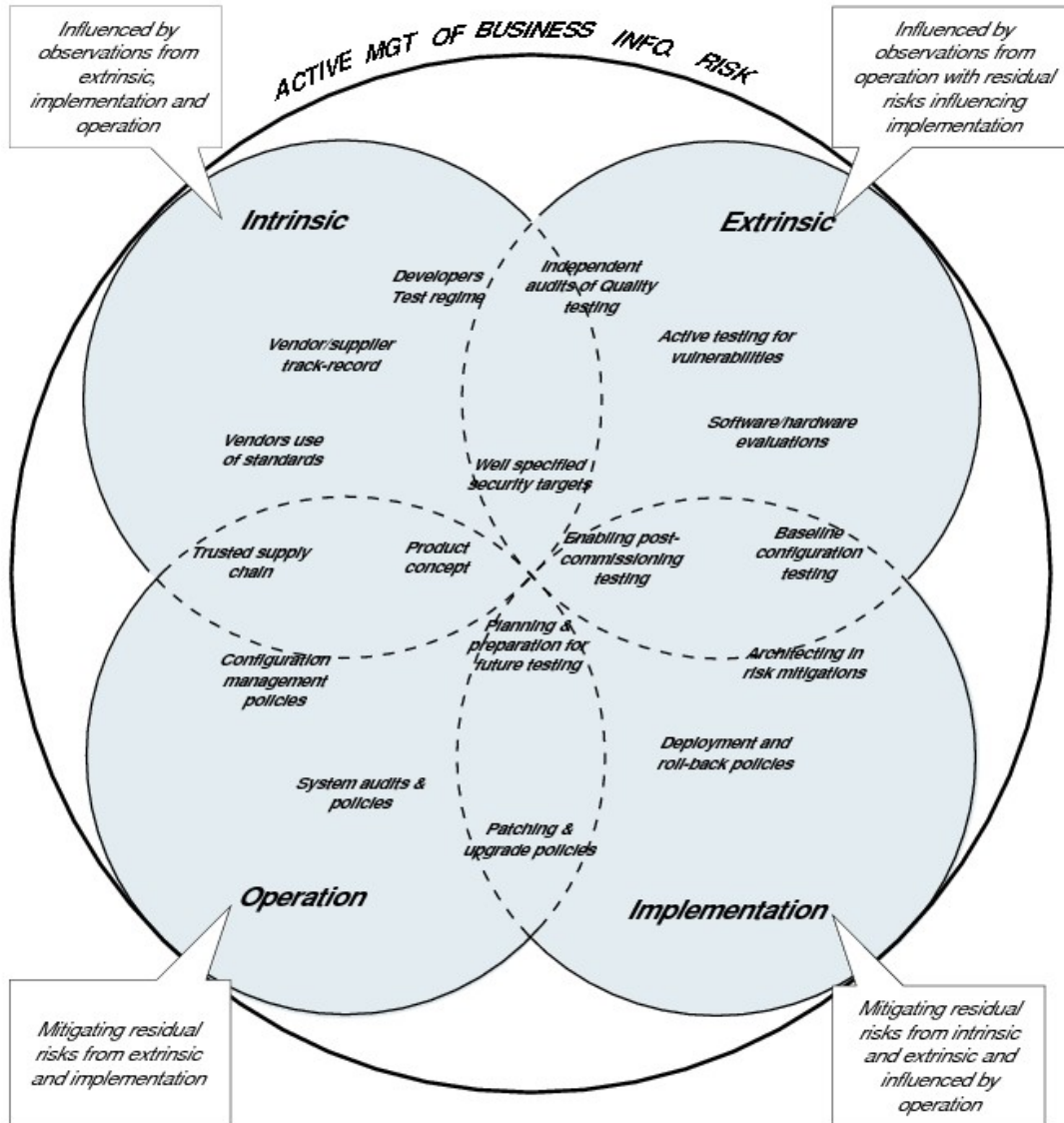
The Model itself comprises four elements:

- those considerations associated with the concept, origin and development of an ICT solution (Intrinsic);
- those considerations associated with the independent testing of an ICT solution outside the development environment (Extrinsic);
- those considerations associated with the architecture of the ICT solution and its integration with the business (Implementation);
- those considerations associated with an ICT solution that handles 'live' information or that is used or relied on by a business (Operation).

By considering the mitigations for a risk across all of these elements the risk managers or owners can build up a whole-life risk management plan. This has the potential to increase their level of confidence at less cost than would be the case were such mitigations to be 'bolted on' later in the solutions life. More importantly, by taking an holistic approach the risk manager can choose the most appropriate approach to managing an information risk, balancing the needs of the business for functionality with the needs of the business to manage the risks to the integrity, availability and confidentiality of its information asset. In providing a whole-life context to the risk owner the Model can help to identify mitigations that may be better suited to current business need – and business risk - than those that have traditionally been relied on.

CESG is currently trialling the Model to increase its understanding of what the Model means for the services that it provides to Government. This is the first part of a major business change within CESG that will see the Model – and its underpinning philosophy – made the foundation to our service portfolio. CESG intends to make the Model central to its engagement with Government and Industry stakeholders, since the Model represents a philosophy that CESG believes is immediately accessible to them. The project to trial the Model will complete later this year, and the results and

latest information will be made available to all stakeholders and partners. If you would like more information on the new CESG Assurance Model then please visit our web site at www.cesg.gov.uk.



The new CESG Assurance Model, showing the overlap between the elements and some of the factors from which risk mitigations can be derived.

Case study

A firewall is a simple component that controls accesses across an IT network boundary. Without the Model an accreditor managing the risks associated with a network connection might review the residual risk, and determine that an assured product is needed, but no more. Using the Model, however, the accreditor can acquire a broader set of supporting information and might ask questions such as:

- How much trust will be needed in the supply chain, both now and later? (Intrinsic, Operation)
- How will upgrades or patching be performed? (Intrinsic, Operation)
- Does the hardware or software need to be evaluated to mitigate the risks, or would regular penetration testing be more appropriate? (Extrinsic, Operation)
- Will the firewall be integrated into the business so its security functions aren't degraded? (Implementation)
- Can the firewall be configured to support the access policies that my business needs? (Intrinsic, Implementation)
- How will illicit access attempts be identified and what will be done if they occur? (Implementation, Operation)

By considering the answers to such questions a product vendor or system integrator might reduce or mitigate their delivery risks when seeking to gain accreditation for an ICT solution and identify areas for design improvements.